UNIVERSIDAD DE SEVILLA - FACULTAD DE DERECHO

TRABAJO FIN DE MÁSTER

MÁSTER UNIVERSITARIO EN ESTUDIOS EUROPEOS

LA DEFENSA COLECTIVA DE EUROPA ANTE EL DESAFÍO CIBERNÉTICO

Autor: Pablo Solano Díaz

Tutora: Carmen Márquez Carrasco
Catedrática de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Sevilla

Sevilla, a 17 de julio de 2014.

Universidad de Sevilla

Facultad de Derecho

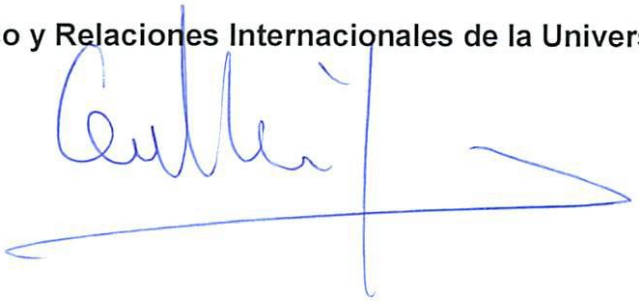
Trabajo fin de Máster

Máster Universitario en Estudios Europeos

Título: La defensa colectiva de Europa ante el desafío cibernético

Autor: Pablo Solano Díaz
Fdo.:

Tutora: Carmen Márquez Carrasco. Catedrática de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Sevilla
Fdo.:



Sevilla, a 17 de julio de 2014.

A mis padres y a mi novia, que siempre me apoyan o acompañan en mis incursiones euroatlánticas.

ÍNDICE:

ABREVIATURAS:

CAN.....Consejo del Atlántico Norte
CIJ.....Corte Internacional de Justicia
CMUE.....Comité Militar de la Unión Europea
CNU.....Carta de las Naciones Unidas
COPS.....Comité Político y de Seguridad
DARPA……*Defense Advanced Research Projects Agency*
EES.....Estrategia Europea de Seguridad
EMUE.....Estado Mayor de la Unión Europea
EU SOFA.....*European Union Status Of Forces Agreement*
IESD…….....Identidad Europea de Seguridad y Defensa
ONU.....Organización de las Naciones Unidas
OTAN.....Organización del Tratado del Atlántico Norte
PCSD.....Política Común de Seguridad y Defensa
PESC.....Política Exterior y de Seguridad Común
PESD.....Política Europea de Seguridad y Defensa
SACEUR.....*Supreme Allied Commander Europe*
SEAE.....Servicio Europeo de Acción Exterior
SHAPE.....*Supreme Headquarters Allied Powers Europe*
TAN…….....Tratado del Atlántico Norte
TFUE.....Tratado de Funcionamiento de la Unión Europea
TUE.....Tratado de la Unión Europea
UEO.....Unión Europea Occidental
URSS.....Unión de Repúblicas Socialistas Soviéticas

Resumen: *El presente trabajo tiene por objeto examinar el marco jurídico y político regulador del ejercicio de la legítima defensa en la Unión Europea y en la Organización del Tratado del Atlántico Norte, tanto en general como concretamente en el ámbito cibernético, para extraer conclusiones acerca del presente y futuro próximo de la cooperación entre las dos principales organizaciones internacionales de seguridad europeas en el contexto más amplio de las relaciones transatlánticas. Para ello, la exposición comienza con en una primera parte dedicada a evaluar el estado del Derecho internacional público en relación con el uso cibernético de la fuerza, seguida de una descripción del marco político de la cooperación entre la Unión y la Alianza, con expresa referencia a la rebautizada Política Común de Seguridad y Defensa. La tercera parte se consagra a analizar específicamente la colaboración UE-OTAN en materia de ciberdefensa y a exponer los puntos clave que marcarán el desarrollo futuro de la esta asociación estratégica a modo de conclusión para finalizar con un conjunto de propuestas al respecto.*

Abstract: *This thesis aims at assessing the legal and political framework governing the exercise of self-defence by the European Union and the North Atlantic Treaty Organisation both from a general standpoint and from the cyber perspective, in order to draw conclusions about the present and near future of the cooperation between the two main European security organisations within the broader context of the transatlantic relations. To this end, this dissertation begins with a first part dedicated to ascertaining the state of the art of Public International Law as regards the cyber use of force, followed by a description of the political framework regulating the cooperation between the Union and the Alliance, with specific reference to the re-christened Common Security and Defence Policy. The third part is devoted to analysing the EU-NATO collaboration in the field of cyberdefence and exposing the cornerstones of the future development of this strategic partnership by way of conclusion, finishing with several recommendations on the way ahead.*

Palabras clave: *acuerdo Berlín Plus, ciberdefensa, ciberseguridad, Estrategia Europea de Ciberseguridad, legítima defensa individual y colectiva, Organización del Tratado del Atlántico Norte, Política Común de Seguridad y Defensa, relaciones transatlánticas, Unión Europea, uso de la fuerza.*

Keywords: *Berlin Plus agreement, Common Security and Defence Policy, cyberdefence, cybersecurity, Cybersecurity Strategy of the European Union, European Union, individual and collective self-defence, North Atlantic Treaty Organisation, transatlantic relations, use of force.*

Mots clés: *accord Berlin Plus, cyberdéfense, cybersecurité, légitime défense individuelle et collective, Organisation du Traité de l'Atlantique Nord, Politique de Sécurité et de Défense Commune, relations transatlantiques, Stratégie Européenne de Cybersécurité, Union Européenne, usage de la force.*

1 INTRODUCCIÓN:

El concepto de seguridad ha experimentado grandes cambios desde que el mundo bipolar de la Guerra Fría diera paso a un nuevo escenario geoestratégico caótico en el que distintos actores estatales y no estatales y potencias emergentes y re-emergentes disputan el poder al tradicionalmente todopoderoso occidente, tratando de pescar en el río revuelto post-westfaliano de la globalización. En los últimos años, además, el progreso tecnológico exponencial ha difuminado el poder y generado nuevas amenazas a la vez que una devastadora crisis económica ha convertido en inasequibles o a supeditado a otras partidas en los presupuestos nacionales algunas de la capacidades necesarias para hacer frente a aquellos desafíos. En este contexto, la superpotencia norteamericana, que no es ajena a esta deriva multipolar ni a la coyuntura recesiva que impone restricciones presupuestarias inéditas incluso al gigante militar, se ha visto obligada a concentrar sus recursos en sus nuevas áreas de interés, como Oriente Medio y Asia-Pacífico, dejando “Europa para los europeos”.

Este panorama representa la oportunidad idónea para que la Unión Europea (en adelante UE), que ha ido progresivamente forjando un política de seguridad y defensa dentro de su acción exterior aún de marcado carácter intergubernamental, reclame de la Organización del Tratado del Atlántico Norte (en adelante OTAN) una mayor responsabilidad en la defensa de Europa, definiéndose así una nueva asociación estratégica más equitativa para ambas organizaciones internacionales de seguridad. Ello habría de realizarse en el marco de unas relaciones transatlánticas más equilibradas desde hace tiempo reclamadas por Washington en aras de un mayor reparto de los costes, aunque con la condición de que una defensa autónoma de la Unión no se construyera en perjuicio del protagonismo de la Alianza (todo es negociable).

El ciberespacio, última frontera de la seguridad y fuente de nuevas amenazas, por regular jurídicamente y por controlar militarmente, sin fronteras nacionales y con infinitas posibilidades de desarrollo de capacidades, es la excusa ideal para forjar esta nueva imagen de la UE como actor internacional de seguridad fuerte que habla de tú a tú a la OTAN y a Estados Unidos como

su socio único y esencia, a la vez consciente de la necesidad de cooperar estrechamente con ellos para la protección de los valores e intereses comunes y de no depender de ellos totalmente para su defensa.

No obstante, este camino está plagado de obstáculos, entre los que destaca la diferente concepción del Derecho internacional predominante a ambas orillas del Atlántico y consecuentemente entre la UE y la OTAN e incluso dentro de éstas, que lleva a adoptar posiciones divergentes, si irreconciliables o no será objeto de un extenso análisis en este trabajo, en lo que respecta al marco jurídico regulador de la legítima defensa individual y colectiva ante ciberataques. A la presentación de este marco y las diferentes perspectivas al respecto se dedica la primera parte. La segunda y la tercera se reservan para el análisis del marco político de la cooperación entre la Unión y la Alianza en general y específicamente en el ámbito de la ciberdefensa respectivamente, dejando entrever que bajo la punta del iceberg constituido por aquella diferencia de concepciones se esconden mayores escollos como son las diferencias ideológicas y, sobre todo, la falta de voluntad de los Estados miembros por definir una política común de seguridad y defensa coherente que permita a la UE ocupar el lugar que le corresponde en las relaciones internacionales. Al fin y al cabo, querer es poder.

2 REVISIÓN DE LA BIBLIOGRAFÍA:

En la elaboración de este trabajo se ha combinado la lectura de diversas obras de expertos en Derecho internacional, notablemente Antonio Remiro Brotóns (2010), en la materia del uso de la fuerza, especialmente el Manual de Talín de Michael Schmitt (2013), o en las relaciones entre la UE y la OTAN, particularmente Martin Reichard (2006), con el estudio de documentos institucionales de la Unión y de la Alianza. Entre estos últimos destacan los que se incluyen en los anexos, concretamente la Estrategia Europea de Seguridad, la Estrategia de CIberseguridad de la UE, las conclusiones del Consejo Europeo de diciembre de 2013, la nota de prensa que contiene el acuerdo Berlín Plus y la Política de Ciberdefensa de la OTAN.

PARTE I: MARCO JURÍDICO DEL USO CIBERNÉTICO DE LA FUERZA EN EUROPA:

3 MARCO JURÍDICO DE LA LEGÍTIMA DEFENSA COLECTIVA EN DERECHO INTERNACIONAL PÚBLICO:

3.1 AMENAZA Y USO DE LA FUERZA Y ATAQUE ARMADO:

El marco jurídico de la legítima defensa en el Derecho Internacional Público se articula en torno a dos normas, cuya validez universal como reglas de Derecho Internacional consuetudinario es generalmente aceptada [1]: la prohibición general de "la amenaza y el uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas", consignada en el artículo 2.4 de la Carta de las Naciones Unidas (en adelante CNU); y su excepción, "el derecho inherente a la legítima defensa, individual o colectiva, en caso de ataque armado" consagrado en el artículo 51 del mismo tratado fundacional. En consecuencia, el análisis del alcance normativo de estos preceptos y la propia virtualidad del sistema de defensa colectiva previsto en la Carta parten de la delimitación de los conceptos de "amenaza y uso de la fuerza" y "ataque armado".

Si se atiende a los trabajos preparatorios de la Carta[2], el artículo 2.4 establece una presunción *iuris et de iure* de ilegalidad de cualquier amenaza o uso de la fuerza, aunque no se dirija efectivamente contra la integridad territorial o la independencia política de un Estado[3]. Tal es la lógica "institucionalizadora" del sistema de seguridad "onusiano", sustentado sobre la premisa de que los Estados miembros de la Organización de las Naciones

[1] En este sentido se pronunció la Corte Internacional de Justicia*, Sentencia de 17 de junio de 1986 en el asunto de las actividades militares y paramilitares en y contra Nicaragua, Organización de las naciones Unidas*, La Haya, 1986, párrafos 176 y 193.

[2] Asamblea General de las Naciones Unidas, *Documentos 1123 (I/8, 6 UNCIO), 65 (1945), 784 (I/1/27, 6 UNCIO), 336 (1945), 885 (I/1/34, 6 UNCIO) y 387 (1945)*, Organización de las Naciones Unidas, San Francisco, 1945.

[3] Schmitt, Michael (coord.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, p. 45, regla 10.

Unidas (en adelante ONU) ceden de derecho soberano clásico a recurrir unilateral y discrecionalmente a la fuerza[4], *ius ad bellum*, a una autoridad superior concentrada en el Consejo de Seguridad para que, en caso de "amenaza a la paz, quebrantamiento de la paz o acto de agresión"[5], dicho órgano lo ejercite de forma colectiva, "a nombre de"[6] todos los miembros, y con la sola finalidad de mantener o restablecer la paz y la seguridad internacionales. Este mecanismo permite a las Naciones Unidas cumplir su propósito primordial de mantener la paz y la seguridad internacionales[7].

En lo que respecta al ámbito de esta prohibición del recurso a la fuerza, el primer problema es la deliberada indeterminación jurídica de la noción de "fuerza", en torno a la cual los Estados miembros, particularmente las potencias occidentales, prefirieron mantener la ambigüedad y no incluir en el artículo 2.4 de la CNU la redacción que sí dieron en el Preámbulo[8], en la se condena la "coerción militar, política, económica o de cualquier otra índole contra la independencia política o la integridad territorial de cualquier Estado" [9]. Veinticinco años después, la Asamblea General, en su "Declaración sobre los Principios de Derecho Internacional relativos a las Relaciones de Amistad y a la Cooperación"[10], ofreció una solución de compromiso al desacuerdo entre, por una parte, el Bloque Occidental y, por otra, los países en desarrollo apoyados

[4] Esta cesión se opera a través de Organización de las Naciones Unidas, *Carta de las Naciones Unidas de 24 de octubre de 1945* [1 UNTS XVI], San Francisco, 1945 [disponible en http://www.un.org/es/documents/charter, último acceso el 1 de julio de 2014], artículo 24.

[5] *Ibíd.*, artículo 39.

[6] *Ibíd.*, artículo 24.

[7] *Ibíd.*, artículo 1.1.

[8] Véase Randelzhofer, Albrecht, "Article 2(4)", en Simma, Bruno, *The Charter of the United Nations: A commentary*, Oxford, Oxford University Press, 2002, pp. 117 y ss., p. 118, donde mantiene que los Estados redactores, particularmente las potencias occidentales, rechazaron la propuesta brasileña en este sentido, reticentes a reducir a la ilegalidad todo medio coercitivo de ejercer presión sobre otros Estados

[9] Remiro Brotóns, Antonio (coord.), *Derecho Internacional*, Madrid, Tirant lo Blanch, 2010, p.ágina1061.

[10] Asamblea General de las Naciones Unidas, *Resolución 2625 (XXV)*, Organización de las Naciones Unidas, Nueva York, 1970, párrafo 31.

por la Unión de Repúblicas Socialistas Soviéticas (en adelante URSS)[11], situando la ilicitud de las formas de coerción no militares en el ámbito del principio de no intervención en los asuntos internos de los Estados. En cualquier caso, la posición doctrinal predominante considera que la prohibición se limita a la fuerza armada[12].

Sí es claro que la amenaza o el uso de la fuerza en el interior de un Estado no están proscritos por el artículo 2.4 de la CNU, en tanto el interno es un plano reservado a la actividad policial -*law enforcement*- y protegido de injerencias externas por el mencionado principio de no intervención en los asuntos internos de otros Estados, también de Derecho internacional general[13] y cristalizado en el artículo 2.7[14] CNU, sin perjuicio de la controvertida "responsabilidad colectiva internacional de proteger [*responsibility to protect*] a las poblaciones del genocidio, los crímenes de guerra, la depuración étnica y los crímenes de lesa humanidad" declarada en el Documento Final de la Cumbre Mundial de 2005[15].

En lo que respecta al segundo concepto objeto de análisis en este epígrafe, el asunto de las "Actividades militares y paramilitares en y contra Nicaragua"[16], la Corte Internacional de Justicia (en adelante CIJ) definió el "ataque armado" como "la más grave forma de uso de la fuerza", postulando de este modo la existencia de una "zona gris" integrada por aquellas amenazas o usos de la fuerza que, aunque prohibidos convencional y consuetudinariamente en todo caso, no traspasan el umbral del ataque armado y, por lo tanto, no justifican el ejercicio del derecho a la legítima defensa. Por el contrario, un acto coercitivo

[11] Harrison Dinniss, Heather, *Cyber Warfare and the Laws of War*, Cambridge, Cambridge University Press, 2012, p. 47.

[12] Dinstein, Yoram, *War, Aggression and Self-Defence*, Cambridge, Cambridge University Press, 2001, p. 86.

[13] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 202.

[14] Organización de las Naciones Unidas, *op. cit., supra* (nota 4), artículo 2.7.

[15] Asamblea General de las Naciones Unidas, *Documento Final de la Cumbre Mundial*, Organización de las Naciones Unidas, Nueva York, 2005, párrafo 139.

[16] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 191.

situado dentro de este espectro generaría meramente el derecho a la adopción de contramedidas, entendiendo por tales aquellas

> "medidas que serían contrarias a obligaciones internacionales del Estado lesionado respecto al Estado responsable si no hubieran sido tomadas por aquél en respuesta a un acto internacionalmente ilícito de éste para procurar su cesación y reparación"[17].

La puesta en marcha de un contraataque armado en legítima defensa o, por el contario, de una simple contramedida como respuesta un ilícito constitutivo de amenaza o uso de la fuerza es en primera instancia una decisión política del Estado objeto del mismo, basada en una calificación razonable del ilícito al que se responde como ataque armado o no y con inmediata comunicación en el primer caso al Consejo de Seguridad[18].

En este sentido, los artículos 2 y 3 del anexo a la resolución la Asamblea General de las Naciones Unidas de 1974, rubricada "Definición de la agresión", [19] establece los criterios que deben guiar la constatación por el Consejo de Seguridad de un ataque armado (*agression armée* en la versión francesa de la Carta) y, por lo tanto, la reacción de los Estados víctimas de actos coercitivos. Así, la consideración del "primer uso de la fuerza armada por un Estado en contravención de la Carta" como "prueba *prima facie* de un acto de agresión" se condiciona a que "el hecho de que los actos de que se trata o sus consecuencias" revistan la "suficiente gravedad"[20], lógica asumida por la CIJ en su criterio de "escala y efectos" [21]. Cumulativamente y a título meramente ejemplificativo[22], se mencionan, como supuestos de ataque armado

[17] Crawford, James, *The International Law Commission´s Articles on State Responsibility*, Cambridge, Cambridge University Press, 2002, p. 281.

[18] Organización de las Naciones Unidas, *op. cit., supra* (nota 4), artículo 51.

[19] Asamblea General de las Naciones Unidas, *Resolución 3314 (XXIX) sobre la definición de la agresión*, Organización de las Naciones Unidas, Nueva York, 1974.

[20] *Ibíd.*, artículo 2.

[21] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 195.

[22] Véase Asamblea General de las Naciones Unidas, *Resolución 3314 (XXIX)..., op. cit., supra* (nota 19), artículo 4, que establece que "la enumeración de los actos mencionados

o agresión, la "invasión y la ocupación militar, el bombardeo, el bloqueo de los puertos o de las costas o el ataque contra las fuerzas armadas terrestres, navales o aéreas o la flota mercante o aérea" de un Estado por parte de las fuerzas armadas de otro[23].

También pueden considerase ataques armados en función de su escala y efectos, incluyendo el nivel de control o participación por parte del infractor, las agresiones indirectas, como son la utilización de unidades situadas en bases extranjeras en infracción de lo acordado o prolongando en ellas su permanencia más allá de lo convenido[24], supuesto sobre el que falló la CIJ en el asunto de las "Actividades armadas en el territorio del Congo"[25], o la financiación de grupos insurgentes o terroristas y la organización y reclutamiento de bandas armadas o mercenarios. Parece más razonable, en cambio, considerar las amenazas de la fuerza, tales como las demostraciones militares, los ultimatos y la concentración de tropas en la frontera, como "usos menos graves de la fuerza"[26] que no justifican la legítima defensa, pero que están prohibidos en la medida en que lo estuviera su materialización en un acto[27], justificando el ejercicio de contramedidas.

Además, los conceptos de amenaza y uso de la fuerza y de ataque armado, como las piezas clave en el marco jurídico internacional regulador del derecho a la guerra, se exigen mutuamente. Por una parte, el derecho inmanente a la legítima defensa individual y colectiva, a pesar de su carácter

anteriormente no es exhaustiva y el Consejo de Seguridad podrá determinar qué otros actos constituyen agresión, con arreglo a las disposiciones de la Carta".

[23] Asamblea General de las Naciones Unidas, *op. cit., supra* (nota 19), artículo 3.a)-d).

[24] *Ibíd.*, artículo 3.e).

[25] Corte Internacional de Justicia, *Sentencia de 19 de diciembre de 2005 en el asunto de las actividades armadas en el territorio del Congo*, Organización de las Naciones Unidas, La Haya, 2005.

[26] Remiro Brotóns, *op. cit., supra* (nota 9), p. 1060.

[27] Así lo pone de manifiesto la Corte Internacional de Justicia, *Sentencia de 12 de diciembre de 1996 en el asunto de las plataformas petrolíferas*, Organización de las Naciones Unidas, La Haya, 1996.

inherente o natural[28] confirmado por la CIJ[29], sólo adquiere significado jurídico en tanto excepción a una prohibición general del recurso a la fuerza, siendo lógicamente insustancial en presencia de un derecho soberano *ad nutum* a hacer la guerra[30] y gozando, en cualquier caso, de reconocimiento universal[31]. Por otra parte, la Carta procede a asumir la regulación consuetudinaria preexistente como cláusula de salvaguardia necesaria del sistema institucionalizado de seguridad colectiva de las Naciones Unidas, presidido por el a menudo inoperante Consejo de Seguridad.

A este respecto, la CIJ, en el asunto de las "Plataformas Petrolíferas", ha desautorizado la interpretación de algunos Estados en virtud de la cual el artículo 51 de la CNU introduce una regulación convencional paralela a la de Derecho Internacional general y de menor alcance que ésta[32]. Efectivamente, frente a la pretensión estadounidense de justificar su ataque contra buques iraníes en la regulación convencional del derecho a la legítima defensa recogido en el artículo XX de un tratado bilateral de 1955 sobre amistad, relaciones consulares y derechos entre ambos Estados, el Tribunal de la Haya sostuvo que

> "la interpretación y aplicación de ese artículo implicará necesariamente un análisis de las condiciones de la legítima defensa bajo el Derecho Internacional [...], es decir, las provisiones de la Carta de las Naciones Unidas y el Derecho Internacional consuetudinario".

Tampoco es razonable afirmar que la regulación convencional de la legítima defensa derogue o sustituya a la consuetudinaria, pues de la metodología jurídica general y la doctrina de la interpretación de las fuentes

[28] En la versión inglesa, se puede leer *inherent right* y la de nuevo más elocuente traducción francesa hace referencia a un *droit naturel*.

[29] Corte Internacional de Justicia*, op. cit., supra* (nota 1), párrafo 190.

[30] Remiro Brotóns, *op. cit., supra* (nota 9), p. 1064.

[31] Díez de Velasco, Manuel, *Instituciones de Derecho Internacional Público*, Madrid, Tecnos, 2013, p. 1073.

[32] Corte Internacional de Justicia, *Opinión consultiva de 8 de julio de 1996 sobre legalidad de la amenaza o el uso de las armas nucleares*, Organización de las Naciones Unidas, La Haya, 1996, párrafos 40 y 42.

jurídicas se deriva que una costumbre jurídica está vigente hasta que haya evidencia suficiente de una nueva regulación consuetudinaria sobre la misma materia[33].

Además de la respuesta individual a un ataque armado, el derecho de legítima defensa presenta también una vertiente colectiva que ampara la reacción de terceros Estados sobre la base de la solicitud de ayuda por parte del Estado víctima, requisito exigido por el antes referido principio de *ius cogens* de no intervención en los asuntos internos de los Estados[34], o de un tratado bilateral o multilateral en virtud del cual un conjunto de Estados se obliga internacionalmente a asistir a cualquiera de ellos en caso de ataque armado[35]. Los ejemplos clásicos de este tipo de convención son el artículo 3 del Tratado Interamericano de Asistencia Recíproca o Pacto de Río de 1947 y el artículo 5 del Tratado del Atlántico Norte (en adelante TAN) de 1949, que, con una estructura similar, consignan el compromiso de las partes de considerar cualquier ataque armado contra una de ellas como un ataque dirigido contra todas que justifica una reacción colectiva en ejercicio del derecho a la legítima defensa reconocido en el artículo 51 de la CNU. El Tratado de Lisboa de 2007 añadió una cláusula similar en el artículo 42.7 del Tratado de la Unión Europea (en adelante TUE), que será objeto de un análisis detallado en el siguiente epígrafe, recogiendo el testigo del Tratado constitutivo de la Unión Europea Occidental (en adelante UEO) de 1948 e igualmente respetuosa de "los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte" [36].

Estos tratados de asistencia mutua quedan integrados en el sistema de seguridad colectiva de la Carta, que, en el Capítulo VIII dedicado a los "Acuerdos Regionales", no sólo permite su existencia siempre que sea

[33] Brownlie, Ian, *Principles of Public International Law*, Oxford, Oxford Press University, 1990, pp. 3-4.

[34] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 185.

[35] Remiro Brotóns, *op. cit., supra* (nota 9), p. 1065.

[36] Unión Europea, *Versión consolidada del Tratado de la Unión Europea* [2010/C 83/01], Lisboa, 2007, artículo 42.7.

compatible con los Propósitos y Principios de las Naciones Unidas[37], sino que además los convierte en instrumentos de las medidas coercitivas aplicadas bajo la autoridad, o con la autorización, del Consejo de Seguridad[38], al que en todo momento deben mantener informado "de las actividades emprendidas o proyectadas [...] con el propósito de mantener la paz y la seguridad internacionales"[39].

3.2 CONDICIONES PARA EL EJERCICIO DEL DERECHO A LA LEGÍTIMA DEFENSA:

Una vez presentado el derecho a la legítima defensa individual y colectiva como epicentro del marco jurídico del recurso a la fuerza, en el contexto de un sistema de seguridad en el que el Consejo de Seguridad no es realmente la "instancia de autoridad en la Comunidad internacional vertebrada e integrada"[40] que cabría esperar de la estricta lectura del Capítulo VII de la Carta, se hace necesario determinar las condiciones bajo las cuales el ejercicio de aquel derecho está justificado desde el punto de vista de la CNU y del Derecho Internacional general.

Lo primero que cabría preguntarse es si un ataque armado puede ser perpetrado por agentes distintos a los Estados, consideración que choca frontalmente con una concepción tradicional reduccionista de la subjetividad internacional[41], la cual por otra parte ha sufrido una radical transformación como consecuencia de acontecimientos como los del 11 de septiembre de 2001 que dan fe del auge del terrorismo internacional. A este respecto, algunos autores han llegado a inferir de la aceptación que mostró la Comunidad internacional hacia la intervención estadounidense en Afganistán una costumbre *new look* que extiende el concepto de ataque armado a los actos

[37] Organización de las Naciones Unidas, *op. cit., supra* (nota 4), artículo 52.

[38] *Ibíd.*, artículo 53.

[39] *Ibíd.*, artículo 54.

[40] Carrillo Salcedo, Juan Antonio, *Curso de Derecho internacional Público*, Madrid, Tecnos, 1991, p. 224.

[41] Remiro Brotóns*, op. cit., supra* (nota 9), p. 1070.

terroristas de alcance masivo[42]. En esta línea parece ir el propio Tratado de Funcionamiento la Unión Europea (en adelante TFUE) de Lisboa al incorporar una cláusula de solidaridad en su artículo 222, en virtud de la cual "la Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano [...]". Este precepto será objeto de análisis detenido más adelante.

Aunque es un extremo polémico, parece justificado el ejercicio de la legítima defensa contra actores que, aun no ostentando la condición de sujetos de Derecho Internacional, actúen como tales al tener control fáctico sobre un espacio físico y unos recursos dentro del territorio de un Estado incapaz de imponer su autoridad[43], siempre que el ataque sea lo suficientemente grave y que la respuesta se circunscriba a dichos espacio físico y recursos, no afectando al resto del territorio del Estado en el que se encuentran[44]. Las Resoluciones del Consejo de Seguridad 1368 y 1373[45], emitidas unos días después de los ataques contra Washington y Nueva York, avalan implícitamente esta tesis que ha calado hondo desde el principio en la práctica estatal de las potencias occidentales.

Al margen de este requisito subjetivo, operan también condicionantes objetivos. Efectivamente, el Tribunal de la Haya ha afirmado [46] en la

[42] Condorelli, Luigi, "Les attentats du 11 septembre et leurs suites: où va le droit international", *Revue Générale de Droit International Public*, número 105, 2001, pp. 829-848, p. 843.

[43] En caso de beneplácito o apoyo del Estado desde cuyo territorio se orquesta el ataque armado no cabe imputar a este no permite atribuirle automáticamente la responsabilidad por el mismo, como destacó la CIJ (1986), pero al menos estaría incumpliendo el principio de Derecho Internacional general de precaución, que impone a los Estados la obligación de no permitir conscientemente que su territorio sea usado para actos contrarios a los derechos de otros Estados" reconocido en el asunto del "Estrecho de Corfú" (Corte Internacional de Justicia, 1949, p. 22).

[44] Remiro Brotóns, *op. cit., supra* (nota 9), p. 1072.

[45] Consejo de Seguridad, *Documentos S/RES/1368, de 12 de septiembre de 2001, y S/RES/1373, de 28 de septiembre de 2001*, Organización de las Naciones Unidas, Nueva York, 2001.

[46] Corte Internacional de Justicia*, op. cit., supra* (nota 32), párrafo 41.

mencionada opinión consultiva sobre la "Licitud de la amenaza o el uso de armas nucleares" y reiterado en sucesivos pronunciamientos[47] que la sumisión del ejercicio del derecho a la legítima defensa a las condiciones de necesidad y proporcionalidad es una regla de Derecho Internacional consuetudinario. En concreto, el presupuesto de necesidad implica ante todo la discriminación entre las medidas de fuerza susceptibles de ser empleadas, pero también la imposibilidad de cumplir el objetivo defensivo a través de otros medios, constituyendo así la otra cara de la moneda de la proporcionalidad[48], y la dimensión espacio-temporal de inmediatez, tercer requisito de *ius cogens*. Las tres condiciones fueron referidas en la carta de 1842 del Secretario de Estado estadounidense Daniel Webster al británico Lord Ashburton[49] en relación con el asunto "Caroline"[50], considerada la primera formulación de los límites a la legítima defensa y en la que muchos ven el origen de la doctrina anticipatoria.

Adicionalmente, un sector de la doctrina defiende que una evidencia creíble de la identidad del atacante y de la fuente del ataque armado debe situarse en pie de igualdad con los otros tres principios[51], con el inconveniente de que no existe un estándar aplicable a los casos en los que no es posible probar claramente aquella imputación. En este sentido, la CIJ rechazó la pruebas indiciaria y altamente indiciaria (*suggestive evidence* and *highly suggestive evidence*) alegada por Estados Unidos como base suficiente para afirmar la

[47] *Ibíd.* y Corte Internacional de Justicia, *op. cit., supra* (nota 25).

[48] Ago, Roberto, "Adición al octavo informe sobre la responsabilidad de los Estados", *Anuario de la Comisión de Derecho Internacional* [Doc. A/CN.4/318/Add. 5 a 7], volumen II, 1980.

[49] Ministerio de Asuntos Exteriores del Reino Unido, *British and foreign State papers, volume 30, 1841-1842*, Reino Unido de la Gran Bretaña e Irlanda del Norte, Londres, 1842, pp. 195-196.

[50] Véase Moore, John Bassett, *A digest of international law, volume 217*, Washington D. C., Government Printing Office, 1906, donde relata que, según Webster, la alegación de la legítima defensa debe fundarse en "la necesidad inmediata e imperiosa de defensa propia, que no permita otra elección ni deje tiempo para deliberar".

[51] Gill, Terry y Ducheine, Paul, "Anticipatory Self-Defense in the Cyber Context", International Law Studies of the US Naval War College, volumen 89, 2013, pp. 438-471, pp. 451-452.

vinculación iraní con los ataques sobre buques mercantes en el Golfo Pérsico en el asunto de las "Plataformas Petrolíferas"[52].

Por lo demás, la regulación convencional de la legítima defensa añade otros parámetros exigidos por la propia articulación entre el sistema de seguridad colectiva instituido en la Carta y el derecho a la legítima defensa, cuales son el deber de comunicación inmediata al Consejo de Seguridad de las medidas utilizadas, la temporalidad, provisionalidad o transitoriedad y la subsidiariedad de las medidas estatales respecto de las adoptadas por el Consejo de Seguridad[53]. No obstante, al igual que la inmediatez opera en términos relativos en consideración al tiempo necesario para preparar la respuesta armada, a la subsistencia del ataque y a la neutralización total de los efectos de la agresión, este carácter subsidiario y temporal predicado por la Carta de la acción defensiva estatal no supone la automática cesación de la misma una vez que el Consejo de Seguridad adopte "las medidas necesarias para restablecer la paz y la seguridad internacionales", si aquellos efectos persisten[54] y en la medida en que éste no exprese su intención de que así sea[55]. Sin embargo, una dilación injustificada convierte la acción defensiva legítima en represalias, un uso de la fuerza prohibido por el Derecho internacional[56].

Esta misma concepción teleológica permite evaluar la proporcionalidad de la acción defensiva en función de la naturaleza e intensidad del ataque, no valorando no sólo la equivalencia entre el *quantum* de la agresión y el de la respuesta, sino también la suficiencia de ésta respecto a su finalidad de desactivar aquélla[57], desde una perspectiva que atiende no tanto a una estricta

[52] Corte Internacional de Justicia, *Sentencia de 6 de noviembre de 2003 en el asunto de las plataformas petrolíferas*, Organización de las Naciones Unidas, La Haya, 2003, párrafo 161.

[53] González Campos, Julio Diego, Sánchez Rodríguez, Luis Ignacio y Andrés Sáenz de Santa María, María Paz, *Curso de Derecho Internacional Público*, Madrid, Aranzadi, 2002, pp. 900 y ss.

[54] Remiro Brotóns*, op. cit., supra* (nota 9), pp. 1075-1076.

[55] Gill y Ducheine, *op cit., supra* (nota 51), pp. 447-448.

[56] Asamblea General de las Naciones Unidas, *op.cit., supra* (nota 10).

[57] Remiro Brotóns, *op. cit., supra* (nota 9), pp. 1073.

equivalencia de medios entre ataque y defensa como a un juicio de prudencia o razonabilidad [58]. Desde este punto de vista, podría ser proporcional una respuesta contundente ante un ataque armado conducido a través del ciberespacio, como se analizará en el tercer epígrafe.

3.3 LEGÍTIMA DEFENSA ANTICIPATORIA:

Junto a la proporcionalidad, la necesidad y la inmediatez, un cuarto presupuesto de inminencia parece estar implícito tanto en la regulación convencional como en la consuetudinaria del derecho a la legítima defensa individual y colectiva, en tanto nada obliga a los Estados a diferir su acción defensiva al momento en que la agresión se ha consumado[59]. La aceptación de esta premisa lleva a afirmar la legitimidad de la defensa anticipatoria o "preemptiva" -*pre-emptive self-defence*-, adoptada en defensa de "una manifiesta e inequívoca amenaza de ataque en el futuro próximo"[60], concepto que no debe ser confundido con el de defensa preventiva, mayoritariamente considerada sin cabida en la Carta[61] y basada en la apreciación subjetiva de amenazas potenciales o latentes [62]. La doctrina estratégica de la defensa preventiva, disfrazada bajo el término "acción preemptiva" en la Estrategia de Seguridad Nacional de los Estados Unidos de 2002 [63] por la administración Bush, sirvió de justificación para la invasión de Irak bajo el pretexto infundado de su posesión de armas de destrucción masiva al grito de "nuestra mejor defensa es una buena ofensiva"[64]. En el mismo documento se añade que, si bien a menudo los juristas internacionales han condicionado la legitimidad de la "preempción" en la existencia de una amenaza inmediata, este concepto de

[58] Ortega Carcelén, Martín, *La legítima defensa del territorio del Estado. Requisitos para su ejercicio*, Madrid, Tecnos, 1991.

[59] Remiro Brotóns*, op. cit., supra* (nota 9), pp. 1067.

[60] Gill y Ducheine, *op cit., supra* (nota 51), pp. 453.

[61] Díez de Velasco, *op. cit. Supra* (nota 31), p. 1075.

[62] Remiro Brotóns*, op. cit., supra* (nota 9), pp. 1068.

[63] La Casa Blanca, *The National Security Strategy of the United States*, Estados Unidos de América, Washington D. C., 2002, p. 15.

[64] *Ibíd.*, p. 6.

amenaza inmediata debe ser adaptado a los enemigos de hoy, los "Estados canallas" y los terroristas, que no utilizan medios convencionales de ataque, sino actos de terror y potencialmente armas de destrucción masiva fáciles de ocultar, entregar de forma encubierta y usar sin previo aviso[65].

De este modo, puede considerarse que "las amenazas inminentes están plenamente previstas en el artículo 51", como afirmó el antiguo Secretario General de Naciones Unidas Kofi Annan, no así las "latentes", en cuyo caso "la Carta concede plena autoridad al Consejo de Seguridad para hacer uso de la fuerza militar incluso de forma preventiva, para preservar la paz y la seguridad internacionales"[66].

A mayor abundamiento, incluso puede argumentarse que la anticipación está exigida por los principios de necesidad y proporcionalidad, formando por consiguiente parte de la esencia misma del derecho a la legítima defensa[67] y gozando como aquellos requisitos de una al menos bicentenaria *opinio iuris* inferida de la ya citada carta de Daniel Webster. En cualquier caso, ningún tribunal internacional, como tampoco el Consejo de Seguridad ni la Asamblea General de las Naciones Unidas, que evitó pronunciarse al respecto en su "Definición de la agresión"[68], han propugnado una lectura estricta del artículo 51 de la CNU excluyente de los preparativos claros y manifiestos de un ataque armado, ni siquiera de la intención inequívoca de atacar en un futuro próximo.

Ante la falta de consenso universal en torno a esta cuestión controvertida, se han propuesto diversos paradigmas doctrinales para acomodar la legítima defensa anticipatoria en el marco jurídico convencional y consuetudinario del uso de la fuerza. Quizá el enfoque que goza de mayor aceptación, al menos en el ámbito de la OTAN, es la tesis denominada de la "última ventana factible de oportunidad"[69], en virtud de la cual, mientras que el requisito inmediatez hace

[65] *Ibíd.*, p. 15.

[66] Secretario General de las Naciones Unidas, *Informe sobre un concepto más amplio de libertad*, Organización de las Naciones Unidas, Nueva York, 2005, Parte III, apartado E, párrafos 124-125.

[67] Gill y Ducheine, *op cit., supra* (nota 51), pp. 453.

[68] Asamblea General de las Naciones Unidas*, op. cit., supra* (nota 19).

[69] Schmitt (coord.), *op. cit., supra* (nota 3), pp. 59 y 60, reglas 14 y 15.

referencia a la proximidad temporal entre la agresión y la respuesta, la condición de inminencia puede cumplirse en cualquier momento temporal en el que haya indicios razonables para considerar que de no adoptar acción defensiva alguna la víctima prospectiva se colocaría en una posición de incapacidad para evitar el ataque inequívocamente inminente. Esta línea de argumentación excluye la licitud del uso preventivo de la fuerza justificado por la mera capacidad o intención de conducir un ataque armado en tanto la convergencia entre estos elementos objetivo y subjetivo no cristalice en una unívoca determinación de atacar.

Una teoría alternativa propone el análisis caso por caso de la "capacidad de asestar el primer golpe"[70] atribuida al potencial agresor en comparación a la víctima prospectiva siempre que exista una clara evidencia de un ataque próximo, planeado y decisivo. Esta construcción se basa en la suposición de que los Estados están dispuestos a aceptar una fuerte evidencia de la inminencia un ataque abrumador como equivalente al ataque en sí mismo, permitiendo a un Estado demostrablemente amenazado responder sobre la base del artículo 51 como si el ataque ya hubiera ocurrido[71].

Un interesante corolario de las grandes tendencias coexistentes en la literatura sobre legítima defensa anticipatoria es el ofrecido por Sean Murphy (2005, pp. 727–731), profesor de Derecho Internacional de la Universidad George Washington. En primer lugar, una interpretación restrictiva del artículo 51 es propugnada por los "construccionistas estrictos"[72], partidarios de condicionar el ejercicio del derecho a la legítima defensa a la efectiva ocurrencia del ataque armado y contrarios a la inferencia de ninguna costumbre contraria a aquel precepto a partir de la escasa práctica de los Estados en este

[70] Franck, Thomas, "When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?", *Washington Journal of Law and Policy*, volumen 5, 2001, pp. 51 y ss.

[71] Franck, Thomas, *Recourse to Force: State Action Against Threats and Armed Attacks*, Cambridge, Hersch Lauterpatch Memorial Lectures, 2002, p. 107.

[72] Véase Jessup, Philip, *A Modern Law of Nations*, North Haven, Archon Books, 1968, o Dinstein, *op. cit., supra* (nota 12), p. 167.

sentido[73]. Más flexible es la tesis del "ataque inminente", según la cual no puede ser concedido ni limitado convencionalmente un derecho que es inherente y que, en su regulación consuetudinaria ya formulada por la carta Webster un siglo antes de la Conferencia de San Francisco y confirmada por la práctica estatal subsiguiente a la Carta[74], tiene como presupuesto la inminencia. Un tercer grupo de autores postula una interpretación cualitativa del concepto de ataque armado, extendiéndolo a aquellas amenazas cualificadas en términos de probabilidad e intensidad del ataque prospectivo y de gravedad virtual del daño consiguiente[75]. Por último, hay que mencionar una corriente radicalmente crítica hacia el significado jurídico del régimen del uso de la fuerza establecido en la Carta, el cual consideran derogado *de facto* por la práctica estatal divergente[76], de manera que las decisiones políticas de los Estados desvinculadas de la *lex lata* han instaurado un nuevo marco fáctico dentro del cual tiene cabida la legítima defensa anticipatoria, e incluso preventiva, contra Estados o actores no estatales con notoria "capacidad y voluntad de [...] lanzar un ataque sorpresa" que comprometa la seguridad nacional[77].

Como conclusión puede afirmarse que, aunque no existe consenso en torno al momento temporal en el que surge el derecho a la legítima defensa en respuesta a un ataque armado, sí lo hay en torno a la posibilidad de ejercerlo de forma anticipatoria, ya que incluso los que se oponen a la doctrina "preemptiva" admiten que dicho ejercicio es permisible una vez que el ataque

[73] Véase *ibíd.*, p. 167, donde, no obstante, se admite la licitud de un ataque defensivo sobre un Estado que ha puesto en marcha un ataque armado de forma ostensiblemente irrevocable, aunque sus tropas no hayan cruzado aún la frontera.

[74] Véase el desembarco estadounidense en Bahía de Cochinos en 1961, la *Guerra de los seis días* entre Egipto e Israel de 1967, el ataque israelí contra una instalación nuclear iraquí en 1981 o el bombardeo estadounidense sobre Libia de 1987.

[75] Sofaer, Abraham, "On the Necessity of Preemption", *European Journal of International Law*, volumen 14, 2003, pp. 209 y ss., pp. 219-220.

[76] Glennon, Michael, "Preempting Terrorism: The Case for Anticipatory Self-Defense", *The Weekly Standard*, 28 de enero, 2002, pp. 24 y ss., p. 27.

[77] Congreso de los Estados Unidos, *Joint Resolution number 114 Authorizing the Use of Force Against Iraq, publication 107-243, 16 October 2002*, Estados Unidos de América, Washington D. C., 2002, pp. 1498-1499.

ha sido lanzado y antes de que se materialice[78]. En el siguiente epígrafe se analizan las concepciones predominantes en Europa en relación con el ejercicio de la legítima defensa, así como la posición de UE y OTAN en el debate sobre su posible carácter anticipatorio.

[78] Simma, Bruno, *The Charter of the United Nations: A Commentary*, Oxford, Oxford University Press, 2013, pp. 675-676.

4 LEGÍTIMA DEFENSA COLECTIVA EN EUROPA:

El ejercicio de la legítima defensa colectiva está sujeto a idénticos condicionantes que la legítima defensa individual[79], a saber, ataque armado previo, proporcionalidad, necesidad, inmediatez y el igualmente controvertido de inminencia. No obstante, se trata, más que de una aplicación del *ius ad bellum* a un conjunto de Estado, de su aplicación a la defensa de otro Estado[80], en la medida en que no responde al mero interés particular, sino al general en la paz y la seguridad internacionales[81]. Esta dimensión global constituye la justificación del ya mencionado ensamblaje de los "acuerdos regionales" en el sistema de seguridad colectivo de la Carta a través del Capítulo VIII de la misma. También se ha hecho referencia a la posibilidad de ejercer la legítima defensa colectiva de forma espontánea mediando el consentimiento del Estado víctima en la asistencia, normalmente de forma expresa[82], y la comunicación al Consejo de Seguridad de forma separada por parte de cada uno de los Estados asistentes[83], con arreglo al artículo 51 de la CNU.

En lo que respecta a los tratados bilaterales o multilaterales por los que se constituyen dichas alianzas defensivas, su razón de ser es incorporar al derecho a la legítima defensa colectiva una dimensión de deber de asistencia mutua [84], a la vez que produce un efecto político en las relaciones internacionales de advertencia a amigos y enemigos acerca de la voluntad aliada de intervenir en caso de cumplirse la *casus foederis* o supuesto de hecho en el que se activa el mecanismo de solidaridad previsto[85]. Por su parte,

[79] Dinstein, *op. cit., supra* (nota 12), pp. 237–240.

[80] Skubiszewski, Krzysztof, "Use of Force by States, Collective Security, Law of War and Neutrality", en Sørensen, Maximilian (ed.), *Manual of Public International Law*, Londres, Macmillan, 1968, pp. 745 y ss., p. 769.

[81] Alexandrov, Stanimir, *Self-Defence Against the Use of Force in International Law*, Leiden, Martinus Nijhoff Publishers,1996, p. 102.

[82] Corte Internacional de Justicia*, op. cit., supra* (nota 1), párrafo 232.

[83] Dinstein, *op. cit., supra* (nota 12), p. 240.

[84] Reichard, Martin, *The EU-NATO Relationship: A Legal and Political Perspective*, Hampshire, Ashgate Publishing Limited, 2006, p. 179.

[85] Dinstein, *op. cit., supra* (nota 12), p. 228.

las alianzas como la OTAN surgen de la voluntad de las partes en un tratado de asistencia mutua de ir más lejos de las obligaciones impuestas por el mismo[86], incorporando un mando militar integrado y una estructura organizativa y creando por este cauce una "socialización" entre los aliados de la que es difícil desvincularse en caso de decidirse la intervención[87].

4.1 MARCO DE LA LEGÍTIMA DEFENSA COLECTIVA DE LA OTAN:

El artículo 5 es el precepto nuclear del TAN en la medida en que contiene la cláusula de defensa mutua que fundamenta la propia existencia de la Alianza. Su origen histórico se encuentra en la situación de vulnerabilidad a la que se enfrentaron las potencias occidentales tras la Segunda Guerra Mundial como consecuencia de la presencia de tropas soviéticas en el Este de Europa y el miedo al triunfo del modelo socialista en las débiles economías de posguerra[88]. En este contexto, los Estados de Europa occidental se esforzaron por atraer el apoyo estadounidense para la recuperación económica y política[89], esfuerzo que se vio correspondido por la voluntad de Washington de reforzar los vínculos trasatlánticos acuciado por el mismo miedo al avance ruso.

De este modo, siguiendo el consejo del Secretario de Estado Marshall de crear en primera instancia una asociación de protección netamente europea como paso previo para solicitar el apoyo estadounidense[90], Reino Unido, Francia y Benelux fundaron la UEO incluyendo en el artículo 4 del Tratado de Bruselas, de 17 de marzo de 1948, sobre colaboración económica, social y cultural y legítima defensa colectiva una cláusula de defensa mutua. Desde un punto de vista político, ello supuso un marco para una alianza más amplia de carácter trasatlántico[91]. No obstante, el compromiso consignado en artículo 5

[86] Reichard, Martin, *The EU-NATO Relationship*..., *op. cit., supra* (nota 84), p. 179.

[87] *Ibíd.*, p. 180.

[88] *Ibíd.*, p. 180.

[89] *Ibíd.*, p. 180.

[90] Kay, Sean, *NATO and the Future of European Security. Europe Today*, Washinton D. C., Rowman and Littlefield, 1998, p. 16.

[91] *Ibíd.*, p. 17.

del TAN[92] se formuló en términos no tan estrictos como en el caso del artículo 4 del Tratado de Bruselas, de manera que, en lugar de afirmarse el compromiso de las partes de prestar a la parte atacada toda la ayuda militar y de otro tipo en asistencia de su poder de acuerdo con el artículo 51 de la CNU, se limitó a establecer la obligación de ayudar "a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad".

De este modo, el artículo 5 no contiene una obligación automática de prestar asistencia a la parte víctima del ataque o de asistir por medios militares, decisión que se deja a la voluntad de cada Estado[93]. Este principio de libertad de medios, avalado por la práctica estatal, no se opone al deber de llevar a cabo de buena fe un juicio imparcial y objetivo acerca de la necesidad de prestar una asistencia de naturaleza militar que se deriva de la letra y el espíritu de aquel precepto[94]. En cualquier caso, es una decisión que requiere el acuerdo de las otras partes, las cuales, se sitúan en un pie de igualdad jurídica al respecto, obviamente no tienen el mismo peso político, de manera que Estados Unidos ostenta una posición preeminente derivada de su mayor aportación de medios militares[95].

[92] Dicho artículo establece que "las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales".

[93] Ismay, Hastings, *NATO: the first five years, 1949-1954*, Utrecht, Bosch, 1954, p. 13.

[94] Reichard, *op. cit., supra* (nota 84), pp. 183-184.

[95] Ipsen, Knut, *Rechtsgrundlagen und Institutionalisierung der atlantisch-westeuropäischen Verteidigung*, Hamburg, Hansischer Gildenverlag Heitmann, 1967, p. 50.

En lo que respecta a las demás disposiciones del Tratado que complementan al artículo 5, es destacable que el ámbito del ejercicio de la legítima defensa colectiva en el marco de la OTAN trasciende el paradigma territorial atribuido a la misma en la CNU[96]. A este respecto, a los ataques contra el territorio de los Estados miembros definido en el apartado 1 del artículo 6 como elemento geográfico del *casus foederis*, el apartado 2 añade los ataques contra

> "las fuerzas, buques o aeronaves de cualquiera de las Partes que se hallen en estos territorios, así como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer".

Esta ampliación de la noción de ataque armado se ha traslado en opinión de algunos autores al plano consuetudinario[97], como indica el reflejo de la misma por analogía en el artículo 3.d) de la ya aludida "Definición de la Agresión".

Asimismo relevante es el artículo 9 del TAN, que posibilita, sin establecer una obligación jurídica al respecto más allá de la creación de un Comité de Defensa, el establecimiento de una estructura organizacional provista de un mando militar integrado a partir del Consejo del Atlántico Norte (en adelante CAN), único órgano originario de la OTAN y por decisión del cual se instituyen todos los demás de carácter subsidiario que integran la Alianza[98].

[96] Reichard, *op. cit., supra* (nota 84), p. 185.

[97] Fernández Tomás, Antonio, "El recurso al artículo quinto del Tratado de Washington tras los acontecimientos del 11 de septiembre: mucho ruido y pocas nueces", *Revista Española de Derecho Internacional*, volumen 53, 2001, pp. 205-226, pp. 207-208.

[98] Las Partes establecen, por la presente disposición, un Consejo en el que cada una de ellas estará representada para examinar las cuestiones relativas a la aplicación de este Tratado. El Consejo estará organizado de manera que pueda reunirse rápidamente en cualquier otro momento. El Consejo establecerá cuantos órganos subsidiarios puedan ser necesarios y en particular establecerá inmediatamente un Comité de Defensa que propondrá las medidas apropiadas para la puesta en práctica de los artículos 3 y 5.

Finalmente, se plantea la cuestión teórica de la posibilidad de invocar el artículo 5 contra otro Estado miembro de la Alianza, aunque la situación en la que un aliado ataque a otro es remotamente posible en la práctica[99]. A pesar de que nada en el mencionado precepto parece impedirlo desde un punto de vista literal, la posición sistemática del artículo 51 de la CNU fuera del Capítulo VIII relativo a los acuerdos regionales y la fundamental distinción entre defensa colectiva y seguridad colectiva hacen inviable tal lectura[100]. Además, la declaración de Petersberg de 1992 por los diez Estados miembros de la UEO sostiene que

> "las garantías de seguridad y los compromisos de defensa contenidos en los Tratados que vinculan los estados miembros en el seno de la Unión Europea Occidental, y que los vinculan en el seno de la Alianza Atlántica, se refuerzan mutuamente y no pueden ser invocados, por aquéllos que suscriban la parte III de la Declaración de Petersberg, en las controversias que se produzcan entre los estados miembros de una u otra de las dos organizaciones"[101].

4.2 MARCO DE LA LEGÍTIMA DEFENSA COLECTIVA EN LA UE:

Para comprender el marco jurídico de la legítima defensa en la Unión Europea es preciso introducir el concepto de "poder civil" o "blando" -*soft power*-, que será objeto de discusión en la segunda parte, puesto que el deseo de los países europeos en general por distinguirse del tradicional comportamiento estatal en las relaciones internacionales, particularmente su reticencia imponer por medios coercitivos sus prioridades e intereses, forma parte de su genuina identidad[102]. No obstante, la mencionada introducción de las cláusulas de solidaridad de los artículos 42.7 del TUE y 222 del TFUE, en

[99] Reichard, *op. cit., supra* (nota 84), p. 186.

[100] *Ibíd.*, p. 186.

[101] Consejo de Ministros de la Unión Europea Occidental, *Pertersberg Declaration of 19 June 1992*, Unión Europea Occidental, Bonn, 1992, sección III, párrafo A.

[102] Patomäki, Heikki, "Cultivating the Mood of <<Grieving Delight>> The Moral Lessons of the Study of Narratives and Methaphors in the 1990-1991 Gulf War", *Paper by the second EuPRA Conference of 12-14 November 1993*, Budapest, 1993, p. 14.

línea con la remodelación de la Política Exterior y de Seguridad Común (en adelante PESC), trata de reflejar el equilibrio entre los Estados miembros y capacitar a la vez a la UE en su conjunto para promover y proteger mejor los intereses y valores europeos a nivel global[103].

La idea de una defensa común netamente europea al margen de la OTAN ha estado latente desde los años ochenta y patente en la pos-Guerra Fría. En efecto, la misma se abrió paso en las negociaciones del Tratado de Maastricht de 1991, con el apoyo franco-alemán, y se materializó en la introducción en el artículo J.4 del antiguo TUE de una dimensión militar hasta entonces inédita en las Comunidades[104]. En los años sucesivos, aumentó la conciencia acerca de la inevitable necesidad estratégica de abordar la legítima defensa colectiva europea desde las estructuras comunitarias[105] para la defensa de los intereses esenciales y vitales comunes a sus Estados miembros[106]. Aunque el potencial de las Comunidades en términos de la cohesión necesaria para articular una defensa colectiva era mayor que el de la OTAN, la capacidad militar europea era insuficiente para sostener una infraestructura militar independiente, de manera que se preservó el consenso acerca de mantener la defensa territorial del viejo continente al margen del marco comunitario[107].

El panorama continuó inmutable tras la reforma de Ámsterdam en 1997, a pesar de los esfuerzos de un grupo de Estados miembros dirigidos por Francia y Alemania hacia la integración completa de la UEO en la UE con el fin de hacer a esta última responsable de todos los aspectos relativos a la seguridad

[103] Comisión Europea, *Documento de 10 de julio de 2007 sobre la reforma de Europa para el siglo XXI* [COM (2007) 412 final], Comunidades Europeas, Bruselas, 2007.

[104] Reichard, *op. cit., supra* (nota 84), p. 192.

[105] Nerlich, Uwe, "The relationship between a European common defence and NATO, the OSCE and the United Nations", Martin, Lawrence y Roper, John (eds.), *Towards a common defence policy*, París, Instituto de Estudios Estratégicos de la Unión Europea Occidental, 1995, pp. 69-97, p. 82.

[106] D'Oléon, Michel y Jopp, Mathias, "The way ahead for European defence cooperation", en Martin, Lawrence y Roper, J. (eds.), *Towards a common defence policy*, París, Instituto de Estudios Estratégicos de la Unión Europea Occidental, 1995, pp. 98 y ss., pp. 103.

[107] Menon, Anand, "Defence policy and integration in Western Europe", *Contemporary Security Policy*, volumen 17, número 2, 1996, pp. 264 y ss., p. 273.

y la defensa comunes[108]. El final de siglo fue testigo de cómo la preocupación por establecer una capacidad de gestión de crisis para hacer frente a situaciones como la de los Balcanes arrebató a la defensa colectiva su estatus de prioridad[109], sin hacerla desaparecer del programa político de la UE, como prueba la resolución del Parlamento Europeo en la que señala que,

> "en virtud de los artículos 51 y 52 de la Carta de las Naciones Unidas, una organización como la Unión Europea tiene derecho a la legítima defensa y a la defensa colectiva y que, sobre esta base, la Unión Europea está capacitada para establecer progresivamente una política de defensa común"[110].

Tampoco el Tratado de Niza supuso un progreso significativo en materia de defensa[111], ámbito que fue abordado de nuevo durante los trabajos de la Convención para la redacción de la *non nata* Constitución para Europa. En el contexto de las negociaciones de este texto el "Informe Barnier"[112] propuso la introducción de un compromiso acerca de la legítima defensa colectiva en los Tratados o en un Protocolo anexo posiblemente a través de una cláusula de *opting-in* que permitiera adherirse a aquellos Estados miembros que lo desearan o tuvieran las capacidades necesarias[113], una a modo de "Eurozona para la Defensa"[114]. La acogida de esta propuesta por las Instituciones fue buena[115].

---

[108] Reichard, *op. cit., supra* (nota 84), p. 193.

[109] Consejo de la Unión Europea, *German Presidency Paper of 24 February 1999: Informal Reflection at WEU on Europe's Security and Defence*, Unión Europea, Bonn, 1999, sección II.1, párrafo 2.

[110] Parlamento Europeo, *Resolution of the European Parliament of 14 May 1998 on the gradual establishment of a common defence policy for the European Union* [A4–0171/98], Comunidades Europeas, Estrasburgo, 1998, párrafo 5.

[111] Reichard, *op. cit., supra* (nota 84), p. 196.

[112] Barnier, Michel, *WEU Assembly Press Release 3/2003 of 12 February 2003: Eurozone for Defence*, Asamblea Parlamentaria de la Unión Europea Occidental, París, 2003.

[113] Reichard, *op. cit., supra* (nota 84), p. 199.

[114] Barnier, *op. cit., supra* (nota 112).

[115] Reichard, *op. cit., supra* (nota 84), p. 200.

Pero la gran remodelación de la fachada exterior de la Unión Europea no se acomete hasta el Tratado de Lisboa, que como en otros ámbitos rescata los avances introducidos por la fallida tentativa constituyente. En efecto, en un esfuerzo de ganar visibilidad en el plano internacional, el nuevo marco jurídico de la Política Exterior y de Seguridad Común (en adelante PESC), cuyo análisis será abordado en mayor detalle más adelante. Baste ahora referir que las modificaciones no se restringen al establecimiento de una diplomacia más eficiente encauzada a través de la figura del Alto Representante de la Unión para Asuntos Exteriores y de Política de Seguridad y del Servicio Europeo de Acción Exterior (SEAE en adelante), sino que además se acomete una reforma de la antigua Política Europea de Seguridad y Defensa (en adelante PESD)[116]. De este modo, la ahora denominada Política Común de Seguridad y Defensa (en adelante PCSD), aunque se mantiene fiel al predominio de la gestión de crisis, introduce instrumentos para la consecución de una defensa común propia, potenciando así la credibilidad internacional UE [117].

Concretamente, se incorporan dos cláusulas interrelacionadas a través de la PESC y la PCSD que responden a la dimensión interna y externa indisolublemente unidas de la UE, la cláusula de solidaridad del artículo 222 del TFUE[118] y la cláusula de asistencia mutua o "cláusula atlantista" del artículo

[116] Martín y Pérez de Nanclares, José, "Seguridad y acción exterior de la Unión Europea: La creciente relevancia de la dimensión exterior del espacio de Libertad, Seguridad y Justicia", *Revista Electrónica del Instituto Español de Estudios Estratégicos*, número 0, 2012, pp. 135-154, p. 139.

[117] Rubio García, Dolores, "Las cláusulas de asistencia mutua y solidaridad introducidas por el Tratado de Lisboa: el refuerzo de la seguridad y la defensa en la Unión Europea", *Documento de trabajo 57/2011*, Observatorio de Política Exterior Española, Madrid, 2011, p. 23.

[118] "1. La Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano. La Unión movilizará todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros, para:

- prevenir la amenaza terrorista en el territorio de los Estados miembros;
- proteger a las instituciones democráticas y a la población civil de posibles ataques terroristas;
- prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de ataque terrorista;

42.7 del TUE [119] respectivamente, a través de las que se construye una solidaridad reforzada entre los Estados miembros [120]. Por su posición sistemática la cláusula de solidaridad se sitúa a medio camino entre las dimensiones externa e interna, en tanto se contiene en el TFUE y, por lo tanto, al margen de la regulación de la PESC, pero en la Parte VII relativa a la Acción Exterior. Su razón de ser es la de posibilitar una reacción colectiva ante las amenazas no tradicionales que, al desarrollarse en el interior de los Estados, escapan al ámbito de la legítima defensa, sobre todo el terrorismo internacional

-prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de catástrofe natural o de origen humano.

2. Si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano, a petición de sus autoridades políticas los demás Estados miembros le prestarán asistencia. Con este fin, los Estados miembros se coordinarán en el seno del Consejo.

3. Las modalidades de aplicación por la Unión de la presente cláusula de solidaridad serán definidas mediante decisión adoptada por el Consejo, a propuesta conjunta de la Comisión y del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Cuando dicha decisión tenga repercusiones en el ámbito de la defensa, el Consejo se pronunciará de conformidad con el apartado 1 del artículo 31 del Tratado de la Unión Europea. Se informará al Parlamento Europeo.

A efectos del presente apartado, y sin perjuicio del artículo 240, el Consejo estará asistido por el Comité Político y de Seguridad, con el apoyo de las estructuras creadas en el marco de la política común de seguridad y defensa, y por el comité contemplado en el artículo 71, que le presentarán, en su caso, dictámenes conjuntos.

4. Para asegurar la eficacia de la actuación de la Unión y de sus Estados miembros, el Consejo Europeo evaluará de forma periódica las amenazas a que se enfrenta la Unión".

[119] "Si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros.

Los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte, que seguirá siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta".

[120] Rubio García, *op. cit., supra* (nota 117), pp. 23-24.

que había azotado a España en 2004 y a Reino Unido en 2005. *A sensu contrario*, ello permite entender que la "cláusula atlantista" se activa por los actos de terrorismo de Estado[121], entendiendo por tales la infracción del

> "deber de abstenerse de organizar, instigar, ayudar o participar en actos de [...] terrorismo en otro Estado, o de consentir actividades organizadas dentro de su territorio encaminadas a la comisión de dichos actos, cuando los actos a que se hace referencia en el presente párrafo impliquen el recurrir a la amenaza o al uso de la fuerza"[122].

Esta arquitectura integradora o comprensiva de la seguridad colectiva -en el sentido de interna y externa, civil y militar y orientada tanto combatir las causas como a las amenazas en sí- deriva de la constatación de la indisolubilidad de las amenazas clásicas y nuevas, sobre todos desde los atentados de Madrid y Londres, y se ve complementada por la inclusión en el artículo 43.1 [123] de un inciso final en virtud del cual las "misiones de Petersberg"[124] "podrán contribuir a la lucha contra el terrorismo, entre otras cosas mediante el apoyo prestado a terceros países para combatirlo en su territorio". Ello permite abordar la lucha contra las nuevas amenazas también

[121] Calduch Cervera, Rafael, "El Tratado de Lisboa y la amenaza terrorista en Europa", en Martín y Pérez de Nanclares, José (coord.), *El Tratado de Lisboa. La salida de la crisis constitucional*, Madrid, Iustel, 2008, pp. 451-468, p. 459.

[122] Asamblea General de las Naciones Unidas, *op. cit., supra* (nota 10).

[123] "Las misiones contempladas en el apartado 1 del artículo 42, en las que la Unión podrá recurrir a medios civiles y militares, abarcarán las actuaciones conjuntas en materia de desarme, las misiones humanitarias y de rescate, las misiones de asesoramiento y asistencia en cuestiones militares, las misiones de prevención de conflictos y de mantenimiento de la paz, las misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz y las operaciones de estabilización al término de los conflictos. 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".

[124] Misiones de la Unión Europea en el exterior apoyadas en las capacidades civiles y militares proporcionadas por los Estados miembros con el objeto de garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la CNU.

desde una perspectiva militar, aunque siempre desde la óptica preponderante de la gestión de crisis.

Por otra parte, en lo que respecta a su naturaleza, la cláusula de asistencia mutua disfruta de una naturaleza plenamente intergubernamental, como se deduce de su localización en el Capítulo 2 del TUE dedicado a la PESC, ya que, a pesar de la formal desaparición de la estructura de pilares, la cesión de competencias soberanas no alcanza al ámbito de la seguridad y la defensa[125], debiendo adoptarse las decisiones del Consejo y del Consejo Europeo en dicho ámbito por unanimidad y quedando excluida del mismo la adopción de actos legislativos *ex* artículo 31.1 del TUE. En cambio, la cláusula de solidaridad tiene un carácter institucional orientado a permitir la acción de la Unión Europea complementaria en ámbitos que son propios de la competencia estatal[126].

Finalmente, es preciso aclarar que la invocación de la "cláusula atlantista" genera una obligación jurídica para los Estados miembros de carácter automático, dado que a diferencia del artículo 5 del TAN no requiere un acuerdo político previo para ponerse en marcha, así como más amplio que en el caso de la Alianza en términos geográficos -incluyendo los territorios no europeos de los Estados miembros- y materiales -abarcando medios civiles y militares-[127]. Algunas voces críticas incluso han puntualizado que

> "la obligación explícita a reaccionar en cualquier caso cuando se trate de una agresión armada contra un Estado miembro va más allá que la cláusula de asistencia mutua de la OTAN puesto que también se cubrirían los ataques no armados"[128].

Por su parte, la cláusula de solidaridad requiere una decisión del Consejo a propuesta de la Comisión y del Alto Representante subsiguiente a su

[125] Rubio García, *op. cit., supra* (nota 117), p. 39.

[126] *Ibíd.*, p. 41.

[127] *Ibíd.*, p. 54.

[128] Comisión de Asuntos Exteriores del Parlamento Europeo, *Informe de 31 de octubre de 2012 sobre las cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa* [2012/2223(INI)], Unión Europea, Estrasburgo, 2012, opinión minoritaria del Grupo GUE/NGL por Sabine Lösing y Willy Meyer.

invocación por el Estado víctima para activarse [129], pero es igualmente obligatoria para los Estados miembros, que deben actuar conjuntamente, excluyéndose las acciones unilaterales. Además, su ya señalada vocación comprensiva se manifiesta en el hecho de que se desarrolle en los planos de la prevención -propia del ámbito del Espacio de Libertad, Seguridad y Justicia y consiguientemente limitada al territorio de los Estados miembros y previa a la consumación de la amenaza-, la protección -propia del ámbito de la PESD y por ende sin límites territoriales, pero restringida subjetivamente a las instituciones democráticas y a la población civil, y también de carácter previo- y la asistencia -que opera a posteriori y mediante solicitud previa de las autoridades del Estado miembro víctima-[130]. Esta dimensión extraterritorial de la solidaridad europea es la que conduce a la Comisión de Asuntos Exteriores del Parlamento Europeo a señalar "que la cláusula de solidaridad podría cubrir también incidentes graves que se produzcan fuera de la Unión y tengan un impacto directo e importante en un Estado miembro"[131].

4.3 INTERACCIÓN ENTRE AMBOS MARCOS JURÍDICOS:

Las siguientes palabras de Pérez de Nanclares (2012, p. 137) resumen los epígrafes anteriores e introducen el presente con gran elocuencia de la siguiente forma:

> "la articulación de la seguridad colectiva en Europa se ha hecho sobre todo en torno a la Alianza Atlántica (OTAN) y, en mucha menor medida, a la Unión Europea Occidental (UEO); de hecho, en el ADN de la UEO ha estado, desde su mismo origen en octubre de 1954 hasta su defunción por inanición en 2010, la renuncia a disponer de una estructura militar propia, quedando ésta bajo el paraguas de la OTAN".

[129] Unión Europea, *Versión consolidada del Tratado de Funcionamiento de la Unión Europea* [2010/C 83/01], Lisboa, 2007, Artículo 222.3 del TFUE.

[130] Rubio García, *op. cit., supra* (nota 117), pp. 44-45.

[131] Comisión de Asuntos Exteriores del Parlamento Europeo, *op. cit., supra* (nota 128), párrafo 20.

Sin ánimo de entrar a analizar en profundidad las relaciones entre ambas organizaciones internacionales europeas, que será el objeto de la segunda parte, baste ahora con presentar la articulación entre ambos marcos jurídicos reguladores del ejercicio de la legítima defensa colectiva. En este sentido, si la inclusión de las cláusulas de asistencia mutua y solidaridad responde en gran medida al intento de lograr un mayor equilibrio en las relaciones transatlánticas, el encaje entre aquéllas y el artículo 5 del TAN es crucial para no deteriorar estas relaciones, que constituyen uno de los elementos centrales del sistema internacional [132]. Ello implica en suma transitar de la dependencia a la complementariedad en la asociación entre UE y OTAN sin debilitarla, dotándose aquélla de instrumentos que permitan una respuesta genuinamente europea, pero sin prescindir de la misma, entre otras razones porque la asunción de un papel más relevante en la seguridad internacional requiere de capacidades militares que permitan una respuesta rápida y ello impide preservar las relaciones bilaterales, especialmente con Estados Unidos[133].

Aunque como ya se ha afirmado, el ámbito de la cláusula atlantista de la UE es mayor que el de su homóloga de la Alianza en términos geográficos y materiales y a diferencia de ésta opera *ipso iure*, la obligación jurídica que impone a los socios comunitarios en ante todo compatible con sus

> "compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte, que seguirá siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta"[134].

[132] Consejo de la Unión Europea, *Estrategia Europea de Seguridad de 12 de diciembre de 2003: Una Europa más segura en un mundo mejor*, Unión Europea, Bruselas, 2003 [disponible en http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf, último acceso el 26 de junio de 2014], p. 9.

[133] Rubio García, *op. cit*., *supra* (nota 117), p. 54.

[134] Artículo 42.7 del TUE.

En consecuencia, el Tratado de Lisboa apuesta claramente por posibilitar la cooperación y el reparto de misiones entre ambas organizaciones[135], como no puede ser de otra manera en un ámbito de competencias como la política de seguridad y defensa propio de la esfera de la soberanía estatal y cuyo carácter específico en cada Estado miembro debe ser respetado por la PESC[136], siendo significativa la mención expresa de la compatibilidad entre las PCSD y la "política común de seguridad y defensa establecida en dicho marco [el de la OTAN]"[137]. Se trata por lo tanto de encontrar un equilibrio entre, por un parte, el hecho de

> "que la gran mayoría de los Estados miembros de la UE son miembros de la OTAN y que, en consecuencia, la política común de seguridad y defensa debe ser compatible y coherente con los compromisos en el seno de la OTAN y respetar al mismo tiempo la autonomía de la UE",

de manera que "la cláusula de asistencia mutua de la UE no debería activarse nunca sin haber consultado a la OTAN y buscado su participación"; y, por otra parte, "el carácter específico de las políticas de seguridad y defensa de aquellos Estados de la UE que no son miembros de la OTAN"[138].

En cualquier caso, la compatibilidad práctica entre ambos marcos jurídicos de la legítima defensa europea parece asegurada si se considera que ambos comparten la filosofía subyacente del carácter integrado de la seguridad y la defensa, siendo manifiestas "las complementariedades existentes entre los objetivos de la OTAN y los contemplados en el artículo 43 del Tratado UE"[139], y

[135] Yaniz Velasco, Federico, "La Alianza Atlántica y la Unión Europea. La evolución de unas relaciones complejas", *Documento marco 09/2013*, Instituto Español de Estudios Estratégicos, Madrid, 2013, p. 7.

[136] Unión Europea, *op. cit, supra* (nota 36), Artículo 42.2 del TUE.

[137] *Ibíd.*, Artículo 42.2 del TUE.

[138] Comisión de Asuntos Constitucionales del Parlamento Europeo, *Opinión de 10 de octubre de 2012 para la Comisión de Asuntos Exteriores sobre las cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa*, Unión Europea, Bruselas, 2012, párrafo 9.

[139] Comisión de Asuntos Exteriores del Parlamento Europeo, *op. cit., supra* (nota 128), párrafo 4.

que, además, si bien yendo un paso más allá en esta enfoque comprensivo, las cláusulas de asistencia mutua y solidaridad en realidad tratan de

> "emular el planteamiento de la OTAN, que tiene presente las circunstancias inevitables en las que se requiere prevenir las amenazas externas para promover los intereses en materia de seguridad de los aliados y se necesita la proyección de fuerza"[140].

[140] *Ibíd.*, párrafo 5.

5 USO DE LA FUERZA, LEGÍTIMA DEFENSA COLECTIVA Y CIBERATAQUES:

Varios acontecimientos producidos en los últimos siete años, de mayor impacto mediático que jurídico, han llevado el concepto jurídico indeterminado "ciberataque" o "ataque cibernético"[141] a los titulares de los periódicos, las estrategias de seguridad nacionales y las agendas de los foros internacionales de más alto nivel, incluyendo la UE y la OTAN. Sin embargo, parece existir una cierta reluctancia a establecer el alcance de este término, como evidenció la negativa de la Alianza Atlántica a emitir una declaración oficial tras la serie de ataques digitales contra Estonia que causaron daños estimados en decenas de millones de euros, quizá por la reticencia general de los Estados a considerar los actos indirectos de agresión como ataques armados[142].

En este subapartado se trata de ofrecer una panorámica de las particularidades que presenta la aplicación del marco jurídico internacional de la amenaza y el uso de la fuerza[143], descrito en el primer subapartado, a las "operaciones cibernéticas"[144], partiendo de la premisa de que dicho marco es

[141] Ver Agencia de Normalización de la Organización del Tratado del Atlántico Norte, "Glosario de la OTAN de términos y definiciones", *Documento AAP-6(2012)(2)*, Organización del Tratado del Atlántico Norte, Bruselas, 2012, que evita pronunciarse sobre el significado el término "ciberataque" o "ataque cibernético", pero en cambio sí define lo que califica como un tipo de "ciberataque", el "ataque a redes informáticas" -*Computer network attack* o *attaque de réseaux informatiques* en las lenguas oficiales de la Alianza-, como la "acción tomada para interrumpir, denegar, degradar o destruir información residente en un ordenador y/o red de ordenadores, o el propio ordenador y/o la red de ordenadores", aclarando a continuación que se trata de, pero sin definir este término.

[142] Harrison Dinniss, Heather, *Cyber Warfare and the Laws of War*, Cambridge, Cambridge University Press, 2012, p. 39.

[143] A partir de ahora, salvo que se diga lo contrario, lo afirmado respecto del uso de la fuerza se considera aplicable *mutatis mutandi* a la amenaza de la fuerza, en tanto aquél es el resultado virtual de la consumación ésta.

[144] El término "operaciones cibernéticas" es definido en la Directiva Política del Presidente de los Estados Unidos (2012, p. 3) de 16 de octubre de 2012 como las "operaciones y programas o actividades relativos -distintos de la defensa de las redes y la recolección de datos- […] en o a través del ciberespacio, que tienen por objetivo permitir o producir efectos cibernéticos, es

único y aplicable a cualquier uso de la fuerza con independencia del arma empleada[145], incluidas las virtuales, ante la ausencia de argumentos jurídicos o prácticos que fundamenten lo contrario[146]. A tal efecto, una vez abordada la caracterización general de este tipo de operaciones, es preciso determinar bajo qué circunstancias puede considerarse que un "ataque a redes informáticas"[147] constituye un uso de la fuerza prohibido por el artículo 2.4 de la CNU. El segundo paso lógico es establecer en qué casos una ofensiva conducida a través del denominado "quinto dominio", por sí sola o como complemento de la fuerza física, se reputa ataque armado y, por consiguiente, justifica el ejercicio del derecho a la legítima defensa individual y colectiva.

Por supuesto, ha de tenerse presente que cualesquiera otras actividades que se desarrollen en el ámbito interno de los Estados o incluso en el ámbito internacional contraviniendo los ordenamientos jurídicos nacionales u otras normas internacionales distintas a aquéllas que regulan el recurso a la fuerza, tales como el espionaje industrial, el tráfico de datos de carácter protegido o los delitos cometidos a través de Internet, sobrepasan el objeto de este trabajo, esto es, el análisis de la aplicación del *ius ad bellum* en el nuevo campo de batalla que es el ciberespacio, entendido como un "un escenario estratégico, operacional y táctico"[148].

decir, la manipulación, interrupción, paralización o destrucción de ordenadores, sistemas de información o comunicación, redes, infraestructuras físicas controladas por ordenadores o sistemas de información o información residente en los mismos". Dado su parecido con la definición de "a redes informáticas" que ofrece Glosario de la OTAN (Agencia de Normalización de la Organización del Tratado del Atlántico Norte, *op. cit., supra* (nota 141), 2012 y entendiendo que ninguno de los dos prejuzga el carácter de uso de la fuerza o ataque armado, se emplean como sinónimos a los efectos de este trabajo.

[145] Corte Internacional de Justicia, *op. cit.,supra* (nota 32), párrafo 39.

[146] Gill y Ducheine, *op. cit., supra* (nota 51), p. 439.

[147] Agencia de Normalización de la Organización del Tratado del Atlántico Norte, *op. cit., supra* (nota 141).

[148] Centro Superior de Estudios de la Defensa Nacional, "Guerra cibernética: Aspectos organizativos", *Documento del Grupo de Trabajo nº 3 del XXXIII Curso de Defensa Nacional*, Ministerio de Defensa, Reino de España, Madrid, 2013, p. 6.

5.1 CARACTERIZACIÓN GENERAL DE LOS CIBERATAQUES:

En ausencia de una definición jurídica internacional, tres rasgos definitorios parecen delimitar el concepto de ciberataque, su accesibilidad para cualquier actor, su opacidad en lo que respecta a la autoría y su carácter en principio no letal[149]. Efectivamente, las operaciones cibernéticas combinan anonimato, discreción y rapidez[150], lo que hace especialmente relevante y complejo delimitar claramente en Derecho internacional el umbral a partir del cual una acción coercitiva inesperada, inimputable y dañina en un sentido muy diferente al clásico debe considerarse como uso de la fuerza o ataque armado. Un elemento que viene a dificultar aun más esta calificación es su disponibilidad por parte de actores no estatales como organizaciones internacionales, activistas políticos, grupos terroristas, medios de comunicación o Estados no reconocidos, lo que convierte a Internet en una de las armas más habituales en los conflictos asimétricos[151].

Por ello, en la práctica, el rastreo del autor sólo puede realizarse en un plano indiciario que difícilmente permite fundamentar jurídicamente la imputación de responsabilidad. Por ejemplo, los ejercicios conjuntos organizados a gran escala, como el bautizado “Cyber Europe 2012”, efectuado por veintinueve Estados europeos para probar sus capacidad de reacción coordinada ante un ataque de denegación de servicios -*Distributed Denial of Services* o *DDoS*-, están más orientados a conseguir un nivel adecuado de preparación sobre la base de la representación que se obtiene del adversario y a construir una imagen de la amenaza a partir de las debilidades identificadas[152].

En cualquier caso, si se venciera la práctica imposibilidad de establecer con certeza el origen geográfico del ataque, ello no bastaría para imputar al

[149] Baudin, Laura, *Les cyber-attaques dans les conflits armées. Qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire*, París, L’Harmattan, 2014, p. 33.

[150] Baudin, *op. cit., supra* (nota 149), p. 34.

[151] Baudin, *op. cit., supra* (nota 149), p. 35.

[152] Ventre, Daniel, *Ciberattaque et cyberdéfense*, París, Lavoisier, 2011, p. 114.

estado en cuestión la responsabilidad internacional[153], en tanto no se puede probar incontestablemente la implicación de un Estado en un acto de espionaje o de guerra cibernética, sobre todo en la medida en que las autoridades estatales suelen recurrir a *hackers* conocedores de las técnicas más sofisticadas de camuflaje tales como las bombas lógicas, imperceptibles pero provocadoras de un grave efecto dominó una vez detonadas [154] . Adicionalmente, los Estados se muestran reticentes a emitir acusaciones que pudieran ser infundadas por sus efectos nocivos en el plano diplomático al menos hasta que se desarrollen sistemas que permitan rastrear con precisión el origen de una operación cibernética[155].

En suma, aunque se están realizando progresos, como el arma cibernética desarrollada por Fujitsu bajo el mandato del Gobierno japonés para identificar la fuente del ataque de denegación de servicios y los autores del robo de datos [156] , en el futuro previsible las armas cibernéticas mantendrán las peculiaridades propias de la naturaleza intangible y omnipresente de la red, que las hacen tan efectivas como invisibles: (a) no necesitan un lugar particular de lanzamiento, (b) pueden ser creadas por cualquier persona en cualquier lugar con o sin una motivación particular, (c) dejan escaso margen a la anticipación, la prevención, la detección o la reacción y (d) utilizan generalmente una multitud de ordenadores repartidos en distintos países para aumentar su eficacia operativa y dificultar el rastreo[157].

Por otra parte, los ciberataques pueden adoptar una forma meramente operativa, constituyendo un simple complemento de la guerra convencional, o estratégica, suponiendo una forma autónoma de conducir las hostilidades

[153] Arpagian, Nicolas, "La cyberattaque, nouvelle arme de guerre des États", *www.franceinfo.fr*, 2013 [disponible en http://www.franceinfo.fr/high-tech/vie-quotidienne/article/la-cyberattaque-nouvelle-arme-de-guerre-des-etats-239231, último acceso el 22 de junio de 2014].

[154] Baudin, *op. cit., supra* (nota 149), p. 40.

[155] Baudin, *op. cit., supra* (nota 149), p. 40.

[156] Baud, Michel, "La cyberguerre n'aura pas lieu mais il faut s'y préparer", *Politique étrangère*, volumen 77, número 2, 2012, pp. 305-314.

[157] Bweless, Charles, "Peut-on dissuader dans le cyberespace? ", *Revue de la défense nationale*, número 731, 2010, pp. 25 a 30.

sustitutiva de la tradicional[158]. De este modo, a la vez que un tipo de coerción independiente en opinión de algunos autores susceptible de calificarse de uso de la fuerza o de ataque armado, también es evidente que constituye una nueva arma orientada a maximizar las posibilidades de éxito de los soldados y evitar eventuales víctimas en las filas de los ejércitos mediante la neutralización de los sistemas enemigos, retrasar o paralizar la actuación de su Estado mayor o influir o modificar sus percepciones de la situación[159]. Sin embargo, esta faceta de las operaciones cibernéticas como instrumento al servicio de conflictos armados ya iniciados debe ser abordada desde la óptica del Derecho Internacional Humanitario o *ius in bello* y, por lo tanto, sobrepasa el ámbito de este trabajo, limitado al tratamiento de los ciberataques autónomos o estratégicos en el plano del *ius ad bellum* contra las infraestructuras críticas y vitales de un Estado, que atentan de este modo contra el funcionamiento de la sociedad en su conjunto, que queda situada en una posición de inseguridad y vulnerabilidad[160].

Para concluir este epígrafe, se incluyen algunas definiciones relevantes extraídas de la Orden del ministerio de Defensa por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas[161]:

> "1. Ciberespacio: Dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información.
>
> 2. Ciberataque: Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

[158] Baudin, *op. cit., supra* (nota 149), p. 57.

[159] Baud, *op. cit, supra* (nota 156).

[160] Baudin, *op. cit., supra* (nota 149), pp. 51 y 52.

[161] Ministerio de Defensa del Reino de España, "Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas", *Boletín Oficial del Ministerio de Defensa*, número 40, pp. 4154-4156, Reino de España, Madrid, 2013, art. 2.

3. Ciberseguridad. Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

4. Ciberdefensa militar: Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control de las Fuerzas Armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos".

En definitiva, aunque ambas tienen por objeto la protección del ciberespacio frente a los ciberataques, la ciberdefensa es "el subconjunto más operativo de las capacidades de ciberseguridad, lo que parece lógico y coherente si pensamos que en el mundo físico la defensa es la parte más operativa de las capacidades que desarrollan las naciones para garantizar la Seguridad Nacional"[162]. En otras palabras, la ciberdefensa es la parte de la ciberseguridad que se desarrolla en el plano militar, en el cual rige un principio de libertad de acción que permite actuar sobre los sistemas de información adversarios[163] en determinadas circunstancias cuya evaluación a la luz del *ius ad bellum* es el propósito de los siguientes epígrafes.

5.2 USO CIBERNÉTICO DE LA FUERZA:

Si no existe un consenso internacional acerca de la definición precisa de las operaciones "cinéticas"[164] subsumibles dentro del concepto de uso de la

[162] Centro Superior de Estudios de la Defensa Nacional, *op. cit., supra* (nota 148), p. 18.

[163] *Ibíd.*, p. 18.

[164] Empleo aquí una traducción de la voz inglesa *kinetic warfare*, neologismo acuñado por el periodista de *The Washington Post* Robert Woodward y asumido por la jerga militar estadounidense en eufemística contraposición a los menos violentos y más tecnológicos medios de guerra englobados dentro del concepto *cyber warfare*, como afirma Noah, Timothy, "Birth of a Washington Word", *www.slate.com*, 2002 [disponible en

fuerza, con mayor razón no lo hay en el ciberespacio, de manera que corresponde a cada Estado establecer sus propios criterios para definir el umbral del uso de la fuerza[165] mediante una evaluación lo suficientemente razonable y necesariamente política. Sí parece existir acuerdo en considerar que la noción de fuerza prohibida tiene que ser armada, incluyendo no sólo las armas que lo son por naturaleza, sino también las armas que se consideran como tales por su uso previsible, es decir, aquéllas cuya función primordial no es armamentística, pero que pueden ser utilizadas o destinadas a ser utilizadas como armas en determinadas circunstancias[166]. Además, el uso de la fuerza está tradicionalmente asociado con las actividades militares, aunque estos conceptos no siempre van de la mano.

La mayor parte de los autores parece coincidir en que el parámetro básico para identificar un uso cibernético de la fuerza es su comparación cualitativa y cuantitativa con aquellas medidas coercitivas físicas que traspasan el umbral del artículo 2.4 CNU, dada la ausencia de un estándar específico aplicable a los ciberataques. En este sentido, la regla 11 del Manual de Talín establece que "una operación cibernética constituye un uso de fuerza cuando su escala y efectos[167] son comparables a los de operaciones no cibernéticas que alcanzan el nivel de uso de la fuerza"[168].

Este enfoque encuentra un fundamento en los trabajos preparatorios de la Carta, de los cuales se infiere la voluntad de establecer un criterio instrumental para determinar la legalidad de la coerción estatal consistente en evaluar objetivamente la fuerza efectivamente ejercida en lugar de atender a la gravedad de las consecuencias que de la misma se derivan para la paz y la

http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html, ultimo acceso el 16 de julio de 2014].

[165] Schaap, Arie, "Cyber Warfare operations: developments and use under international law", *Air Force Law Review*, volumen 64, 2009, p. 121 y ss.

[166] Baudin, *op. cit., supra* (nota 149), pp. 101-102.

[167] Recuérdese que el ya mencionado criterio de la escala y los efectos fue establecido por la Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 195.

[168] Schmitt, *op. cit., supra* (nota 3), p. 47.

seguridad internacionales[169]. Esta concepción estricta conduce un escenario poco realista en el que ninguna operación cibernética puede calificarse como uso de la fuerza en la medida en que le falte alguna de las características físicas tradicionales[170], con independencia del daño que pueda causar. Por esta razón, se han desarrollado otros marcos analíticos de referencia alternativos para la determinación de la ilegalidad de las operaciones cibernéticas por parte de los Estados sobre la base de los principios generales que rigen el uso de la fuerza también en el quinto dominio.

El primero de ellos, opuesto a la anterior aproximación -que estaba centrada en la comparación de la fuerza objetivamente ejercida y los medios utilizados con las operaciones físicas-, es el enfoque basado en los efectos, es decir, en el *quantum* de daño producido por el ataque. El problema que plantea este análisis es que introduce un alto grado de subjetividad que lo hace demasiado maleable en función de las capacidades e intereses de los Estados. En segundo lugar, el denominado "test de la equivalencia cinética"[171] sitúa el umbral del uso cibernético de la fuerza en la existencia de un daño similar al que se habría logrado mediante un ataque únicamente cinético, con el consiguiente inconveniente de excluir todas aquellas acciones hostiles cibernéticas que no resulte en un daño físico. En tercer lugar, algunos autores[172] abordan este análisis desde una perspectiva centrada en el objetivo

[169] Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, volumen 37, 1999.

[170] Schmitt, Michael, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts", *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy*, Consejo Nacional de Investigación de Estados Unidos, 2010, pp. 151-178 [disponible en http://sites.nationalacademies.org/CSTB/cs/groups/cstbsite/documents/webpage/cstb_059439.pdf, último acceso el 16 de julio de 2013].

[171] Hollis, Duncan, "Why States need and International Law for information operations", *Lewis and Clark Law Review*, volumen 11, 2007, p. 1023.

[172] Ver Stevens Sharon, "Internet War Crimes Tribunals and Security in an Interconnected World", *Transnational Law and Contemporary Problems*, volumen 18, 2009, pp. 676 y ss. o Condron, Sean, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law and Technology*, volumen 20, 2007, pp. 404 y ss.

del ataque, postulando que la mera intención hostil de dirigir un ataque contra las infraestructuras críticas e intereses vitales de un Estado es suficiente para dar lugar a responsabilidad internacional con independencia del daño causado.

Sin embargo, el llamado "análisis de Schmitt"[173] es el modelo analítico para calificar las operaciones cibernéticas como uso ilegítimo de la fuerza que goza de mayor aceptación en la literatura internacional, en la medida en que concilia con éxito los enfoques contrapuestos basados en los instrumentos y en las consecuencias y adopta una postura realista que puede describirse como *de lege lata*, en la medida en que se ciñe al marco jurídico preexistente sin prejuzgar como debería regularse este extremo por el Derecho internacional, campo reservado a la especulación jurídica. En este contexto, Schmitt propone un conjunto de factores con valor indiciario y no concluyente[174] concebidos para guiar a los Estados en su decisión sobre la permisibilidad de un ataque cibernético, decisión que, como cualquier otra sobre la calificación de cualquier forma de coerción, reviste un estricto carácter político. En concreto, los siete criterios siguientes deben ser tenidos en cuenta por los Estados:

1. Severidad -*severity*-: La amenaza o la causación de un daño físico por parte de la operación cibernética es evidentemente[175] el factor más relevante en la consideración de la misma como uso de la fuerza y puede determinar o excluir por sí mismo la calificación de la misma como un uso de la fuerza[176]. A este respecto, Schmitt implícitamente opta por la prevalencia del enfoque basado en los efectos.

2. Inmediación -*immediacy*-: La operaciones cibernéticas hostiles que generan efectos inmediatos, no dejando margen a medidas atenuantes o a procedimientos pacíficos de arreglo difícilmente pueden ser consideradas permisibles.

[173] Schmitt, *op. cit, supra* (nota 170) y Schmitt, *op. cit., supra* (nota 3).

[174] *Ibid.*

[175] *Ibid.*

[176] Schmitt, Michael, "Cyber operations and the jus ad bellum revisted", *Villanova Law Review*, volumen 56, 2011, pp. 569-606, p. 569.

3. Causalidad directa -*directness*-: La existencia de un nexo causal directo entre la operación cibernética y las consecuencias dañinas claramente perceptible para los Estados necesariamente va a ser considerado por éstos como un indicio de uso de la fuerza.

4. Carácter intrusivo -*invasiveness*-: Este criterio se centra en la intensidad de la invasión en los sistemas cibernéticos del Estado objetivo en términos de la clasificación de seguridad penetrada o la medida en que el único objeto del ataque es un Estado en particular.

5. Mensurabilidad -*measurability*-: Si las consecuencias son objetivamente identificables y cuantificables, es más probable que los Estados consideren que su causa proximal constituye un uso ilegítimo de la fuerza. A este respecto, Schmitt previene que, mientras la coerción económica no es susceptible de ser calificada como uso de la fuerza, en todo caso se considerará como tal un ataque militar que cause un grado limitado de destrucción.

6. Legitimidad presumida -*presumptive legitimacy*-: En la medida en que el aforismo *permissum videtur in omne quod not prohibitum* es aplicable en el ámbito del Derecho internacional, la presunción de legalidad opera en ausencia de prohibición.

7. Responsabilidad (*responsibility*): Una operación cibernética susceptible de ser inequívocamente imputada a un determinado Estado es plausiblemente calificable como un supuesto de uso de la fuerza por el mismo. De hecho, el propio Schmitt advierte que la atribución de los ataques cibernéticos a un agente estatal representa un prerrequisito de la evaluación llevada a cabo a través de estos factores, puesto que, aunque no puede descartarse que el uso de la fuerza también en el ciberespacio por actores no estatales o incluso *hackers* individuales pueda suponer un amenaza para la paz y la seguridad internacionales que requiera la adopción de las medidas colectivas necesarias por el Consejo de Seguridad[177] como tampoco puede excluirse su relevancia en los ámbitos del Derecho Internacional Humanitario o del Derecho Penal

[177] Melzer, Nils, *Cyberwarfare and International Law*, Instituto de las Naciones Unidas de Investigación para el Desarme, Ginebra, 2011, p. 12.

Internacional, sí es claro que no está prohibido por el artículo 2.4 de la CNU[178]. Empero, como quiera que la responsabilidad estatal es un continuo que abarca desde operaciones conducidas por el propio Estado a otras en las que su participación es reducida [179], el apoyo a ciberataques ejecutados por organizaciones no estatales puede hacer al Estado internacionalmente responsable por la asistencia indirecta prohibida por el principio de no intervención o en función de su escala y efectos por el propia prohibición del uso de la fuerza, pero en ningún caso directamente por la fuerza empleada por aquellos actores, salvo que sean *de facto* sus agentes[180].

Estos u otros elementos de juicio informan la antes mencionada decisión política de los Estados sobre la caracterización de un ciberataque como recurso prohibido a la fuerza y la adopción de una respuesta consecuente cuya legalidad dependerá de la razonabilidad de aquella evaluación previa. De esta forma, los modelos teóricos como el expuesto no sólo son el único expediente que permite identificar una transgresión cibernética del artículo 2.4 de la CNU, sino también el parámetro de legitimidad de la reacción ante la misma, al menos mientras persista la incapacidad o falta de disposición de los Estados para alcanzar un consenso en torno a la definición de uso cibernético de la fuerza en el futuro previsible, en parte debidas a la voluntad de preservar una ambigüedad que deja margen a los ataques cibernéticos esponsorizados por los Estados.

El informe del Instituto de las Naciones Unidas de Investigación para el Desarme (UNIDIR) de 2011 considera ejemplos notables de uso de la fuerza las operaciones cibernéticas destinadas a manipular los sistemas informáticos para provocar una crisis en una central nuclear, a abrir las compuertas de una presa situada sobre una zona densamente poblada o desactivar los dispositivos de control aéreo de un aeropuerto concurrido durante malas condiciones meteorológicas, todas ellas con consecuencias potencialmente terribles en

[178] Randelzhofer, *op. cit., supra* (nota 8), p. 121.

[179] Schmitt, *op. cit., supra* (nota 176), p. 569.

[180] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafos 205 y 247.

términos de víctimas mortales, heridos y daños materiales[181]. En sentido contrario, el mismo documento afirma que la mención expresa de la "interrupción total o parcial de [...] medios de comunicación" por el artículo 41 de la CNU como una medida que no implica el uso de la fuerza armada parece excluir de dicho concepto ataques como la denegación de servicios[182].

No obstante lo anterior, no debe concluirse la ausencia de efectos violentos sea incompatible necesariamente con la fuerza armada[183], pues ello resultaría contrario al propósito de mantener la paz y la seguridad internacional que preside desde la artículo 1 de la CNU la estructura de seguridad mundial al circunscribir la prohibición del artículo 2.4 al empleo de medios y métodos equivalentes a todos los efectos a un quebrantamiento de la paz entre los Estados implicados[184]. Tampoco el hecho de aceptar, como proponen algunos autores, que los ciberataques tienen que producir los mismos efectos que los ataques convencionales para constituir un uso ilegítimo de la fuerza [185] supondría excluir a aquéllos que no provoquen una destrucción física si se considera que pueden traspasar este umbral los actos como el armamento o el entrenamiento de guerrillas que no pueden calificarse como fuerza armada, como ha puesto de manifiesto la CIJ en el asunto de las "Actividades militares y paramilitares en y contra Nicaragua"[186].

Por el contrario, la prohibición impuesta por el artículo 2.4 de la CNU comprende cualquier recurso a la fuerza con independencia de su magnitud y duración[187] y del arma empleada[188] en un continuo que abarca desde los actos menores de fuerza interestatal, que permiten la adopción de contramedidas,

[181] Melzer, *op. cit., supra* (nota 177), p. 7.

[182] Ibíd., p. 7.

[183] Schmitt, *op. cit., supra* (nota 169), p. 912.

[184] Melzer, *op. cit., supra* (nota 177), p. 8.

[185] Baudin, *op. cit., supra* (nota 149), p. 105.

[186] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 228.

[187] Corte Internacional de Justicia, *Sentencia de 9 de abril de 1949 en el asunto del estrecho de Corfú*, Organización de las Naciones Unidas, La Haya, 1949, p. 47, opinión separada del juez Álvarez.

[188] Corte Internacional de Justicia, *op. cit., supra* (nota 32).

hasta los más graves de ataque armado o agresión, que justifican el ejercicio del derecho a la legítima defensa. El siguiente epígrafe se propone trazar una frontera en éstos y aquéllos en el ámbito cibernético.

5.3 CIBERATAQUE ARMADO:

La primera cuestión que se plantea en relación con la consideración de una operación cibernética como ataque armado, la más grave forma de uso de la fuerza prohibido[189] y fundamento del derecho a la legítima defensa previsto en el artículo 51 de la CNU es de orden literal, es decir, para dar lugar a un "ataque armado", el ciberespacio tiene que ser considerado un "arma"[190]. En este sentido, valga lo argumentado en el epígrafe anterior a propósito de la fuerza armada como noción comprensiva de las armas no sólo por naturaleza, sino también por uso previsible[191], en tanto no es la denominación de un dispositivo ni su uso habitual lo que lo convierte en un arma, sino la intención con que se utiliza y sus efectos, pudiendo reputarse que el uso de cualquier dispositivo o conjunto de dispositivos resultando en pérdidas de vidas humanas o grave destrucción material cumple los requisitos de un ataque armado[192].

Aclarado este extremo, debe tenerse en cuenta asimismo que la mayoría de los autores parece interpretarlo en el sentido de que una operación cibernética constituye un ataque armado en todo caso si sus efectos son equivalentes a los de un ataque convencional en términos de pérdidas de vidas, lesiones a seres humanos o destrucción material[193]. En ausencia de estos resultados, dada la insuficiente práctica de los Estados al respecto, sólo parece razonable calificar como tal aquel ciberataque con el potencial de provocar una disfunción severa de las funciones esenciales o de la estabilidad

[189] Corte Internacional de Justicia, *op. cit., supra* (nota 1), párrafo 191.

[190] Melzer, *op. cit., supra* (nota 177), p. 13.

[191] Baudin, *op. cit., supra* (nota 149), p. 57.

[192] Zemanek, Karl, "Armed attack", en Rüdiger Wolfrum (ed.), *Encyclopedia of Public International Law*, Max Planck, 2010, entrada 21.

[193] Ver Gill y Ducheine, *op. cit.,supra* (nota 51), pp. 444 y 445.

del Estado víctima y su incapacidad para eliminar estos efectos durante un prolongado periodo de tiempo por afectar a infraestructuras vitales[194].

El primero de estos dos enfoques, relativo a la equivalencia de las consecuencias, que también se presentó como generalmente aceptado en sede de uso de la fuerza cibernético[195], ha sido empero objeto de crítica. Efectivamente, retomando el citado criterio de la escala y efectos[196] presentado por la CIJ para delimitar el ataque armado de los usos menos graves de la fuerza, si el mismo fuera interpretado exclusivamente en el sentido de efectos equivalentes a la destrucción física, su aplicación daría lugar a una definición de agresión cibernética demasiado restrictiva, excluyendo los ciberataques con consecuencias tan graves como la disfunción de toda la red eléctrica nacional de un Estado, sus telecomunicaciones o su sistema de defensa aérea, o demasiado amplia, incluyendo denegaciones de servicios a gran escala contra infraestructuras no esenciales, en función de lo que se entienda por "equivalente"[197].

Ello obliga a definir una segunda aproximación a la aplicación del criterio de la escala y efectos para la definición de los ciberataques armados, construida en torno al concepto de infraestructura crítica. De este modo, puede considerarse agresión armada una operación cibernética cuyos "efectos" sean la disfunción de los servicios esenciales un Estado, afectando así al conjunto de su población, mediante la alteración de "escala" suficiente del normal funcionamiento de alguna infraestructura crítica, conceptuándose ésta de distinta forma en función del gobierno u organización internacional. A continuación se ofrecen algunas definiciones a título de ejemplo.

1. La Unión Europea entiende por tal

> "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la

[194] *Ibíd.*, pp. 439, 440, 445 y 459.

[195] Schmitt, *op. cit., supra* (nota 3), p. 47.

[196] Corte Internacional de Justicia, *op. cit., supa* (nota 1), párrafo 195.

[197] Melzer, *op. cit., supra* (nota 177), p. 14.

población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones"[198].

2. La Asamblea General de las Naciones Unidas, "reconociendo que cada país determinará sus propias infraestructuras de información esenciales", orienta esta decisión mencionando como ejemplo

"las utilizadas para, entre otras cosas, la generación, transmisión y distribución de energía, el transporte aéreo y marítimo, los servicios bancarios y financieros, el comercio electrónico, el suministro de agua, la distribución de alimentos y la salud pública- y las infraestructuras de información esenciales que interconectan y afectan cada vez más sus operaciones"[199].

3. Washington hace mención expresa al ciberespacio al concebir como infraestructuras críticas los sistemas físicos y cibernéticos esenciales para el funcionamiento mínimo de la economía y el gobierno incluyendo, *inter alia*, las telecomunicaciones, la energía, la banca, las finanzas el transporte, los sistemas hidráulicos y los servicios de emergencia, tanto públicos como privados[200]. Desde el punto de vista de la seguridad, se incluyen los sistemas y activos, físicos o virtuales, hasta tal punto vitales para los Estados Unidos que su disfunción o destrucción tendría un impacto debilitador en la seguridad, la seguridad económica nacional, la salud y la seguridad públicas nacionales o cualquier combinación de los mismos[201].

4. En el ordenamiento jurídico español, infraestructuras críticas son

[198] Consejo de la Unión Europea, *Ofrecer seguridad en un mundo en evolución. Informe de 11 de diciembre de 2008 sobre la aplicación de la Estrategia Europea de Seguridad* [S407/08], Unión Europea, Bruselas, 2008 [disponible en http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf, último acceso el 26 de junio de 2014], art. 2.a).

[199] Asamblea General de las Naciones Unidas, *Resolución de 30 de enero de 2004 sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales*, Organización de las Naciones Unidas, Nueva York, 2004.

[200] Presidente de los Estados Unidos, *US Presidential Decision Directive 63 of 22 May 1998 on Critical Infrastructure Protection*, Estados Unidos de América, Washington D. C., 1998, sección I.

[201] Congreso de los Estados Unidos, *op. cit., supra* (nota 77), art. 1016(e).

> "las infraestructuras estratégicas [entendiendo por tales "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales"] cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales [considerando como tal "el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas"]"[202].

Desde el punto de vista fáctico, una parte de la literatura no sólo ha visto un ejemplo claro de operación dirigida contra las infraestructuras críticas de un Estado, sino además un estadio avanzado en la ciberguerra al permitir la destrucción física de las infraestructuras[203], en la inutilización en 2010 de mil centrifugadores de la central nuclear iraní de Natanz, un quinto de los que estaban en activo, por el *malware* Stuxnet, presuntamente como parte de una campaña secreta de ataques cibernéticos contra el programa nuclear de Irán iniciada por el anterior presidente de Estados Unidos George Bush bajo el nombre en clave "Juegos Olímpicos", intensificada por la administración Obama y apoyada por Israel . Dos años atrás, *hackers* aparentemente al servicio del Kremlin, que negó su implicación ante las acusaciones de Tiblisi, ya había provocado una serie de denegaciones de servicio en páginas *web* oficiales clave de Georgia, impidiendo al Gobierno la comunicación *online* como paso previo a la invasión rusa convencional del territorio de la república caucásica. De la misma forma, Israel utilizó en 2007 un programa similar al estadounidense "Suter" para introducir información falsa en los medios de detección del sistema integrado de defensa aérea de Siria con el fin de entrar

[202] Cortes del Reino de España, "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas", *Boletín Oficial del Estado número 102 de 29 de abril de 2011 páginas 43.370-43.380*, Reino de España, 2011, art. 2.

[203] Mongin, Dominique, "Les cyber-attaques, arme de guerre en temps de paix", *Revue Esprit*, número de enero, 2013, pp. 32 y ss.

en su espacio aéreo y ejecutar un bombardeo sobre unas instalaciones nucleares en Al-Kibar bajo la clave “Operación Orchard”.

Para otros autores, en cambio, hasta el momento ningún ciberataque ha superado el umbral del artículo 51 CNU, en tanto los que más se acercaron, como la infección con gusano Stuxnet, no supuso daños a seres humanos ni destrucción material grave ni afectó a una infraestructura crítica distorsionando el funcionamiento o la estabilidad del Estado objetivo, más allá de ralentizar la producción de uranio iraní. En general, parece poco probable que por el momento una operación cibernética independiente, es decir, no enmarcada dentro de una ofensiva más amplia que implique el uso fuerza física, pueda causar daños humanos o perjuicios materiales en infraestructuras críticas lo suficientemente graves y persistentes como para considerarlo un ataque armado[204]. En cualquier caso, las operaciones meramente cibernéticas no son tan eficaces para destruir objetivos militares como para alcanzar fines de espionaje y sabotaje por debajo del umbral de un ataque armado [205], limitándose en la práctica el riesgo de que se produzcan tales efectos graves a la manipulación de instalaciones situadas cerca de núcleos de población.

Los ataques a redes informáticas destinados a apoyar operaciones militares saboteando o a inutilizar las armas o los sistemas de comunicación del enemigo son un escenario más realista que incluso cuenta con un precedente en la referida “Operación Orchard”[206]. De hecho, la integración coherente de las actividades cibernéticas dentro del abanico de capacidades militares ya es una realidad en muchas estrategias de seguridad y defensa nacionales, como la británica, que creó un Grupo de Operaciones Cibernéticas de Defensa dentro del Ministerio de Defensa en 2010[207], o la española, en cuyo

[204] Tsang, Rose, “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks 21, University of California”, *Working Paper*, Goldmand School of Public Policy, Berkeley, 2009.

[205] Gill y Duchaine, *op. cit., supra* (nota 51), p. 463.

[206] Garwood-Gowers, Andrew, “Israel’s Airstrike on Syria’s Al-Kibar Facility: A Test Case for the Doctrine of Pre-Emptive Self-Defence?”, *Journal of Conflct and Security Law*, volumen 16, 2011, pp. 263-291.

[207] Gobierno del Reino Unido, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review of 19 October 2010*, Reino Unido de la Gran Bretaña e Irlanda del Norte,

marco la Orden Ministerial 10/2013 [208] instituyó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Estos ejemplos muestran la tendencia de algunos Estados a considerar los sistemas de comunicación e información como un arma más frente a la práctica generalizada de utilizarlos como mera barrera defensiva, pero en cualquier caso no como una forma autónoma de hacer la guerra.

Para concluir, es conveniente matizar la perspectiva puramente cuantitativa desde la que se ha analizado la aplicación el criterio de la escala y efectos a las operaciones cibernéticas, pues la calificación de las mismas como ataque armado también depende de la constatación cualitativa de una intención específica de transgredir la esfera de soberanía del Estado víctima atribuible al Estado agresor[209]. Ello explica que un ataque resultante en el asesinato de un individuo por agentes estatales en el territorio de otro Estado pueda calificarse en sí mismo de agresión, como el que dio lugar a la condena de Israel por el Consejo de Seguridad[210] tras asesinar a un líder Palestino en Túnez.

En todo caso, ni desde la perspectiva cuantitativa ni desde la puramente cualitativa existe acuerdo acerca del umbral a partir del cual una operación cibernética puede considerarse un ataque armado que active la cláusula derogatoria de la prohibición del uso de la fuerza contemplada en el artículo 51 de la CNU, al igual que ocurría con la prohibición en sí. También en este caso será precisa una decisión política del Estado víctima razonable a la luz de algunos de los modelos teóricos que, como los expuestos en el epígrafe anterior, han sido desarrollados por la doctrina científica También las organizaciones internaciones que, como la UE y la OTAN, cuenten con cláusulas de defensa mutua tienen un papel importante en la definición de

2010 [disponible en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf, ultimo acceso el 16 de julio de 2014], p. 47.

[208] Ministerio de Defensa del Reino de España, *op. cit., supra* (nota 161).

[209] Corte Internacional de Justicia, *op. cit., supra* (nota 52), párrafo 64.

[210] Consejo de Seguridad de las Naciones Unidas, *Resolución 611 de 25 de abril 1988 sobre Israel-Túnez*, Organización de las Naciones Unidas, Nueva York, 1988.

criterios para determinar la legalidad del ejercicio de la legítima defensa colectiva, como se analiza en el último epígrafe de este apartado.

Pero antes de estudiar las perspectivas de la UE y la OTAN al respecto, es obligado aclarar que los expuestos condicionantes consuetudinarios de necesidad, proporcionalidad e inmediatez, así como los demás instituidos por la CNU, a los que se encuentra sujeto el ejercicio del derecho a la legítima defensa son igualmente de aplicación en el ciberespacio, como también lo es el cuarto y más controvertido requisito de inminencia introducido por la doctrina anticipatoria, dada por buena en el último apartado del epígrafe anterior en relación con las agresiones convencionales. A este respecto, la regla 15 del Manual de Talín puntualiza que el derecho al uso de la fuerza en legítima defensa surge si un ciberataque ocurre o es inminente, repasando a continuación los principales enfoques respecto de la anticipación que fueron analizados en relación con el mundo físico. A título de recordatorio, cabe mencionar la aproximación estricta, rechazado por la mayoría del grupo internacional de expertos redactor del Manual[211], que requiere que el ataque armado esté a punto de ser lanzado[212]. Por oposición, la ya mencionada "tesis de la última ventana factible de oportunidad" no restringe temporalmente la acción defensiva, la cual debe llevarse a cabo en cualquier momento a partir del cual pueda razonablemente entenderse que la inacción del Estado víctima prospectivo determinaría su incapacidad para defenderse de forma efectiva[213].

Cualquiera que sea el enfoque adoptado para interpretar la doctrina anticipatoria, es claro que ésta debe entenderse directamente aplicable a aquellos ciberataques incardinados en una operación militar mayor que suponga el uso de la fuerza física con los mismos requisitos convencionales y consuetudinarios ya mencionados, a saber, una amenaza manifiesta e inequívocamente inminente de ataque armado en el futuro próximo[214]. Ello no es más que la aplicación de la doctrina anticipatoria en sus términos clásicos,

[211] Schmitt, *op. cit., supra* (nota 3), p. 61.

[212] Bowett, Derek, *Self-defence in International Law*, Praeger, Nueva York, 1958, p. 187-192.

[213] Schmitt, *op. cit., supra* (nota 170), 2010.

[214] Gill y Ducheine, *op. cit., supra* (nota 51), p. 465.

como también lo es la adopción medidas de legítima defensa necesarias y proporcionales para impedir que la amenaza se materialice ante una operación cibernética que se juzgue razonablemente destinada a reducir la capacidad de la víctima prospectiva de responder a una inminente agresión cinética, en la medida en que permita identificar al futuro agresor y ponga de manifiesto la intención hostil del mismo.

En el caso de operaciones meramente cibernéticas, la aplicación de la doctrina anticipatoria no es tan automática como en el supuesto de los ataques que combinan la fuerza digital y física, debido a que la incertidumbre propia del ciberespacio, aunque cada vez más reducida gracias al desarrollo de las capacidades de seguridad cibernética, impide una evaluación precisa de la autoría, alcance y efectos pretendidos de la agresión y la consiguiente ponderación de las medidas defensivas dentro de los parámetros de necesidad y proporcionalidad [215] . No obstante, cabe destacar que la teoría de la "acumulación de eventos"[216], denominada de los *pin-prick attacks* en inglés o *nadelstichtaktic* en alemán, defiende el ejercicio del derecho de la legítima defensa para detener una sucesión de ataques digitales de pequeña escala por debajo del umbral del ataque armado interconectados en términos de tiempo y finalidad o para evitar una subsecuente agresión a mayor escala.

Por su parte, el Instituto de las Naciones Unidas de Investigación para el Desarme[217] adopta el enfoque contrario al sostener que la acción de legítima defensa en el ciberespacio no es permisible en respuesta a un daño ya consumado consecuencia de operaciones cibernéticas hostiles, sino tan sólo con vistas a prevenir o repeler un ataque inminente o actual y sólo en la medida necesaria para alcanzar tal propósito. También advierte que, si bien el daño causado por la medida cibernética defensiva debe estar justificado por la gravedad del ataque a prevenir, la rapidez, la imprevisibilidad, la subrepción, la automatización y el diferimiento en el tiempo de los efectos, a veces producidos

[215] *Ibíd.*, p. 471.

[216] Blum, Yehuda, "State Response to Acts of Terrorism", *German Yearbook of International Law*, volumen 19, 1976, pp. 223-237.

[217] Melzer, *op. cit., supra* (nota 177), p. 18.

meses después de la intrusión, hacen muy difícil la evaluación de la necesidad y la proporcionalidad, así como la identificación del atacante, análisis que debe realizarse caso por caso.

A pesar de todo, la legítima defensa anticipatoria es un resorte marginal, especialmente en el ciberespacio, donde la probabilidad de que se produzca un ataque armado es reducida, y la práctica de la mayoría de los Estados, sobre todo europeos, muestra un enfoque más defensivo que ofensivo de la seguridad cibernética que será objeto de análisis en la tercera parte de este trabajo al valorar la compatibilidad entre las políticas de la UE y la OTAN en materia de ciberdefensa.

5.4 LEGÍTIMA DEFENSA COLECTIVA Y CIBERATAQUES:

Nada impide que la vertiente colectiva de la legítima defensa opere en el ciberespacio con la misma virtualidad y alcance que en el mundo físico y sujeta a los mismos condicionantes que en su dimensión individual. Así lo reconoce la regla 16 del Manual de Talín al sostener que la legítima defensa contra un ciberataque calificado de ataque armado puede ser ejercida colectivamente, pero sólo a solicitud del Estado víctima y dentro del ámbito de dicha solicitud[218], salvaguarda exigida por el principio de no injerencia que también se predica de de las intervenciones cinéticas[219]. En cualquier caso, este requisito de consentimiento se entiende cumplido en el caso de la UE y la OTAN por la existencia de cláusulas de asistencia mutua, cuya aplicación al quinto dominio se estudia a continuación.

En lo que respecta a la Alianza Atlántica, la primera cuestión que se plantea es determinar si las operaciones cibernéticas dirigidas contra Estados miembros son subsumibles dentro del artículo 4[220] o 5 del TAN, es decir, si el *casus foederis* consistente en un ataque armado contra uno o varios miembros

[218] Schmitt, *op. cit., supra* (nota 3), p. 63.

[219] Corte Internacional de Justicia, *op. cit., supra* (nota 1).

[220] Dicho artículo establece que “las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada”.

incluye también los ciberataques[221]. A este respecto, la posición de la OTAN y sus miembros en relación con la extrapolación del deber de asistencia mutua al ciberespacio no es clara, lo cual es especialmente relevante tratándose de una organización internacional en la que, a diferencia, de la UE, la cláusula de asistencia mutua no opera automáticamente, sino que la última decisión corresponde a los aliados[222], y éstos han optado por mantener una cierta "ambigüedad estratégica" en los distintos intentos de definir una postura común al respecto.

Así, la Declaración Final de la Cumbre de Bucarest celebrada en abril de 2008[223], mediante la cual los Jefes de Estado y de Gobierno de los aliados aprobaron la Política de Ciberdefensa adoptada tres meses atrás por la OTAN, reconoció la necesidad de los Estados miembros de proteger los sistemas de información claves de acuerdo con sus respectivas responsabilidades, compartir buenas prácticas y desarrollar una capacidad para ayudar a las naciones aliadas, previa solicitud, a contrarrestar un ciberataque[224]. Tampoco en vísperas del Nuevo Concepto Estratégico el informe elaborado en mayo de 2010 por el Grupo de Expertos resuelve la indeterminación, limitándose a afirmar que las "amenazas menos convencionales contra la Alianza" como los "ciberasaltos" pueden o no alcanzar el nivel de un ataque del artículo 5[225] y que los ciberataques a gran escala contra los sistemas de control y mando y las redes eléctricas de la OTAN garantizarían automáticamente las consultas

[221] Roscini, Marco, *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014, p. 93.

[222] Häußler, Ulf, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty", *International Cyber Security Legal & Policy Proceedings 2010*, Centro de Excelencia Cooperativo de Ciberdefensa, Talín, 2010, p. 107.

[223] Consejo del Atlántico Norte, *Bucharest Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008*, Organización del Tratado del Atlántico Norte, Bucarest, 2008.

[224] *Ibíd.*, párrafo 47.

[225] Grupo de Expertos sobre el Nuevo Concepto Estratégico de la OTAN, *NATO 2020: assured security; dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO of 17 May 2010*, Organización del Tratado del Atlántico Norte, Bruselas, 2010, p. 9.

previstas en el artículo 4 y podrían conducir a la adopción de medidas de defensa colectiva al amparo del artículo 5[226]. En todo caso, corresponde al CAN determinar si un peligro no convencional, como un ciberataque, activa los mecanismos de defensa del artículo 5, atendiendo a la naturaleza, fuente, alcance y otros aspectos de la concreta amenaza a la seguridad[227].

El propio Concepto Estratégico de Lisboa adoptado en noviembre de 2010 se resiste a arrojar luz sobre la materia y se muestra aún más vago, restringiéndose a prever que la organización continuaría desarrollando su capacidad de prevenir, detectar, defenderse y recuperarse de los ciberataques, haciéndose énfasis en la utilización del proceso de planificación de la OTAN para mejorar, coordinar, centralizar e integrar las capacidades de sus miembros[228], pero sin pronunciarse sobre el alcance o la base jurídica de la respuesta ante los mismos. Asimismo, evita el término "ataque armado" al referirse a la defensa colectiva prevista en el artículo 5 como una de las tareas esenciales de la Alianza, prefiriendo las expresiones "amenaza de agresión" y "desafíos de seguridad emergentes" que amenacen la seguridad esencial de aliados individuales o del conjunto de los mismos[229], conceptos más indeterminados si cabe y aparentemente menos exigentes en lo que respecta al umbral establecido por el artículo 51 de la CNU.

Más recientemente, la versión de la Política de Ciberdefensa de la OTAN revisada en 2011 reconoce expresamente que "la OTAN mantendrá la ambigüedad estratégica así como la flexibilidad acerca de cómo responder a los diferentes tipos de crisis que incluyen un componente cibernético", añadiendo que "cualquier respuesta de defensa colectiva de la OTAN está sujeta a las decisiones políticas del Consejo del Atlántico Norte" y que "la OTAN no prejuzga ninguna respuesta y mantiene de este modo la flexibilidad

[226] *Ibíd.*, p. 45.

[227] *Ibíd.*, p. 20.

[228] Consejo del Atlánatico Norte, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the Northern Treaty Organisation of 19 November 2010*, Organización del Tratado del Atlántico Norte, Lisboa, 2010, párrafo 19.

[229] *Ibíd.*, párrafo 4.a).

en lo que respecta a decidir el curso de acción que debe o no ser tomado"[230]. No pueden reseñarse posteriores avances en este sentido, a pesar de que los Ministros de Defensa de la Alianza, en la primera reunión monográfica sobre ciberdefensa celebrada el 4 de junio de 2013 anunciaron su acuerdo de continuar las conversaciones sobre cómo la OTAN puede apoyar y asistir a los aliados que solicitan ayuda en caso de ciberataque en su reunión del 22 de octubre del mismo año[231].

En la práctica, esta falta de definición se tradujo en la ausencia de respuesta colectiva frente a los ataques por denegación de servicios dirigidos contra el Parlamento, el gobierno, los partidos políticos, la banca y los medios de Estonia en 2007 presuntamente por agentes dependientes de Rusia como represalia por la retirada de una estatua conmemorativa de los caídos soviéticos en la Segunda Guerra Mundial. En esta ocasión, la reacción de la Alianza se limitó a consultas posteriores al ataque sin invocación formal del artículo 4[232], aunque el Primer Ministro báltico al parecer consideró la posibilidad de hacer valer el artículo 5. No obstante, el Ministro de Defensa Jaak Aaviksoo reconoció que "en el presente, la OTAN no define los ciberataques como una clara acción militar" y que "ni un sólo Ministro de Defensa de la OTAN definiría un ciberataque como una clara acción militar en el presente", lo que significa que la previsión del artículo 5 "no será automáticamente extendida al país atacado", añadiendo que "este asunto necesita ser resuelto en el futuro próximo"[233]. Con este objeto Estonia y la

[230] División de Diplomacia Pública de la Organización del Tratado del Atlántico Norte, *Defending the Networks. The NATO Policy on Cyber Defence 2011*, Organización del Tratado del Atlántico Norte, Bruselas, 2011 [disponible en http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf, ultimo acceso el 25 de junio de 2014], p. 2.

[231] Organización del Tratado del Atlántico Norte, Organización del Tratado del Atlántico Norte, "NATO and cyber defence", *www.nato.int*, 2013 [disponible en http://www.nato.int/cps/en/natolive/topics_78170.htm, último acceso el 25 de junio de 2013].

[232] Häußler, *op. cit., supra* (nota 222), p. 120.

[233] Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, jueves 17 de mayo, 2007.

OTAN firmaron un memorando de entendimiento el 23 de abril de 2010 para facilitar el intercambio de información y crear un mecanismo de asistencia en caso de ciberataques contra el aliado báltico[234], aunque sin considerarlos como ataques armados contra la OTAN[235].

No obstante, la postura de algunos Estados miembros parece favorable a abrir la puerta a la ampliación del ámbito de aplicación del artículo 5 del TAN al ciberespacio. En este sentido, Roscini (2014, p. 95) enumera un conjunto de declaraciones oficiales relevantes en el ámbito de la defensa de los distintos aliados, tales como la del el Ministro de las Fuerzas Armadas del Reino Unido, afirmando que dicho precepto es "potencialmente" aplicable a los ciberataques; la del Jefe de Personal de Defensa británico, que sostuvo que un ciberataque sería un ataque armado en el sentido del artículo 5 si sus efectos fueran "severos"; o la del Informe del Comité Parlamentario de Seguridad Italiano de 7 de julio de 2010, apuntando que la noción de seguridad colectiva en el contexto de dicho precepto debería verse ampliada para comprender los ciberataques. En cualquier caso, el gobierno neerlandés ha declarado que la procedencia de la aplicación de la cláusula de asistencia mutua de la OTAN, incluso en el dominio digital, es una decisión que debe reservarse al ámbito político[236].

Para hacer frente a la incertidumbre que la Alianza y los aliados han preferido mantener en torno a la legítima defensa colectiva en el ciberespacio, puede plantearse la aplicación de las reglas generales de interpretación de los tratados[237], concretamente al artículo 31.3.c) de la Convención de Viena de 1969[238], que remite a "toda forma pertinente de derecho internacional aplicable

[234] Organización del Tratado del Atlántico Norte, "NATO and Estonia conclude agreement on cyber Defence", *www. nato.int*, 2010 [disponible en http://www.nato.int/cps/en/natolive/news_62894.htm, último acceso el 17 de julio de 2014].

[235] Roscini, *op. cit., supra* (nota 221), p. 95.

[236] Gobierno del Reino de los Países Bajos, *Government response of 6 April 2012 to the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law on cyber warfare*, Reino de los Países Bajos, La Haya, 2012.

[237] Roscini, *op. cit., supra* (221), p. 96.

[238] Organización de las Naciones Unidas, *Convención de 23 de mayo de 1969 sobre el Derecho de los Tratados* [1155 UNTS. 331], Viena, 1969, Artículo 31.3.a).

en las relaciones entre las partes", como lo es por antonomasia en este ámbito el propio artículo 51 de la CNU, mencionado expresamente en el artículo 5 del TAN como marco jurídico internacional del derecho a la legítima defensa. Adicionalmente, el artículo 7 del TAN establece que "el Tratado no [...] se podrá interpretar que afecte de modo alguno a los derechos y obligaciones derivados de la Carta", cláusula de subordinación a la Carta que no es necesaria para garantizar la primacía de la misma, al establecer el artículo 103 de la CNU que,

> "en caso de conflicto entre las obligaciones contraídas por los Miembros de las Naciones Unidas en virtud de la presente Carta y sus obligaciones contraídas en virtud de cualquier otro convenio internacional, prevalecerán las obligaciones impuestas por la presente Carta".

Por lo tanto, una operación cibernética tiene la condición de ataque armado a los efectos de activar el mecanismo de respuesta colectiva previsto en el artículo 5 del TAN si reúne las condiciones para considerarse como tal en el sentido del artículo 51 de la CNU, lo que retrotrae este análisis al punto de partida expuesto en epígrafes anteriores, esto es, se trata de una decisión política que, en el caso de la OTAN, deben tomar los aliados reunido en el seno del CAN.

Finalmente, el hecho de que el artículo 6, como ya se mencionó, limite territorialmente el ámbito del precepto que lo precede en el TAN y que los ciberataques carezcan de una localización geográfica concreta no impide la aplicación de la cláusula de asistencia mutua de la OTAN a los mismos, que se ubican allí donde causen pérdidas de vidas humanas, lesiones o daños materiales o donde radiquen las infraestructuras críticas afectadas[239]. En cualquier caso, las acciones coercitivas de la OTAN pueden tener lugar fuera de los límites de la región europea y atlántica si se encuentran funcionalmente vinculadas a la necesidad de responder a amenazas que puedan amenazar la estabilidad y la seguridad del área[240].

[239] Roscini, *op. cit., supra* (nota 221), p. 96

[240] Cannizzaro, Enzo, "NATO's New Strategic Concept and the Evolving Legal Regulation of the Use of Force", *The International Spectator*, volume 36, número 1, 2001, p. 67-74, p. 70.

En lo que respecta a la UE, la Estarategia de Ciberseguridad afirma que "un incidente o ataque cibernético de especial gravedad podría ser motivo suficiente para que un Estado miembro invocara la cláusula de solidaridad de la UE (artículo 222 del Tratado de Funcionamiento de la Unión Europea)"[241], sin hacer referencia a la cláusula atlantista del artículo 42.7 del TUE, respecto de la cual la Comisión de Asuntos Exteriores del Parlamento Europeo

> "considera que incluso los ataques no armados, por ejemplo los ciberataques contra infraestructuras críticas, lanzados con ánimo de ocasionar graves daños y perturbaciones a un Estado miembro e identificados como procedentes de una entidad externa, podrían considerarse cubiertos por la cláusula si la seguridad del Estado miembro se ve amenazada de manera significativa por sus consecuencias, dentro del pleno respeto del principio de proporcionalidad"[242].

De cualquier forma, una agresión virtual de la suficiente entidad no ha de quedar sin respuesta militar en el ámbito de la UE, ya que, por una parte, la cláusula de solidaridad es tan amplia como para justificar una reacción tal en caso de un" incidente o ataque cibernético de especial gravedad". Por otra parte, teniendo en cuenta que la redacción de la cláusula de asistencia mutua menciona expresamente el artículo 51 de la CNU, la aplicación del mismo criterio interpretativo del artículo 3.1.c) de la Convención de Viena de 1969 antes utilizado en relación el artículo 5 del TAN permitiría concluir la virtualidad del artículo 42.7 del TUE en relación con aquellos ciberataques constitutivos de ataque armado en las mismas condiciones arriba analizadas para el caso de la Alianza Atlántica. Ello se verifica con más razón en relación con aquellos socios que además son miembros de ésta por la previsión explícita del respeto a "los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte".

[241] Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *Comunicación conjunta de 7 de febrero de 2013 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro* [JOIN(2013) 1 final], Unión Europea, Bruselas, 2013.

[242] Comisión de Asuntos Exteriores del Parlamento Europeo, *op. cit., supra* (128), párrafo 13.

PARTE II: MARCO POLÍTICO DE LA COOPERACIÓN ENTRE UE Y OTAN:

Definido el marco de Derecho Internacional Público, concretamente de la parte del mismo que gobierna el recurso a la fuerza -*ius in bellum*-, que restringe en el ámbito cibernético, como en cualquier otro, la actuación defensiva de dos sujetos de Derecho internacionales como son la UE y la OTAN y de sus respectivos Estados miembros, el resto de este trabajo se dedica a incorporar las directrices políticas que dentro de aquellos límites rigen esta actuación. En otras palabras, si hasta ahora se ha tratado de dar respuesta a la cuestión de qué pueden hacer la UE y la OTAN en materia de ciberdefensa, la dimensión estratégica que ahora se introduce contesta a la pregunta de qué quieren hacer la UE y la OTAN en materia de ciberdefensa.

6 POLÍTICA COMÚN DE SEGURIDAD Y DEFENSA Y CIBERDEFENSA:

6.1 LA POLÍTICA EXTERIOR Y DE SEGURIDAD COMÚN Y LA POLÍTICA COMÚN DE SEGURIDAD Y DEFENSA EN EL TRATADO DE LISBOA:

Para el análisis del marco político de la ciberdefensa desde la perspectiva de la UE, es preciso dedicar un apartado al tratamiento que la defensa en general y la defensa cibernética en particular reciben en el nuevo escenario creado por el Tratado de Lisboa. Como ya se apuntó al presentar las cláusulas de asistencia mutua y solidaridad, la reforma de los Tratados de 2007, en línea con la *non nata* Constitución para Europa, acomete una remodelación de la PESC con el principal objetivo de lograr la visibilidad en el plano internacional de una UE a menudo tachada de "gigante económico, enano político y gusano militar"[243]. Primer signo de esta voluntad de convertirse en un actor global relevante es la afirmación expresa de la personalidad jurídica de la UE en el

[243] Frase atribuida a Mark Eyskens, Ministro de Exteriores belga durante la Primera Guerra del Golfo, citado en Sánchez Pereyra, Antonio, *Geopolítica de la expansión de la OTAN*, México D.F., Plaza y Valdés, 2003, p. 311.

artículo 47 del TUE, despejándose las dudas sobre la misma que llevaron al ex-Presidente de la Comisión Jacques Delors a definir como "objeto político no identificado"[244] a este nuevo paraguas creado por el Tratado de Maastricht de 1992 para recubrir a los denominados "tres pilares", las Comunidades Europeas y la cooperación intergubernamental en asuntos exteriores y de justicia e interior.

Lisboa también ha supuesto, al menos formalmente, la desaparición de aquella estructura tripartita, quedando en lo sucesivo los pilares intergubernamentales segundo, correspondiente a la PESC, y tercero, relativo a la Cooperación en Asuntos de Justicia e Interior, integrados en el pilar comunitario. Sin embargo, la "comunitarización" de la PESC es hasta cierto punto aparente, pues, como advierten Martín y Pérez de Nanclares y Urrea Corres (2010, p. 33), se mantienen peculiaridades institucionales, tales como la adopción de decisiones por unanimidad del Consejo Europeo y del Consejo y la exclusión de los actos legislativos previstas en el artículo 31.1 del TUE, y restricciones competenciales, orientadas a preservar el papel predominante de los Estados miembros, que permiten hablar de "de un (imaginario) pilar de inspiración intergubernamental dentro de una Unión que por lo demás ejercita sus competencias al <<modo comunitario>> de manera (casi) plena".

Otros cambios institucionales relevantes son la creación de los cargos de Presidente del Consejo Europeo, que "asumirá, en su rango y condición, la representación exterior de la Unión en los asuntos de política exterior y de seguridad común, sin perjuicio de las atribuciones del Alto Representante"[245], y de Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, que "estará al frente de la política exterior y de seguridad común de la Unión", "presidirá el Consejo de Asuntos Exteriores" , "será uno de los Vicepresidentes de la Comisión"[246] y, "en el ejercicio de su mandato, [...] se

[244] Citado por Quermonne, Jean-Louis, "Existe-t-il un modèle politique européen?", *Revue Française de Science Politique*, volumen 40, número 2, 1990, p. 192-211, p. 196.

[245] Unión Europea, *op. cit., supra* (nota 36), Artículo 15.6.

[246] *Ibíd.*, Artículo 18.

apoyará en un servicio europeo de acción exterior" que "trabajará en colaboración con los servicios diplomáticos de los Estados miembros"[247].

En lo específicamente relativo a la nueva PCSD, deben destacarse tres aspectos relevantes[248]: (a) el contraste entre la ambiciosa formulación de objetivos de acción exterior en los artículos 3.5[249] y 21[250] del TUE y el escaso desarrollo institucional, (b) la incorporación de las cláusulas de asistencia mutua y solidaridad que han sido objeto de estudio pormenorizado y (c) la previsión en los artículos 42.6 y 46 de un mecanismo de Cooperación Estructurada Permanente en materia de defensa para aquellos "Estados miembros que cumplan criterios más elevados de capacidades militares y que hayan suscrito compromisos más vinculantes en la materia para realizar las misiones más exigentes". Adicionalmente, dentro de la óptica de gestión de crisis que preside la lógica de la acción exterior europea en materia de defensa,

[247] *Ibíd.*, Artículo 27.3.

[248] Martín y Pérez de Nanclares, *op. cit., supra* (nota 114), pp. 139-140.

[249] "En sus relaciones con el resto del mundo, la Unión afirmará y promoverá sus valores e intereses y contribuirá a la protección de sus ciudadanos. Contribuirá a la paz, la seguridad, el desarrollo sostenible del planeta, la solidaridad y el respeto mutuo entre los pueblos, el comercio libre y justo, la erradicación de la pobreza y la protección de los derechos humanos, especialmente los derechos del niño, así como al estricto respeto y al desarrollo del Derecho internacional, en particular el respeto de los principios de la Carta de las Naciones Unidas".

[250] La Unión dirigirá la política exterior y de seguridad común:

a) definiendo sus orientaciones generales;

b) adoptando decisiones por las que se establezcan:

i) las acciones que va a realizar la Unión;

ii) las posiciones que va a adoptar la Unión,

iii) las modalidades de ejecución de las decisiones contempladas en los incisos i) y ii);

y

c) fortaleciendo la cooperación sistemática entre los Estados miembros para llevar a cabo sus políticas.

las “misiones de Petersberg” incluidas en el antiguo 17.2 del antiguo TUE[251] se amplían en el artículo 43.1 del nuevo TUE[252].

No obstante, a pesar de su nombre, la PCSD no es, al menos por el momento una política común, como deja claro el artículo 42.2 del TUE al prever la mera “definición progresiva de una política común de defensa de la Unión” que “conducirá a una defensa común una vez que el Consejo Europeo lo haya decidido por unanimidad” y recomendar “a los Estados miembros que adopten una decisión en este sentido de conformidad con sus respectivas normas constitucionales”. Esta lógica de cooperación hace depender el presente y el futuro de la defensa de la UE de la mayor o menor voluntad de los Estados miembros, la cual será objeto de análisis a continuación.

Pero, antes, para concluir esta presentación de la nueva PCSD, es conveniente describir brevemente su estructura institucional[253], en cuya cúspide se encuentra el Comité Político y de Seguridad de la UE (en adelante COPS), responsable en el plano militar de la dirección política del desarrollo de la capacidad de defensa, con el asesoramiento del Comité Militar de la UE asistido por el Estado Mayor de la UE (en adelante EMUE), y del control político y la dirección estratégica de las operaciones de gestión de crisis, bajo la autoridad de la Alta Representante. En el plano político, constituye el órgano preferente para el diálogo sobre la PESD con otros organismos internacionales, como la OTAN, y se encarga de monitorizar la situación internacional en el ámbito de la PESC. Por debajo del COPS se encuentra el Comité Militar de la UE (en adelante CMUE), un foro de consulta y cooperación militar entre los

[251] “Misiones humanitarias y de rescate, misiones de mantenimiento de la paz y misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz”.

[252] “Las actuaciones conjuntas en materia de desarme, las misiones humanitarias y de rescate, las misiones de asesoramiento y asistencia en cuestiones militares, las misiones de prevención de conflictos y de mantenimiento de la paz, las misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz y las operaciones de estabilización al término de los conflictos”.

[253] Esta breve descripción se ha elaborado a partir de Reichard, *op. cit., supra* (nota 84), pp. 64-65.

Estados miembros en los ámbitos de prevención de conflictos y gestión de crisis cuyas funciones comprenden asesorar al COPS emitiendo recomendaciones y dictámenes por consenso sobre asuntos militares y asumir la dirección militar del EMUE en caso de crisis mediante la adopción de directrices militares.

En la base de la pirámide se halla el EMUE, que constituye el vínculo entre el CMUE y los recursos militares a disposición de la UE, responsabilizándose de la supervisión y evaluación de las fuerzas y capacidades que los Estados miembros ponen a disposición de la UE y de la presentación de recomendaciones al respecto, así como de la determinación y enumeración de las fuerzas europeas nacionales y multinacionales para las operaciones dirigidas por la Unión y coordinadas con la OTAN. Realiza estas tareas teniendo en cuenta el Proceso de Planificación de la Defensa de la OTAN así como el Proceso de Planificación y Análisis de la Asociación para la Paz y trabaja asimismo en estrecha cooperación con la Agencia Europea de Defensa, creada en 2004 para la promoción de la industria armamentística creando un mercado europeo competitivo de equipos de defensa.

6.2 PANORAMA GENERAL DE LA DEFENSA EUROPEA:

Expuestos los avances realizados en el plano jurídico con el objetivo de convertir a la UE en un actor global, es preciso evaluar si se han traducido a nivel político en un verdadero compromiso en este sentido, partiendo de la premisa de que la ausencia de una verdadera política común de defensa y del carácter esencialmente intergubernamental de la PCSD dejan su definición a la voluntad de los Estados miembros. Efectivamente, el Tratado de Lisboa se limitó a establecer “los pilares necesarios para construir una defensa común si los socios europeos así lo desean”[254]. A este respecto, cabe adelantar que el hecho de que, desde su entrada en vigor y hasta el presente, ninguna de las disposiciones en materia de defensa haya sido desarrollada indica “la falta de

[254] Colom Piella, Guillem, “Los Límites de la Política Común de Seguridad y Defensa”, *Revista General de la Marina*, número de abril, 2014, pp. 447-454, p.451.

visión común y una limitada voluntad política para desarrollar una defensa europea creíble"[255].

Que la UE tiene que reclamar su protagonismo e influencia más allá de su región geográfica en el ámbito de las relaciones internacionales es algo en que todos los Estados miembros están de acuerdo, ya que así lo entienden incluso aquellos socios con una visión más limitativa o pragmática de la construcción europea, como pone de relieve el hecho de que fuera precisamente Suecia la que impulsara durante su presidencia en 2009 un conjunto de contactos y reuniones ministeriales formales e informales bajo la rúbrica "Europa como actor global"[256]. El consenso acerca de la necesidad de que la UE adopte este rol de forma eficaz se basa en un conjunto de elementos de base compartidos, concretamente (a) la cada vez más estrecha relación entre los intereses de la UE y los del resto del mundo, siendo en este sentido esencial explotar la pertenencia a un bloque potente como el europeo; (b) la idoneidad de los instrumentos de actuación de la UE para contribuir al desarrollo de la paz y la seguridad internacionales; (c) el objetivo de contribuir a construir un sistema internacional multilateral con las ONU en la cúspide; y (d) la difusión de los límites entre las dimensiones exterior e interior de la seguridad debido a la creciente complejidad de las amenazas[257].

No obstante, la UE como actor global con objetivos e intereses necesita dotarse para la realización de los mismos de una política y no sería del todo exacto considerar a la PCSD como tal, ya que no se construye sobre intereses compartidos a partir de los cuales se fijan objetivos, sino que más bien reviste la naturaleza de relaciones de seguridad y defensa basadas en la consulta para tratar de encontrar posiciones en los objetivos individuales previamente establecidos[258]. Este vacío estratégico de la política de seguridad y defensa

[255] *Ibid.*

[256] Mora Benavente, Enrique, "Introducción", en Instituto Español de Estudios Estratégicos, "La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa", *Cuadernos de Estrategia, volumen 145, número de marzo*, 2010, pp. 11-27, pp. 11-12.

[257] *Ibid.*, pp. 12-13.

[258] Arteaga Martín, Félix, "La Política Europea de Seguridad y Defensa", en Instituto Español de Estudios Estratégicos, "La Política Europea de Seguridad y Defensa (PESD) tras la entrada en

trató de colmarse con la Estrategia de Seguridad Europea (en adelante EES) de 2003[259], la cual no logró su propósito de definir los intereses de la UE y proyectar sus valores de cara al exterior dado que su incapacidad para imponer compromisos de futuro a los Estados miembros la restringió a las zonas de consenso[260]. Así, el documento se limitó a identificar como riesgos comunes el terrorismo, la proliferación de armas de destrucción masiva, el crimen organizado, los conflictos regionales y los Estados fallidos; a establecer como principios de acción en materia de seguridad y defensa ser más activos, capaces, coherentes y cooperativos; y matizar el papel de las organizaciones internacionales en la seguridad colectiva añadiendo al multilateralismo el calificativo de "efectivo", sin indicar como puede conseguirse.

En suma, aunque no constituye *stricto sensu* una estrategia de seguridad típica en el sentido de que las diferencias estratégicas entre Estados miembros le impiden definir las circunstancias en las que se puede recurrir al uso de la fuerza, decisión que depende de cada uno de los socios[261], y del gran desfase existente entre las misiones y los medios, que dependen de la voluntad y capacidad nacionales, ha de reconocerse a la EES el mérito de proclamar la vocación de la UE como actor internacional y romper con su tradición de potencia civil[262]. Por el contrario, no fue capaz de adoptar una noción comprensiva de seguridad que integrara las dimensiones externa e interna, defecto que, una vez suprimida la diferencia entre los pilares segundo y tercero tras Lisboa, ha contribuido a dejar obsoleta la EES.

No obstante, la imposibilidad de pactar una nueva EES es un ejemplo claro del anquilosamiento de la defensa europea en los últimos años. Todo lo que se ha logrado en este sentido se circunscribe a un simple ejercicio de revisión de

vigor del Tratado de Lisboa", *Cuadernos de Estrategia*, volumen 145, número de marzo, 2010, pp. 31-67, p. 33.

[259] Consejo de la Unión Europea, *op. cit., supra* (nota 132).

[260] Arteaga Martín, *op. cit., supra* (nota 258), p. 37.

[261] Heisbourg, François, "The European Security Strategy is not a Security Strategy" en Everts, Stevens y otros, *A European Way of War*, Londres, Centre for Economic Reform, 2004, pp. 27-39.

[262] Arteaga Martín, *op. cit., supra* (nota 258), p. 38.

su puesta en práctica a finales de 2008[263], cuando Francia trató de aprovechar su presidencia del Consejo para adoptar un nuevo texto acorde con los cambios en el entorno internacional y con la posibilidad de avanzar en la integración militar introducida por el Tratado de Lisboa, que ante la oposición liderada por Reino Unido no pasó de mero informe sobre la implementación de la estrategia[264]. Este documento añadió la seguridad de los sistemas de información, junto con la seguridad energética y el cambio climático, a los riesgos de seguridad identificados por la EES, pero manteniendo el interrogante acerca del papel de la defensa para afrontarlos y la aplicación limitada del uso de la fuerza[265]. En este contexto, se ha optado por elaborar estrategias de segundo nivel como la Estrategia de Ciberseguridad[266].

En línea con lo anterior, diversos factores se han apuntado para explicar la marginación de la defensa en la agenda de seguridad de la UE en los años anteriores a 2013, como la tradición neutral de algunos miembros, el desinterés de la Alta Representante por los aspectos militares, la crisis económica en la que se halla sumida Europa y que ha llevado a los gobiernos a recortar el gasto militar y la coexistencia no siempre pacífica de diferentes conceptos de seguridad y defensa en los distintos socios en función de su posición geopolítica[267]. Este último ingrediente sin duda es especialmente relevante, pues las distintas culturas estratégicas de los veintiocho Estados miembros impiden identificar los intereses estratégicos europeos comunes, así como los riesgos y amenazas compartidos. En términos de Buzan y Waeber (2003, p.

[263] Consejo de la Unión Europea, "Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección", *Diario Oficial de las Comunidades Europeas número L 345/75 de 23 de diciembre de 2008*, Unión Europea, Bruselas, 2008.

[264] Colom Piella, *op. cit., supra* (nota 254), p. 451.

[265] Arteaga Martín, *op. cit. supra* (nota 258), p. 39.

[266] Ballesteros Martín, Miguel Ángel, "La Política Común de Seguridad y Defensa tras el Consejo Europeo de Diciembre de 2013", *Documento de Análisis 03/2014*, Instituto Español de Estudios Estratégicos, Madrid, 2014 [disponible en http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA03-2014_PoliticaComunSegyDef_MABM.pdf, último acceso el 26 de junio de 2014], pp. 9-10.

[267] Colom Piella, *op. cit., supra* (nota 254), p. 451-452.

44), la UE difícilmente podría calificarse de "complejo de seguridad", caracterizados por la interdependencia entre los problemas nacionales y los colectivos de seguridad, y en ningún caso de "complejo de defensa"[268].

Efectivamente, conviven en la UE diversas culturas estratégicas o actitudes hacia el uso de la fuerza y, en general, la coerción militar como instrumento de política exterior. Mientras que, por ejemplo, Reino Unido y Francia están dispuestos a recurrir a la acción militar si es necesario para la defensa de sus intereses estratégicos, Alemania se abstiene del empleo de tales medios incluso en virtud de mandato constitucional[269]. Adicionalmente, en la cultura estratégica de los distintos Estados miembros se encuentra enraizada la actitud hacia la seguridad transatlántica y, concretamente, hacia el papel de la OTAN. En este contexto, pueden mencionarse como países tradicionalmente neutrales Austria, Chipre, Finlandia, Irlanda, Malta o Suecia; como países más afines a la OTAN Reino Unido, Holanda, Polonia, República Checa, Rumanía, Bulgaria, Estonia, Letonia o Lituania; y como países europeístas Francia o Alemania[270].

Ello explica que durante la mayor crisis que han sufrido las relaciones entre la UE y Estados Unidos con ocasión de la invasión por este último de Irak, los distintos socios optaran, en detrimento de la credibilidad de la Unión, por ganar visibilidad en la escena internacional afirmado su posición por afinidad o por contraste con el gigante norteamericano, confirmando el mito de la división geoestratégica[271] entre la "Antigua Europa" (Estados miembros fundadores partidarios de una seguridad netamente europea) y la "Nueva Europa" (Estados de posterior adhesión defensores de la seguridad trasatlántica organizada en el seno de la Alianza Atlántica, especialmente los países de Europa del Este, por lo general más "alanticistas" que los antiguos socios[272]). Esta tendencia de las potencias regionales a preferir ser los peces grandes en la pecera pequeña, en

[268] Arteaga Martín, *op. cit. supra* (nota 258), p. 41.

[269] *Ibid.*, p. 49.

[270] *Ibid.*, p. 48.

[271] Coşkun, Bezen Balamir, "Does <<strategic culture>> matter? Old Europe, New Europe and the transatlantic security", *Perceptions*, número de verano-otoño, 2007, pp. 71-90.

[272] Kovacs, Charles, "US-European Relations from the Twentieth to the Twenty-First Century", *European Foreign Affairs Journal*, volumen 8, 2003, pp. 435 y ss, p. 454.

lugar de asumir el liderazgo de una PCSD más fuerte que reclame la posición que le corresponde en la escena internacional, no se ha invertido tras el Tratado de Lisboa, como cabría haber esperado.

Precisamente la falta de liderazgo por parte de Francia y Reino Unido, más capacitados para impulsar la PCSD que Alemania -potencia económica pero muy limitada por su ordenamiento jurídico y su opinión pública en el ámbito de la defensa- se añade al elenco de razones antes expuestas para explicar esta pérdida de peso específico de la PCSD tanto en la política europea como en la resolución de los conflictos regionales, entre las que se destacaba la crisis económica y financiera y la falta de definición de los intereses europeos en una verdadera estrategia[273]. También menciona Ballesteros Martín (2014, pp. 6-8) la falta de un verdadero sistema de financiación de las operaciones con cargo a la Unión, las políticas de renacionalización que dañan la solidaridad comunitaria, el desgaste militar de la opinión pública, el desplazamiento de la tutela estadounidense hacia la región Asia-Pacífico o la ausencia de un sistema eficaz de alerta temprana que provea una capacidad de respuesta rápida como causas de que, frente a las veintitrés operaciones que la UE puso en marcha entre 2003 y 2008, sólo dos operaciones militares y tres civiles fueran lanzadas en los cinco últimos años.

6.3 CONSEJO EUROPEO DE DICIEMBRE DE 2013:

Por ello, consciente de la necesidad de incrementar la eficacia y la visibilidad de la PCSD, y en particular de solucionar las carencias de algunas capacidades críticas para la defensa, a fin de potenciar el papel de la UE como actor global, el Consejo Europeo de Bruselas celebrado en diciembre de 2012 [274] solicitó a la Alta Representante la presentación de un informe preparatorio de un Consejo Europeo dedicado a los temas de seguridad y

[273] Ballesteros Martín, *op. cit., supra* (nota 266), pp. 7-8.

[274] Consejo Europeo, *Conclusiones del Consejo Europeo de Bruselas del 13 y 14 de diciembre de 2012* [EUCO 205/12], Unión Europea, Bruselas, 2012 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/134371.pdf, último acceso el 28 de junio de 2014], p. 9.

defensa. Sobre los tres ejes fijados en diciembre de 2012, "aumento de la eficacia, visibilidad e impacto de la PCSD", "mejora del desarrollo de las capacidades de defensa" y "fortalecimiento del sector industrial europeo de la defensa"[275]. El Consejo Europeo se reunió los días 19 y 20 de diciembre de 2013 bajo la premisa de partida "la defensa es importante"[276].

Unos meses antes de la celebración de esta cumbre, Sven Biscop (2013a y 2013b), director del belga Real Instituto Egmont de Relaciones Internacionales, especuló en dos entregas del "Security Policy Brief" acerca de los asuntos a resolver por el Consejo Europeo en los planos estratégico y de capacidades respectivamente. Resulta interesante comparar sus impresiones previas con las contenidas en el número de diciembre, una vez conocidas las conclusiones de los Jefes de Estado y de Gobierno[277] para valorar los logros de una cita de la que se esperaba tanto. En lo que respecta a la agenda del Consejo Europeo, el primer gran punto esperado era la gran asignatura pendiente, tan referida en la líneas anteriores, del debate sobre la posición estratégica de Europa como "proveedor de seguridad" más allá de la vaga y obsoleta EES, es decir, la definición de las prioridades generales acerca del uso de la fuerza militar en función de los intereses vitales y las políticas exteriores de la UE y sus miembros, más allá de la cuestión coyuntural de que la operación se lleve a cabo bajo bandera de la ONU, la OTAN o la propia Unión. Y ello porque, a pesar de la diversidad de culturas estratégicas, existen intereses vitales compartidos tales como prevenir que las amenazas contra el territorio europeo se materialicen, mantener abiertas y seguras las líneas de interacción con el resto del mundo -canales, oleoductos o el mismo ciberespacio-, asegurar el abastecimiento de recursos energéticos para la economía, controlar los flujos migratorios, mitigar el impacto del cambio climático, fortalecer el Derecho

[275] *Ibid.*, p. 10.

[276] Consejo Europeo, *Conclusiones del Consejo Europeo de Bruselas del 19 y 20 de diciembre de 2013* [EUCO 217/13], Unión Europea, Bruselas, 2013 [disponible en http://consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/140263.pdf, último acceso el 28 de junio de 2014], p. 1.

[277] Biscop, Sven y Coelmont, Jo, "Defence, The European Council Matters", *Security Policy Brief 51*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013.

internacional como fundamento de la estabilidad global y preservar la autonomía del proceso de toma de decisiones de la UE frente a la dependencia de potencias externas[278].

La identificación de prioridades estratégicas es el *prius* lógico de un segundo asunto a tratar en el orden del día, el desarrollo de una capacidad de planificación defensiva al servicio de dichas prioridades que se integre con el Proceso de Planificación Defensiva de la OTAN y que armonice las planificaciones defensivas nacionales de los Estados miembros evitando duplicidades y respetando al mismo tiempo los distintos niveles de desarrollo de las mismas sobre el camino marcado por el proceso de Gante. Esta iniciativa germano sueca respaldada por el Consejo de Ministros de Defensa de 2010 fue la carta de naturaleza del enfoque *pooling and sharing* o "mancomunar y compartir"[279], consistente en crear sinergias entre Estados miembros poniendo capacidades militares en común y repartiendo roles y tareas en los ámbitos de la armonización de requisitos militares, investigación y desarrollo, entrenamiento y ejercicios, estructuras y procedimientos de mando y costes operativos, todo ello en el marco y con el apoyo de la Agencia Europea de Defensa[280].

Finalmente, un tercer aspecto a discutir por el Consejo Europeo, necesario punto de conexión entre el nivel político de las prioridades estratégicas y el operativo de la planificación defensiva, era la definición del nivel de ambición deseado, entendiendo por tal el objetivo de fuerzas militares desplegables en misiones de gestión de crisis a conseguir mediante planes de desarrollo de capacidades y sus mecanismos periódicos de revisión. El Objetivo de Helsinki de 1999 fijó el nivel de ambición para misiones expedicionarias en una Fuerza

[278] Biscop, "And What Will Europe Do? The European Council and Military Strategy", *Security Policy Brief 46*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013, p. 2.

[279] Yaniz Velasco, *op. cit., supra* (nota 135), p. 12.

[280] Gobierno de la República Federal Alemana y Gobierno del Reino de Suecia, "European Imperative, Intensifying Military Cooperation in Europe", *Food for Thought of November 2010*, República Federal Alemana y Reino de Suecia, Berlín y Estocolmo, 2010 [disponible en http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260511deseinitiative_/sede260511deseinitiative_en.pdf, ultimo acceso el 28 de junio de 2014].

Europea de Reacción Rápida compuesta por 60.000 efectivos con una autonomía operativa de 60 días, objetivo que no se logró en la fecha prevista de 2003[281], decidiendo el Consejo Europeo de Bruselas de 2004 un nuevo *headline goal* para 2010 con el objetivo declarado de responder con una acción rápida y decisiva se localiza en cualquier nivel de la gama de operaciones de gestión de crisis cubiertas por el TUE[282].

Este enfoque comprensivo es precisamente el que Biscop (2013a, p. 2) reclamaba para la UE en vísperas del Consejo Europeo de diciembre de 2013, advirtiendo que una estrategia militar comprende (a) la prevención, manteniendo una presencia destacada en las áreas prioritarias, (b) la disuasión, proyectando una imagen de poder creíble y sostenible, y (c) todo el espectro de misiones de gestión de crisis, incluido el uso de la fuerza si y sólo si la prevención y la disuasión fracasan. A este respecto, el apoyo político por parte de los demás socios a la intervención francesa en Malí es indicativo de una mayor conciencia de la necesidad de que Europa se ocupe de gestionar las crisis de su entorno más próximo -sea en el marco de la PCSD, la OTAN o coaliciones *ad hoc*- ante la pérdida de interés estratégico del Viejo Continente para los Estados Unidos. Esta coyuntura era aparentemente idónea para un primer acuerdo entre los Jefes de Estado y de Gobierno sobre las regiones y tipos de contingencias respecto de los cuales los Estados miembros estarían dispuestos a asumir responsabilidad[283].

Presentados los elementos de juicio, procede ahora aplicarlos a las conclusiones de la cumbre de diciembre de 2013 para extraer conclusiones

[281] Arteaga Martín, *op. cit., supra* (nota 258), p. 43.

[282] Dirección General de Políticas Externas de la Unión del Parlamento Europeo, *Note of 12 September 2006 on the European Security and Defence Policy. From the Helsinki Headline Goal to the EU Battlegroups*, Parlamento Europeo, Unión Europea, Bruselas, 2006 [disponible en http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede030909notaesdp_/sede030909noteesdp_en.pdf, ultimo acceso el 28 de junio de 2014], p. 16.

[283] Biscop, Sven, "Pool it, Share it, Use it: The European Council on Defence", *Security Policy Brief 44*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013, p. 4 y 5.

sobre el estado de la defensa en Europa. En este sentido, deben destacarse siete avances clave[284]:

a) El primer el logro es que la defensa haya vuelto a la agenda de la más alta instancia política de la UE en la forma de un proceso tutelado por el Consejo Europeo, que "evaluará los avances concretos en todas las materias en junio de 2015"[285].
b) Hay que destacar también el papel que se otorga en este proceso a la Comisión, destinataria de peticiones varias concretas y en general de la invitación a tomar dentro de su ámbito de competencia "medidas decididas y comprobables para poner en práctica las orientaciones antes expuestas"[286], lo cual indica la adopción de un enfoque comprensivo cívico-militar que integra los aspectos internos y externos de la seguridad, implicando el ejercicio de competencias de lógica comunitaria junto a las intergubernamentales propias de la PCSD.
c) Al instar a la Agencia Europea de Defensa "a que estudie maneras en las que los Estados miembros puedan cooperar de manera más eficaz y eficiente en proyectos de contratación agrupada, con miras a volver a informar al Consejo para finales de 2014", el Consejo Europeo respalda el sistema de *pooling and sharing*, buscando siempre la sinergia y la complementariedad con la *Smart Defence* de la Alianza[287]. Este enfoque es ilustrado por Biscop y Coelmont (2013, p.2) mediante el ejemplo de la integración naval belga-neerlandesa, en el que la puesta en común de capacidades militares ha permitido conciliar la especialización con la máxima soberanía y flexibilidad.
d) Sin embargo, la garantía de que este mosaico de grupos de socios que comparten capacidades se traduzca en una mejora coherente de las capacidades a nivel de la UE requiere "una mayor transparencia y la puesta en común de la información en la planificación de la defensa", a efectos de

[284] Biscop y Coelmont, *op. cit., supra* (nota 277).

[285] Consejo Europeo, *op. cit., supra* (nota 274), párrafo 22.

[286] Consejo Europeo, *Ibid.*

[287] Ballesteros Martín, *op. cit., supra* (nota 266), p. 13.

permitir “a los planificadores y responsables nacionales estudiar una mayor convergencia de las necesidades y plazos de disponibilidad de capacidades”, para lo cual se insta a la Alta Representante y a la Agencia Europea de Defensa “a presentar antes de finales de 2014 el oportuno marco político en plena coherencia con los procesos de planificación vigentes de la OTAN”[288]. Se trata de colmar la brecha de estructuras de planificación entre los niveles nacionales y respecto de la Alianza Atlántica, posponiendo una vez más el desarrollo de una capacidad de planificación autónoma al margen de esta organización y obviando referirse al siempre pendiente y controvertido cuartel general europeo.

e) En el plano estratégico destaca la esperable incapacidad del Consejo Europeo para abordar la definición del papel de Europa como proveedor de seguridad, definiendo sus prioridades, nivel de ambición y áreas geográficas de responsabilidad, en parte porque se trata de una cuestión política que excede del ámbito estricto de la PCSD al que se ceñía la cumbre. En este ámbito, los Jefes de Estado y de Gobierno se limitaron a invitar a la Alta Representante en cooperación con la Comisión a evaluar “la incidencia de los cambios del entorno mundial e informe al Consejo en el transcurso de 2015 sobre los desafíos y las oportunidades que se ofrezcan a la Unión, una vez consultados los Estados miembros”, petición que puede interpretarse como el mandato para la elaboración de una nueva estrategia de seguridad.

f) En materia de ciberdefensa, el Consejo Europeo se congratula del “desarrollo de un plan de trabajo y unos proyectos concretos centrados en la instrucción y los ejercicios”, de la “mejora de la cooperación civil-militar sobre la base de la Estrategia de Ciberseguridad de la UE” y de “la protección de los recursos en las misiones y las operaciones de la UE”[289], solicitando “un marco político de la UE para la ciberdefensa en 2014, a partir de una propuesta de la Alta Representante en cooperación con la

[288] Consejo Europeo, *op. cit., supra* (nota 274), párrafo 12.

[289] Consejo Europeo, *op. cit., supra* (nota 274), párrafo 11.

Comisión y la Agencia Europea de Defensa", siempre "de manera coherente con los esfuerzos de la OTAN"[290].

g) Por último, se hace un gran énfasis en la necesidad de desarrollar una base industrial y tecnológica de la defensa competitiva, innovadora, sostenible e integrada, abordando la omnipresente preocupación por situación de crisis económica desde el sector armamentístico. En esta materia, se hace énfasis en la redacción de estándares específicos europeos para productos y aplicaciones militares, encomendándose a la Agencia Europea de Defensa y la Comisión preparar "un programa de trabajo para desarrollar normas industriales de defensa antes de mediados de 2014"[291].

En conclusión, el gran logro del Consejo Europeo de diciembre de 2013 fue devolver la defensa al primer plano de la UE, tanto a las Instituciones como a los gobiernos nacionales y a la opinión pública, proporcionándole así a la PCSD la visibilidad que se proponía. No obstante, evitó cuestiones esenciales como el desarrollo de una capacidad de planificación defensiva autónoma del Proceso de Planificación Defensiva de la OTAN y aplazó otras como la definición de una nueva estrategia de seguridad. Al contrario, optó por primar el enfoque realista de los pequeños pasos, animando la compartición de capacidades militares por grupos de Estados miembros a través del *pooling and sharing*, geometría variable por la que también parece decantarse el Tratado de Lisboa al apostar por la Cooperación Estructurada Permanente. Esta PCSD a la carta presenta la ventaja de respetar las culturas estratégicas y las capacidades existentes de los distintos socios, así como el inconveniente de depender excesivamente de que las potencias regionales como Francia o Reino Unido se comprometan con la integración y asuman el liderazgo que no han asumido hasta el presente.

[290] Consejo Europeo, *op. cit., supra* (nota 274), párrafo 9.

[291] Consejo Europeo, *op. cit., supra* (nota 274), párrafo 19.

7 COOPERACIÓN ENTRE LA UE Y LA OTAN:

7.1 ESTADO ACTUAL DE LAS RELACIONES TRANSATLÁNTICAS:

Para ofrecer una imagen fiel de la relación entre UE y OTAN es indispensable partir de una descripción del panorama más amplio en el que aquélla se encuadra a cuya tectónica obedece, el de las relaciones transalánticas, entendidas como la suma de relaciones de cooperación en un amplio espectro de materias, que comprende la economía, la política, la ciencia e incluso la defensa, entre Europa y Norte América, a menudo concebidas como la interacción de Estados Unidos y la UE[292], valga esta simplificación a los efectos del presente estudio. Especialmente tras la quiebra del modelo de división del trabajo propio de la Guerra Fría, se ha visto influida de forma decisiva por las estrategias de seguridad de Washington como única superpotencia y autoproclamado líder estratégico global.

Ante todo, las relaciones transatlánticas se asientan en un conjunto de valores compartidos procedentes de la Ilustración, tales como la libertad, la igualdad, la tolerancia, el respeto al individuo o la participación, que definen la democracia, así como la idea del capitalismo como mejor sistema económico y organización de la convivencia nacional e internacional[293]. Precisamente, la OTAN surge de la voluntad de proteger este *ethos* común cuando en la posguerra mundial se veía amenazado por la concepción soviética alternativa del Derecho, la economía y la política. La consecuencia de esta deriva histórica es la tutela estadounidense sobre Europa en lo que respecta a la defensa territorial durante la Guerra Fría, periodo durante el cual la doctrina estratégica de la Casa Blanca consideraba el control de la seguridad en ambas orillas del Atlántico como un requisito indispensable para su propia seguridad y sus socios europeos occidentales necesitaban la ayuda norteamericana para su

[292] Reichard, *op. cit., supra* (nota 84), p. 24.

[293] Marsal Muntala, Jordi, “Las relaciones transatlánticas”, en Instituto Español de Estudios Estratégicos, La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa, *Cuadernos de Estrategia*, volumen 145, número de marzo, 2010, pp. 174-204, p. 175 y 176.

propia supervivencia[294]. En suma, mientras persistió la tensión entre bloques, defensa europea fue sinónimo de defensa atlántica[295].

Sin embargo, tras la caída del Telón de Acero, el factor exógeno representado por el inicio de un panorama geoestratégico muy distinto, en el que Europa debió comenzar a responsabilizarse de la seguridad y la defensa al menos de su área de influencia, coincidió con el factor endógeno de la creciente divergencia entre las prioridades de seguridad de Europa y Estados Unidos y sus percepciones acerca de los intereses vitales a proteger[296].

En los albores del nuevo milenio, Estados Unidos había dejado de ser el "benevolente hegemón" [297] bajo cuya protección Europa alcanzó una prosperidad y un estilo de vida comparables a los de la otra orilla del Atlántico y su foco estratégico se desplazaban hacia los incipientes mercados asiáticos y los nuevos desafíos a la seguridad internacional, tales como los Estados fallidos y "canallas", la proliferación de armas de destrucción masiva y el terrorismo internacional, dejando un Viejo Continente "entero y libre" y en paz[298], forzado y dispuesto a postularse como actor global. Y precisamente esta fase de transición caótica de un mundo bipolar westfaliano, con reglas establecidas, a un orden distinto, si unipolar o multipolar no está claro, una fase caracterizada por la aparición de nuevos actores no estatales y amenazas a la seguridad y en la que potencias emergentes, como China, o reemergentes, como Rusia, disputan su hegemonía a los núcleos de poder tradicionales, es el momento en que los actores internacionales pueden y deben definir cuál va a ser su papel futuro en función de su voluntad y su ambición[299].

[294] Link, Werner, "Die NATO im Gefl echt internationaler Organisationen", *Aus Politik und Zeitgeschichte*, volumen 49, número 11, 1999, p. 9 y ss., p. 10.

[295] Haine, Jean-Yves y Gnesotto, Nicole (eds.), *ESDP - The first five years (1999-2004)*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2004, p. 131.

[296] Asmus, Blackwill y Larrabee, Ronald, Blackwill, Robert y Larrabee, Stephen, "Can NATO Survive?", *The Washington Quarterly*, volumen 19, número 2, 1996, p. 79 y ss., p. 88.

[297] Kovacs, *op. cit., supra* (nota 272), p. 445.

[298] Reichard, *op. cit., supra* (nota 84), p. 22.

[299] Marsal Muntala, *op. cit., supra* (nota 293), p. 182.

Aunque el primer paso en este sentido -la institución de la PESC en 1992- dibujó a la UE como una potencia civil, las solas capacidades basadas en el *soft power* se mostraron desde el principio insuficientes, evidenciándose la necesidad de dotarse de mayores instrumentos militares, cuando la incapacidad de la UE para valerse por sí misma durante las Guerras de los Balcanes y especialmente en la crisis de Kosovo de 1999 obligó a la intervención de la OTAN para poner fin al conflicto[300]. Desde entonces, la Unión emprendió el camino hacia un enfoque integral de la seguridad que, combinando los medios civiles con los militares, se ha mostrado el más adecuado para la gestión de crisis en el nuevo siglo y que acaso la lleve a convertirse en una suerte de "potencia posmoderna"[301] distinta a todas las que han existido hasta el momento, cuyos atributos de poder no se fundan exclusivamente en la dimensión diplomática y militar.

En cualquier caso, la toma de conciencia de la necesidad de complementar la arquitectura de seguridad de la UE con una capacidad de defensa autónoma de la OTAN se tradujo en el "proceso de Saint Malo", iniciado por Reino Unido y Francia en la cumbre celebrada en 1998 en la ciudad bretona homónima y respaldado por el Consejo Europeo de Colonia del año siguiente. Este germen de la PESD contó desde el principio con el apoyo de Estados Unidos[302], consciente de la conveniencia de convertir a su socio transatlántico en un aliado útil para la defensa de los valores e intereses comunes, pero a la vez produjo en Washington un cierto temor a que una Europa dotada medios militares suficientes pudiera cuestionar el liderazgo norteamericano e incluso convertirse en un competidor para sus intereses geopolíticos[303], que finalmente se tradujo en una cierta tensión en el seno de la Alianza Atlántica y de las propias Comunidades.

[300] *Ibid.*, pp. 177 y 183-184.

[301] Ortega, Andrés, "Año de siembra en un cruce de siglos", *Anuario Internacional del Centro de Información y Documentación Internacionales en Barcelona*, 1997, pp. 15-26, p. 17.

[302] Reichard, *op. cit., supra* (nota 84), p. 67.

[303] Marsal Muntala, *op. cit., supra* (nota 293), p. 186.

Ciertamente, Estados Unidos no se opuso al desarrollo de una capacidad militar de la UE, siempre que la OTAN siguiera siendo "la organización vital para la seguridad europea[304], condición plasmada por la Secretaria de Estado Madeleine Albright en sus famosas "tres Ds" [305] -no duplicación de las estructuras de la Alianza en la PESD, no discriminación de los aliados no miembros de las Comunidades y no desacoplamiento por parte de la Unión de las estructuras de la OTAN-. Lejos de reprimir el inevitable y necesario desarrollo de la defensa europea, trató de conciliarlo con la primacía de la Alianza, acomodándolo en el seno de ésta en la forma de una Identidad Europea de Seguridad y Defensa (en adelante IESD), a modo de pilar europeo de la OTAN introducido en las cumbres del Consejo del Atlántico Norte de Bruselas, en 1994, y Berlín, en 1996[306]. De este modo, Saint Malo representó en realidad un compromiso entre la potencia "atlantista" europea por excelencia, el Reino Unido, que impulsaba la institución de una política de seguridad y defensa de la UE, y su contraparte "europeísta", Francia, que aceptaba el papel de la Alianza en este proceso[307]. Sobre este punto se volverá en el siguiente epígrafe desde el punto de vista de la relación entre UE y OTAN.

Pero, sin lugar a dudas, el verdadero punto de ruptura en las relaciones transatlánticas se produjo con ocasión de la invasión de Irak por Estados Unidos, alegando que la posesión por la república árabe de armas biológicas y químicas prohibidas susceptibles de ser usadas en un ataque o entregadas a grupos terroristas[308] justificaba una intervención en ejercicio de la legítima

[304] Krenzler y Schomaker, Horst y Schomaker, Astrid, "A new Transatlantic Agenda, European Foreign Affairs Review", *European Foreign Affairs Review*, número 1, 1996, pp. 9-28, p. 11.

[305] Albright, Madeleine, "The Right Balance Will Secure NATO's Future", *Financial Times*, 7 de diciembre, 1998, p. 22.

[306] Reichard, *op. cit., supra* (nota 84), 149-150.

[307] Gnesotto, Nicole (ed.), *Política de Seguridad y Defensa de la Unión Europea*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2004.

[308] Stevenson, Richard, "Remember <<Weapons of Mass Destruction>>? For Bush, They Are a Nonissue", *The New York Times*, 18 de diciembre, 2003.

defensa preventiva[309]. Esta acción difícilmente amparada por el *ius ad bellum* puso de manifiesto, en su máxima expresión alcanzada durante la administración Bush, la aproximación de *hard power* de la estrategia de seguridad americana, basada en la superioridad militar, el unilateralismo y la disposición a hacer uso de la fuerza, incluso de forma preventiva y al margen del Derecho internacional, para proteger sus intereses. Este enfoque, arraigado en opinión de Kagan (2002) en una concepción antropológica que lleva a los americanos a creer en la necesidad del poder en un mundo lejos de ser perfecto y conduce a una noción moderna o hobbesiana de las relaciones internacionales, se opone a la visión posmoderna predominante en la UE, que afronta la seguridad desde el *soft power* o *humanitarian power*, de naturaleza predominantemente civil y comprensiva, confiando en instrumentos económicos, políticos y diplomáticos, junto a los militares, para combatir no sólo las amenazas, sino también sus causas. Esta diferencia de cultura estratégica fue caricaturizada en pleno *impasse* transatlántico por el propio Kagan (2003) al afirmar que los americanos son de Marte y los europeos de Venus.

La "brecha de percepción"[310], que alcanza su clímax en 2003, comienza a manifestarse tras los ataques del 11 de septiembre de 2001, ante los cual Washington reaccionó sumiéndose en una situación de alerta caracterizada por un unilateralismo de tintes moralistas[311] y en la que el uso de la fuerza estaba justificado por un permanente estado de legítima defensa que le confería un estatuto permanente de excepción respecto al Derecho internacional [312],

[309] Ver La Casa Blanca, *op. cit., supra* (nota 63), p. 15, aunque la expresión utilizada sea "preemptiva", debe traducirse por "preventiva" de acuerdo con los conceptos explicados en el primer apartado de este trabajo.

[310] En palabras del entonces Secretario General de la OTAN Jaap de Hoop Scheffer, citado por Hoge, Warren, "NATO Chief criticizes terror <<gap>>", *International Herald Tribune*, 12 de noviembre, 2004.

[311] Reichard, *op. cit., supra* (nota 84), p. 39.

[312] Gnesotto, Nicole, "Visions of the other", en Lindstrom, Gustav (ed.), *Shift or Rift: Assessing US-EU relationships after Iraq*, París, Instituto de Estudios de Seguridad de la Unión Europea, 2003, pp. 7 y ss., p. 26.

mientras que en el otro lado del atlántico el terrorismo se abordó como un fenómeno de profundas raíces políticas y sociales y no se tuvo verdadera conciencia del trauma experimentado por Estados Unidos y la seriedad de su declaración de guerra al terrorismo[313]. De este modo, por un lado, los europeos no reconocían a la América que previamente habían conocido [314], decepcionados por la actitud de ésta, y, por otro lado, los norteamericanos se sorprendieron a su vez de la apatía europea[315].

Esta profunda crisis también desencadenó tensiones internas en la UE, confirmando que las discusiones más virulentas acerca de las relaciones transatlánticas no se producen entre ambos lados del océano, sino entre los propios Estados miembros[316], concretamente entre los que se opusieron a la invasión de Irak, notablemente Francia y Alemania, y los que prestaron su apoyo a la llamada *coalition of the willing* -"coalición de los dispuestos"-[317], mayoritariamente de tradición "atlantista", como son Reino Unido, Países Bajos, Dinamarca, Portugal e Italia, así como España, en otras ocasiones más comprometida con la causa "europeísta", y los países de la ya referida "Nueva Europa", en la víspera de su adhesión, a saber, Bulgaria, República Checa, Hungría , Letonia, Lituania, Polonia, Rumanía y Eslovaquia. En este contexto, Alemania, Francia, Bélgica y Luxemburgo reabrieron en junio de 2003 el debate aun sin resolver, que será tratado con mayor profundidad en el epígrafe siguiente, acerca del establecimiento de un Cuartel General de la UE autónomo de la OTAN en la localidad belga de Tervuren[318].

[313] Reichard, *op. cit., supra* (nota 84), pp. 39 y 40.

[314] Gnesotto, *op. cit., supra* (nota 312), p. 37.

[315] Gompert, David, "What does America want of Europe?" , en Lindstrom, Gustav (ed.), *Shift or Rift: Assessing US-EU relationships after Iraq*, París, Instituto de Estudios de Seguridad de la Unión Europea, 2003, p. 56 y ss., p. 56.

[316] Salmon, Trevor y Shepherd, Alistair, *Towards a European Army - A Military Power in the Making?*, Boulder, Colorado, Lynne Rienner Publishers, 2003, p. 174.

[317] Schifferes, Steve, "US names <<coalition of the willing>>", *BBC News Online*, 18 de marzo, 2003 [disponible en http://news.bbc.co.uk/2/hi/americas/2862343.stm, último acceso el 30 de junio de 2014].

[318] Marsal Muntala, *op. cit., supra* (nota 293), p. 190.

No obstante, a pesar de las diferencias de valores e intereses entre Estados Unidos y las potencias europeas, que unida a la negativa de algunas de éstas a asumir el liderazgo norteamericano ha convulsionado la frágil unidad de la OTAN y de la UE, así como las relaciones entre las mismas, parece claro que ambos lados del Atlántico están abocados a seguir siendo socios, pues conforman lo que Deustch (1957, p. 5) llama una "comunidad de seguridad", entendida como un grupo de Estados con prácticas y expectativas comunes mantenidas a lo largo del tiempo de manera que, aunque pueden presentar diferencias políticas, la guerra entre ellos ha quedado descartada.

En definitiva, la mutua necesidad de ambos socios transatlánticos -que, a pesar de sus divergencias, comparten un sistema de valores e intereses más homogéneo que con cualquier otro actor geoestratégico- y el cambio de centro de atención y recursos de Estados Unidos hacia otras regiones del globo propician la deriva hacia un nuevo equilibrio transatlántico para el cual Reichard (2006, pp. 43-47) propone tres posibles esquemas: (a) Si la UE adoptara el rol que le corresponde como actor global, sería posible un reparto del poder más equitativo entre ambos, asumiendo Europa una mayor responsabilidad sobre su propia seguridad, mientras que Washington conservaría la tutela sobre la capacidad defensiva europea a través de la OTAN, oponiéndose a una capacidad de planificación de la Unión independiente de la Alianza. (b) Otra alternativa es que las potencias regionales europeas diseñen de forma independiente su política de defensa según su postura hacia el liderazgo estratégico global estadounidense, quedando la OTAN como un instrumento militar de apoyo a las coaliciones que de este juego resulten. (c) Finalmente, es posible consensuar una nueva asociación transatlántica que institucionalice la tendencia hasta ahora seguida por la PCSD hacia una división del trabajo en la que Europa haga las veces de *soft power*, función más acorde con su capacidad militar y con sus prioridades políticas, mientras que Estados Unidos se mantendría como *hard power* y seguiría siendo un respaldo estratégico necesario para el papel de la UE, de manera que éste actuaría en los momentos iniciales de los conflictos y aquélla se encargaría de la fase de estabilización posterior.

En cualquier caso, es evidente que el nuevo marco de relaciones transatlánticas debe partir de la definición clara de los intereses y prioridades de ambos socios, siempre obstaculizada por las divergencias estratégicas entre Estados miembros, incapaces de adoptar una actitud coherente que acoja el viraje experimentado en los últimos años por la política exterior estadounidense[319]. En efecto, durante la administración Obama, la visión geoestratégica "excepcionalista" de la superpotencia norteamericana propia del neoconservadurismo del gobierno de Bush se ha visto limitada y, con ello, la percepción de su papel en el mundo ha oscilado del idealismo sólo preocupado por la imposición unilateral de la paz al realismo consciente de la importancia de estabilizar y de la función que otros actores pueden desempeñar a este respecto[320].

Este giro hacia cierto multilateralismo efectivo, como el propugnado por la EES, ha propiciado el acercamiento de las agendas de ambos socios transatlánticos y así se ha plasmado en las últimas cumbres euro-estadounidenses de 2010, 2011 y 2014. En materia de ciberseguridad, sin embargo, la cuestión se ha tratado desde la óptica civil, manteniéndose cierta ambigüedad en relación con la dimensión de ciberdefensa, seguramente por la conciencia de que la disposición de la Casa Blanca a hacer uso unilateral de la fuerza continúa siendo también en el ámbito del ciberespacio el gran punto de ruptura con Europa. Así, con ocasión de la cumbre celebrada en Lisboa en 2010 se estableció un Grupo de Trabajo sobre Ciberseguridad y Cibercrimen[321] y en la última, que tuvo lugar en marzo de 2014, la ciberseguridad se volvió a tratar desde la perspectiva del *law enforcement*, haciéndose referencia a diversas iniciativas en relación con la gobernanza de Internet[322] y sólo

[319] *Ibid.*, p. 191.

[320] *Ibid.*, p. 192-193.

[321] Consejo de la Unión Europea, *EU-US Summit Joint Statement of 20 November 2010* [16726/10 PRESSE 315], Unión Europea, Lisboa, 2010 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/117897.pdf, último acceso el 1 de julio de 2014], p. 3.

[322] Servicio Europeo de Acción Exterior, *EU-US Summit Joint Statement of 26 March 2014* [140326/02], Unión Europea, Bruselas, 2014 [disponible en

mencionándose en el ámbito de la defensa a propósito de los avances del Consejo Europeo de diciembre de 2013 en materia de PCSD, entre los desafíos emergentes a la seguridad en relación con los cuales las partes declaran que continúan trabajando para fortalecer la cooperación entre UE y OTAN[323], pero nuevamente utilizando el término "ciberseguridad" para evitar prejuzgar un enfoque militar.

Por lo tanto, en el quinto dominio, como en todos los demás ámbitos, aunque la posición de Estados Unidos se ha moderado, su cultura estratégica tendente a anteponer sus intereses políticos al estricto respeto del Derecho internacional y, en particular, del *ius ad bellum* sobre la base de consideraciones más morales que jurídicas, así como su enfoque preponderantemente militar de la seguridad seguirán siendo un obstáculo al menos en el futuro próximo a la cooperación entre ambos lados del Atlántico en materia de defensa y, en concreto, de ciberdefensa. Un ejemplo muy ilustrativo es el llamado "Plan X" elaborado por la división del Pentágono conocida como *Defense Advanced Research Projects Agency* (en adelante DARPA) y cuyo objetivo es el desarrollo de una capacidad militar que permita lanzar ofensivas cibernéticas[324], traspasando así los límites de la mera ciberdefensa. El hecho de que el socio transatlántico parezca dispuesto a pasar al ataque en caso de ser necesario, como ponen de manifiesto las filtraciones que revelan la reunión secreta del Presidente Obama con sus asesores jurídicos acerca de la posibilidad de autorizar ciberataques "preemptivos"[325], resulta difícilmente aceptable para la mayoría de los Estados miembros.

http://www.eeas.europa.eu/statements/docs/2014/140326_02_en.pdf, último acceso el 1 de julio de 2014], p. 5.

[323] *Ibid.*, p. 9.

[324] Nakashima, Ellen, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace", *The Washington Post*, 30 de mayo, 2012 [disponible en http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html, ultimo acceso el 1 de julio de 2014].

[325] Sanger, David y Shanker, Thom, "Broad Powers Seen for Obama in Cyberstrikes", *The New York Times*, 3 de febrero, 2013 [disponible en http://www.nytimes.com/2013/02/04/us/broad-

En conclusión, aunque tanto Estados Unidos como la UE parecen estar de acuerdo en reconocer que el ordenamiento jurídico internacional debe ser adaptado a las nuevas amenazas dinámicas y que, de hecho, se está transformando en un "orden de valores" en el cual los principios "constitucionales" como la prohibición del uso de la fuerza no son absolutos, sino que coexisten con otros valores fundamentales que los modulan -justificando por ejemplo las intervenciones humanitarias-, el enfoque unilateral y anticipatorio norteamericano sigue siendo difícil de reconciliar con el multilateralismo efectivo europeo[326]. Está por ver si esta discrepancia será salvada por la voluntad de ambos socios, conscientes de que comparten un núcleo esencial de valores e intereses que deben ser defendidos frente a amenazas comunes, y si para ello será preciso recalibrar el equilibrio de poder en la relación transatlántica y en su espina dorsal, la relación entre la UE y la OTAN, objeto de discusión a continuación.

7.2 ESTADO ACTUAL DE LAS RELACIONES ENTRE UE Y OTAN:

Las anteriores reflexiones han dejado una conclusión clara, el mundo aparentemente unipolar de la Posguerra Fría está dejando paso a una escena internacional multipolar en la que, si bien hablar de mundo "postamericano"[327] o caída del imperio americano es tal vez ir demasiado lejos, lo cierto es que la superpotencia es incapaz de mantener su hegemonía y debe priorizar, centrando sus esfuerzos geoestratégicos en otros puntos del globos y dejando de lado a la relación atlántica como su relación preferente[328]. En consonancia con estos cambios, la UE debe modificar sus prioridades abandonado la égida norteamericana y repartiéndose de forma más equitativa con la OTAN la responsabilidad y los costes de la seguridad de Europa. Por su parte, Estados

powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0, ultimo acceso el 1 de julio de 2014].

[326] Herdegen, Matthias, "Military intervention matter of dispute in transatlantic relations", *Revista Colombiana de Derecho Internacional*, número 10, 2007, pp. 199-208, p. 204 y 205.

[327] Shapiro, Jeremy y Witney, Nick, *Towards a Post-American Europe: a power audit of EU-US Relations*, European Council on Foreign Relations, 2009.

[328] Marsal Muntala, *op. cit., supra* (nota 293), p. 196.

Unidos, envuelto en una sustancial reducción de su presupuesto militar, parece más dispuesto que nunca al desarrollo de una PCSD efectiva y eficiente que, aunque respetando la primacía de la OTAN, comparta los gastos de la defensa europea como un "proveedor" y no un "consumidor" de seguridad[329].

7.3 MARCO JURÍDICO-POLÍTICO PARA LA COOPERACIÓN ENTRE UE Y OTAN:

A nivel oficial, aunque los gobiernos nacionales se han mantenido escépticos en relación con la excesiva institucionalización de la relación entre OTAN y UE que pudiera reducir su margen político de maniobra[330], la grave amenaza a la seguridad europea constituida por la crisis que azotó el oeste de los Balcanes desde principios de la década de los noventa provocó un cambio de actitud en los sectores más reticentes hacia una forma institucionalizada de asociación[331]. En este contexto, la relación institucional de la UE con la OTAN, si bien la posibilidad fue ya contemplada por la mencionada Declaración de la UEO de 1996[332], se remonta a finales de los años noventa, cuando la creación de la PESD y la asunción por la UE de las competencias de la UEO en materia de gestión de crisis[333] en el Tratado de Ámsterdam, evidenció la imposibilidad de eludir una forma de cooperación directa entre las dos organizaciones internacionales de seguridad en el largo plazo.

[329] Coelmont, Jo y De Langlois, Maurice, "Recalibrating CSDP-NATO Relations : The Real Pivot", *Security Policy Brief 47*, Real Instituto Egmont de Relaciones Internacionales, 2013, p. 2.

[330] Kulich, Stanislav, "The concept of division of labour between the EU and NATO: An elusive search for an optimal partition of security tasks", Trabajo de Fin de Máster, King's College, Universidad de Londres, Reino Unido, p. 8.

[331] *Ibid.*, p. 14.

[332] Dehousse, Franklin y Galer, Benoît, "De Saint-Malo a Feira: les enjeux de la renaissance du projet de defense européenne", *Studia Diplomatica*, volumen 52, número 4, Bruselas, 1999, p. 32.

[333] Möttölä, Kari, "Collective and co-operative security arrangements in Europe", en Koskenniemi, Martti (ed.), *International Law Aspects of the European Union*, La Haya, Kluwer Law International, 1998, pp. 87-98, p. 96.

Los encuentros informales entre el Secretario General de la Alianza Robertson y el Alto Representante Solana desde 1999, que dieron como fruto al año siguiente el acuerdo provisional relativo a la Seguridad de la Información entre la Secretaría General del Consejo y la OTAN, fueron la primera piedra de la conexión oficial entre la UE y la OTAN[334], planteándose la institucionalización permanente a finales de 1999 por el propio Solana y Vershbow[335], embajador de Estados Unidos ante la OTAN. Este movimiento de Washington, que recientemente había dejado atrás su ambigüedad al respecto para apoyar abiertamente la PESD[336], fue visto por algunos Estados miembros de la UE, entre ellos Francia, como una amenaza para la recién nacida política de defensa, que se desarrollaría a imagen de la ya madura Alianza y, en última instancia, bajo la influencia de la superpotencia americana[337]. A pesar de ello, el canje de cartas entre la OTAN y la Presidencia sueca de la UE de 24 de enero de 2001, considerada la carta de naturaleza de la cooperación institucional entre ambas organizaciones internacionales, acordó que el COPS y el CAN se reunieran al menos tres veces cada semestre por debajo del nivel ministerial y al menos una a nivel de ministros, siendo la primera sesión en 30 de mayo de 2001[338]. Este intercambio de misivas de gran peso político en lo relativo a la definición del ámbito de la cooperación y las modalidades de consulta acerca de asuntos de seguridad, cuya naturaleza de tratado internacional vinculante en Derecho internacional es descartada por Reichard (2006, p. 354) tras un análisis jurídico pormenorizado[339], pone de manifiesto la aversión a asumir obligaciones jurídicas como nota características de las relaciones entre la UE y la OTAN.

[334] Reichard, *op. cit., supra* (nota 84), p. 123.

[335] Levasseur, Alain y Scott, Richard, *The Law of the European Union: A New Constitutional Order: Materials and Cases*, Durham, Carolina del Norte, Carolina Academic Press, 2001, p. 1028.

[336] Howorth, Jolyon, *European integration defence: the ultimate challenge?*, París, Instituto de Estudios de Seguridad de la Unión Europea Occidental, 2000, p. 56.

[337] *Ibid.*, p. 56.

[338] Salmon y Shepherd, *op. cit., supra* (nota 316), p. 175.

[339] Para el análisis completo ver Reichard, *op. cit., supra* (nota 84), pp. 128-144.

La misma naturaleza meramente política tiene la piedra angular de la relación formal entre ambas organizaciones internacionales, el acuerdo sobre cooperación y seguridad internacional anunciado en la Declaración UE-OTAN[340] sobre la PESD de 16 de diciembre de 2002 comúnmente denominado acuerdo Berlín Plus[341]. No obstante, aunque lo considera desprovisto asimismo de fuerza vinculante *per se*, Reichard (2006, pp. 305-311) entiende que el acuerdo Berlín Plus puede dar lugar a obligaciones jurídicas para la Alianza y la Unión por vía de Derecho internacional consuetudinario regional o del principio de *estoppel*, basado en la buena fe que impide a un sujeto actuar en contra de una expectativa legítima que sus propios actos han generado en otro sujeto causándole de este modo un perjuicio. Desde esta perspectiva, la UE o la OTAN serían responsables en Derecho internacional, por ejemplo, en caso de abandonar a la otra en el curso de una operación de gestión de crisis provocándole un detrimento político, diplomático, financiero e incluso pérdidas de vidas de efectivos[342]. En cualquier caso, ambas partes son conscientes de su gran importancia política y no parece que el peligro sea tanto de incumplimiento como de marginación, como se verá más adelante.

En cuanto al contenido de esta Declaración sobre la PESD, partiendo de las premisas de que la asociación estratégica establecida entre la UE y la OTAN en materia de gestión de crisis se basa en valores comunes y en la indivisibilidad de la dimensión de la seguridad en el siglo XXI y de que la Alianza sigue siendo la base de la defensa colectiva de sus miembros, se reconoce la importancia de una PESD capaz de realizar independientemente operaciones de gestión de crisis al amparo de instrumentos de que ya dispone la UE, pero utilizando las capacidades de planificación de la OTAN, y se

[340] Jefes de Estado y de Gobierno de la Unión Europea y Organización del Tratado del Atlántico Norte, *EU-NATO declaration of 16 December 2002 on ESDP*, Unión Europea y Organización del Tratado del Atlántico Norte, Bruselas, 2002 [disponible en http://www.consilium.europa.eu/uedocs/cmsUpload/73803%20-%20Solana%20-%20Permanent%20arrangements%20+%20NATO%20declaration.pdf, último acceso el 9 de julio de 2014].

[341] Para el análisis completo ver Reichard, *op. cit., supra* (nota 84), pp. 288-311.

[342] Reichard, *op. cit., supra* (nota 84), p. 309.

reafirma la determinación de fortalecer las respectivas capacidades. Además, se afirman solemnemente como principios fundamentales de la asociación estratégica entre las dos organizaciones internacionales la asociación, que garantice el refuerzo mutuo de las operaciones de gestión de crisis de dos organizaciones cuya naturaleza distinta se reconoce; la concertación, el diálogo, la cooperación y la transparencia; la igualdad y el debido respeto a la autonomía de la toma de decisiones y de los intereses de cada una de ellas; el respeto por los intereses de sus respectivos Estados miembros; el respeto por los principios de la CNU, subyacentes al TUE y al TAN; y el coherente, transparente y mutuamente beneficioso desarrollo de requisitos de capacidades militares comunes a ambas. Finalmente, la Unión se compromete a garantizar la participación de los aliados no miembros en la PESD, la Alianza se compromete a garantizar a aquélla el acceso a sus capacidades de planificación y ambas se comprometen a garantizar el referido desarrollo de estándares comunes de capacidades.

Se trató de una solución de compromiso al ya referido proceso de Saint Malo iniciado por Reino Unido y Francia en 1998 para dotar a la UE de una capacidad militar autónoma al que la OTAN dio su beneplácito un año después en Washington garantizando a la Unión acceso inmediato a sus capacidades de planificación para operaciones dirigidas por la misma en las que la Alianza en su conjunto no participara, no así a los demás activos comunes, que deben ser pre-identificados bajo una presunción de disponibilidad[343]. Por su parte, el Consejo Europeo de Colonia y las sucesivas cumbres de Jefes de Estado y de Gobierno de la UE consolidaron la distinción entre operaciones dirigidas de forma autónoma, de menor escala e intensidad, desde estructuras de mando nacionales que permitieran una representación multinacional en los cuarteles generales y aquellas otras dirigidas con ayuda de las planificaciones de

[343] Consejo del Atlántico Norte, *Final Communiqué of the North Atlantic Council Summit of 24 April 1999*, Organización del Tratado del Atlántico Norte, Washington, D. C., 1999, párrafo 10.

defensa de la OTAN y, en su caso, de otros activos pre-identificados cuya disponibilidad se presume[344].

El detalle de la implementación está contenido en un acuerdo marco consistente en un canje de cartas entre el Secretario General de la OTAN y el Alto Representante de la UE de 17 de marzo de 2003[345], que desarrolla la garantía de acceso de la Unión a la planificación operativa de la Alianza, con vistas a una utilización efectiva en el marco de la planificación militar de operaciones de gestión de crisis dirigidas por la UE; la posición del Comandante Supremo de la Alianza o *Supreme Allied Commander Europe* (en adelante *SACEUR*) al mando de las operaciones dirigidas por la Unión, con la posibilidad de un mando OTAN europeo para operaciones dirigidas por la Unión; la disponibilidad de las capacidades y activos comunes de la Alianza para operaciones de gestión de crisis dirigidas por la UE; el acuerdo de seguridad OTAN-UE para el intercambio de información clasificada en virtud de normas de protección recíproca; los procedimientos para la puesta a disposición, seguimiento, devolución y retirada de activos y capacidades de la Alianza; las modalidades de consultas OTAN-UE en el contexto de una operación de gestión de crisis dirigida por la Unión que recurra a activos y capacidades de la Alianza; la integración en el sistema de establecimiento de los planes de defensa de la OTAN de las necesidades y capacidades militares que puedan requerirse para operaciones militares dirigidas por la UE, con vistas a garantizar la disponibilidad de fuerzas bien equipadas y entrenadas para operaciones dirigidas por la Alianza o por la Unión[346].

[344] Consejo Europeo, *Annex III to the European Council of Cologne: Presidency Report on Strengthening the Common European Policy on Security and Defence*, Unión Europea, Colonia, 1999, párrafo 3.

[345] Cameron, Fraser y Quille, Gérard, "The Future of ESDP", *European Policy Centre Working Paper*, Centro Político Europeo, Bruselas, 2004, p. 28.

[346] Unión Europea, "Síntesis de la Legislación de la UE. Política Exterior y de Seguridad", *europa.eu*, 2007 [disponible en http://europa.eu/legislation_summaries/foreign_and_security_policy/cfsp_and_esdp_implementation/l33243_es.htm último acceso el 11 de julio de 2007].

El mecanismo Berlín Plus fue utilizado por primera vez en 2003 y 2004 cuando las operaciones aliadas de estabilización de la paz "Allied Harmony" en Macedonia y "SFOR" en Bosnia fueron relevadas por las misiones de gestión de crisis de la UE "EUFOR Concordia" y "EUFOR Althea" respectivamente. No obstante, a pesar de este éxito inicial, pronto se hizo evidente que la aplicación del acuerdo más allá de los Balcanes se veía decisivamente obstaculizada por el solapamiento entre una y otra organización internacional, funcional y de miembros[347], existiendo una cierta tendencia de determinados socios a utilizar su derecho de veto con fines de política nacional, como demuestra el enfrentamiento entre Turquía, aliado pero no miembro de la UE, y Chipre, miembro de la UE pero no aliado[348]. Esta inoperatividad de Berlín Plus para misiones expedicionarias condujo a la UE a articular sus misiones por medio de estructuras nacionales de planificación y mando al margen del acuerdo por ejemplo en la República Democrática del Congo o en las costas de Somalia, evidenciando que se trataba de un mecanismo institucional obsoleto e incapaz de servir a las necesidades de la defensa europea[349]. Adicionalmente, el interés creciente de la OTAN en el desarrollo de una dimensión civil para sus operaciones condujo a Washington a solicitar a la UE una suerte de Berlín Plus inverso o "Bruselas Plus" que garantizara el acceso de la Alianza a las estructuras de planificación y mando civiles de la Unión[350], oferta que hizo sospechar a algunos europeos que se tratara de una forma de limitar la PESD a la gestión de crisis civil.

Por otra parte, en medio de la ruptura provocada por la invasión de Irak, los líderes de Francia, Alemania, Bélgica y Luxemburgo reabrieron en abril de 2003, en la reunión caricaturizada como la "Cumbre del Chocolate", el debate

[347] Deighton, , Anne, "The European Security and Defence Policy", *Journal of Common Market Studies*, volume 40, número 4, 2002, pp. 719-741, p. 732.

[348] Missiroli, Antonio, "EU-NATO Cooperation in Crisis Management: No Turkish Delight for ESDP", *Security Dialogue*, volume 33, número 1, 2002, pp. 9-26.

[349] Howorth, Jolyon, "NATO and ESDP: Institutional Complexities and Political Realities", *Politique Étrangère*, número 4, 2009, pp. 95-107, p. 97.

[350] Asamblea de Defensa y Seguridad de la Unión Europea Occidental, "The EU-NATO Berlin plus agreements", *Assembly Facts Sheet 14*, Unión Europea Occidental, París, 2009.

sobre la creación de un Cuartel General de la UE en la ciudad belga de Tervuren[351], que dotara a ésta de una capacidad de planificación independiente de la de la Alianza. Este hito marcó la principal fuente de controversia entre la UE y la OTAN tras los acuerdos de Berlín Plus, pues suponía reconocer abiertamente el descontento con esta solución y la voluntad de poner de nuevo en marcha y de forma irreversible el aparentemente abandonado proceso de desarrollo por la Unión de opciones e intereses propios en materia de defensa hacia su total autonomía militar respecto de la Alianza. De este modo, fue necesario que Estados Unidos desplegara todo su arsenal diplomático para forzar la sustitución de esta iniciativa en diciembre del mismo año por un nuevo compromiso, formalizado en el documento político "Defensa Europea: consulta, planificación y operaciones entre la OTAN y la UE" con ocasión de la conferencia intergubernamental de Nápoles de 29 de noviembre de 2003, en la que Reino Unido transigió a la creación de una célula de planificación civil-militar de la UE en el EMUE, con la firma de un Acuerdo sobre el Estatuto de las Fuerzas de la UE o *European Union Status Of Forces Agreement* (en adelante *EU SOFA*)[352], a cambio de que los llamados "chocolateros" aceptaran el recurso al mismo sólo en última instancia y subsidiariamente respecto de las misiones apoyadas por la OTAN y planeadas en la célula de la UE en el Cuartel General de la Alianza europeo o *Supreme Headquarters Allied Powers Europe* (en adelante *SHAPE*)[353], establecida en 2006.

[351] Missiroli, Antonio (ed.), "From Copenhagen to Brussels. European defence: core documents", *Chaillot Paper 47*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2003, pp. 76-81.

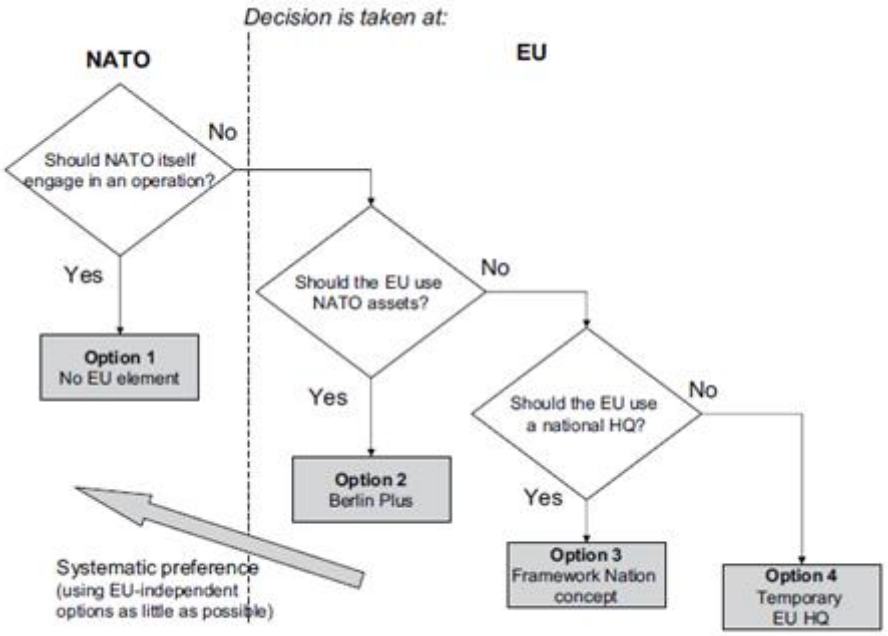
[352] Jefes de Estado y de Gobierno de la Unión Europea, *Agreement between the Member States of the European Union of 17 November 2003 concerning the status of military and civilian staff seconded to the institutions of the European Union, of the headquarters and forces which may be made available to the European Union in the context of the preparation and execution of the tasks referred to in Article 17(2) of the Treaty on European Union, including exercises, and of the military and civilian staff of the Member States put at the disposal of the European Union to act in this context* [OJ C 321/6], Unión Europea, Bruselas, 2003.

[353] Reichard, *op. cit., supra (nota 84)*, pp. 86-87.

Una vez confirmado por el Consejo Europeo de Bruselas de 12 de diciembre de 2003, el aludido documento establece una jerarquía sistemática de cuatro opciones para la conducción de operaciones de paz por ambas organizaciones internacionales [354] : (1º) Campaña dirigida por la OTAN utilizando contribuciones de aliados europeos, pero sin elemento independiente UE; (2º) operación dirigida por la Unión bajo el control político y la dirección estratégica del POCS, utilizando las instalaciones de planificación y demás instrumentos e inteligencia de la Alianza bajo los acuerdos de Berlín Plus -ejemplos de la cual son las misiones "Concordia" y "Althea"-; (3º) operación autónoma dirigida por la UE sin el apoyo de los activos de la OTAN, planificada, organizada y conducida a través del cuartel general nacional de un Estado miembro actuando como nación marco -como la operación "Artemis" liderada por Francia-; y (4º) operación autónoma dirigida por la Unión sin el apoyo de los activos de la Alianza, planificada, organizada y conducida a través de la célula de planificación cívico-militar en el EMUE. Esta última vía se ha utilizado para orquestar desde 2012 la operación naval Atalanta contra la piratería en el Cuerno de África, activando el Consejo por primera vez el Centro de Operaciones de la UE[355] desde su creación en 2003.

[354] Reichard, *op. cit., supra (nota 84)*, pp. 88-90.

[355] Consejo de la Unión Europea, *Comunicado de Prensa de la Sesión número 3157 del Consejo de Asuntos Exteriores, 22 y 23 de marzo de 2012* [7849/12 PRESSE 117 PR CO 18], Unión Europea, Bruselas, 2012, p. 18.



Fuente: Reichard (2006, p. 89).

En cualquier caso, la ambigua redacción del acuerdo Berlín Plus evita abordar expresamente la cuestión de la división del trabajo entre ambas organizaciones internacionales[356], dejando margen al recelo de las potencias europeístas de la "Antigua Europa" acerca del control de Washington sobre la autonomía de la UE mediante el "derecho de tanteo" de la OTAN[357]. Si se considera que, como se concluyó en epígrafes anteriores, la propia PCSD adolece de un grave defecto de definición de prioridades estratégicas debido a la diversidad de intereses de sus Estados miembros y a la falta de voluntad de consenso por los mismos, es lógico que no puedan afirmarse dichas prioridades en las relaciones con la Alianza a fin de constituir un equilibrio más justo en el reparto de la responsabilidad sobre la seguridad europea e incluso mundial, tantas veces reconocido por ambas organizaciones internacionales

[356] Hofmann, Stephanie y Reynolds, Christopher, "EU-NATO Relations: Time to Thaw the <<Frozen Conflict>>", *Stiftung Wissenschaft und Politik Comments 12, Stiftung Wissenschaft und Politik*, Berlín, 2007, p. 8.

[357] Biscop, Sven, NATO, "ESDP and The Riga Summit: No Transformation Without Re-Equilibration", *Egmont Paper 11*, Real Instituto Egmont de Relciones Internacionales, Bruselas, 2006, p. 6.

como necesario y mutuamente beneficioso, pero nunca llevado a la práctica de forma consecuente. Este extremo se discutirá a continuación.

7.4 HACIA UN NUEVO EQUILIBRIO EN LAS RELACIONES ENTRE LA UE Y LA OTAN:

Como ya se ha referido, la reorientación de la OTAN como actor global desde los noventa, para adaptarse a las nuevas amenazas a la seguridad internacional y justificar su existencia tras la Guerra Fría, y el cambio de foco estratégico de la política exterior de Washington, cada vez más proclive a aceptar e incluso a potenciar una defensa europea fuerte bajo la premisa de la primacía de la Alianza, junto con el esfuerzo de la PESC por desarrollar una PESD que hiciera de la UE un actor internacional solvente en materia de defensa, han favorecido cierto cambio de equilibrio de la seguridad europea hacia esta última. La consiguiente convergencia de ambas organizaciones internacionales en la seguridad europea y de su área de influencia, especialmente en el ámbito de las operaciones de gestión crisis, ha revelado, por una parte, una situación de competencia, inevitable consecuencia del solapamiento funcional y geográfico de ambas organizaciones internacionales[358], y, por otra, una necesidad de cooperación potenciada además por el nivel de incertidumbre que la globalización ha introducido en el sistema internacional[359].

De este modo, la relación entre la OTAN y la UE ha oscilado entre la competencia y la cooperación, en función de diversos factores y momentos históricos, sobre la base de una cuidadosa ambigüedad al respecto de una división del trabajo en lo que respecta a la seguridad de Europa, constituyendo precisamente la falta de claridad acerca de esta división del trabajo el principal obstáculo para unas relaciones fluidas entre OTAN y UE según algunos

[358] *Ibid.*, p. 3.

[359] Van der Vleuten, Anna, "Two-level interaction as source of influence. The European Union and equal treatment policies", en Reinalda, Bob y Verbeek, Bertjian (eds.), *Autonomous Policy Making by International Organizations*, London, Routledge, 1998, p. 62-79, p. 63.

autores[360] , ello unido a las diferentes ambiciones de ambas organizaciones internacionales en relación con dicho reparto de tareas[361]. Empero, una clara delimitación del trabajo supondría definir la esfera de responsabilidad de un actor limitando la del otro, tratándose de organizaciones cuyo ámbito de funciones se solapa considerablemente, de manera que se atribuyan a la una responsabilidades que bien podría asumir la otra y se acentúe la rivalidad entre ambas[362] hasta el punto de ser percibida incluso como una lucha darwiniana por la supervivencia[363].

A pesar de ello, desde el plano teórico, se habla de una división del trabajo funcional y geográfica[364] como situación de hecho a limitar o a asumir según las opiniones. Geográficamente, la pérdida de interés de Estados Unidos en el Viejo Continente, progresiva desde la caída del Telón de Acero y radical desde que los atentados del 11 de septiembre destaran la "Guerra del Terror", ha posibilitado y, en cierto modo, forzado un cambio de guardia en la defensa europea que liberara recursos estadounidenses y de la OTAN para sus nuevas prioridades geoestratégicas. Este reparto de las cargas de la seguridad global, cuya premisa es la asunción por parte de la entonces PESD de un papel de "proveedor de seguridad" al menos en su propio territorio y alrededores, tuvo como primera manifestación el relevo de las fuerzas aliadas de estabilización

[360] Menon, Arnand, "Why ESDP is Misguided and Dangerous for the Alliance?", en Howorth, Jolyon y Keeler, John (eds.), *Defending Europe*, London, Macmillan, 2003, pp. 203-219.

[361] Hofmann y Reynolds, *op. Cit., supra* (nota 256), p. 2.

[362] Biermann, Rafael, "Rivalry Among International Organizations Bringing Power Back In", *Paper for the Panel The European Union and Transatlantic Relations of 14 September 2007*, Turín, 2007 [disponible en http://www.ies.be/files/documents/JMCdepository/Rafael%20Biermann,%20Rivalry%20Among%20International%20Organizations.%20Bringing%20Power%20Back%20In.pdf, ultimo acceso el 5 de Julio de 2014], p. 20.

[363] The Economist, "Berlin Minus. There is no excuse for the failure of NATO and the EU to talk to each other", *www.economist.com*, 2007 [disponible en http://www.economist.com/node/8669193, ultimo acceso el 17 de julio de 2014].

[364] Oswald, Franz, *Europe and the United States. The Emerging Security Partnership*, Londres, Praeger Security International, 2006, p. 152.

de la paz por las misiones de gestión de crisis de la UE en Macedonia, 2003, y en Bosnia, 2004, en aplicación del mecanismo de Berlín Plus.

Fuera de suelo europeo, en cambio, la aludida ambigüedad estratégica acerca del reparto de tareas ha llevado a solapamientos y duplicaciones innecesarias, creando una situación de competencia entre misiones exteriores de la Unión y la Alianza desde el primer momento en que aquélla decidió en 2003 llevar a cabo fuera de su territorio la operación "Artemis" en la República Democrática del Congo, bajo mandato de las ONU, pero sin autorización de la OTAN y al margen del marco Berlín Plus[365]. Esta carrera expedicionaria alcanzó su punto álgido en 2008, cuando ambas organizaciones internacionales se embarcaron en sendas operaciones marítimas autónomas, "Ocean Shield" y "EU NAVFOR Atalanta", para combatir la piratería en aguas territoriales de Somalia[366].

Algunos autores han abogado por un equilibrio entre la ambigüedad estratégica y la coherencia[367], pues la clara delimitación de áreas de interés de la UE y la Alianza constituye un peligroso ejercicio de *realpolitik* que recuerda demasiado a la política de las "esferas de influencia" del siglo pasado[368] y es especialmente impracticable en un mundo en el que la globalización ha difuminado las fronteras y el reparto de tareas entre actores de seguridad debe hacerse caso por caso[369], en función de la identificación de la organización internacional, Estado o grupo de Estados mejor posicionado para tomar el mando de la operación de gestión de crisis de que se trate[370].

[365] Kulich, *op. cit., supra* (nota 330), pp. 30-31.

[366] Seibert, Bjoern, "When great powers compete, the pirates win", *Foreign Policy*, 30 de marzo, 2009.

[367] Chivvis, Christopher, "Recasting NATO's Strategic Concept, Possible Directions for the United States", Occasional Paper, RAND Corporation, Santa Mónica, California, 2009 [disponible en http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP280.pdf, ultimo acceso el 5 de julio de 2014], p. 2.

[368] Hofmann y Reynolds, *op. cit., supra* (nota 256), p. 8.

[369] Kulich, *op. cit., supra* (nota 330), pp. 34-35.

[370] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 4.

También se ha propuesto como una alternativa más tolerable a la división del trabajo geográfica la funcional[371], convenida como premisa de la propia PESD entre Francia -cabeza de la facción "europeísta"- y el Reino Unido -Estado miembro "atlantista" por excelencia- en la ya mencionada Cumbre de Saint Malo de 1998[372], ante la evidencia del atraso de las capacidades militares europeas respecto de las estadounidenses durante la crisis de Kosovo y el hecho de que el apoyo norteamericano a aquella política estuviera condicionado a la primacía de la Alianza. La consecuencia es que la relación entre la PESD y la OTAN se ha articulado desde el principio sobre el elemento central de la dependencia asimétrica de aquélla respecto de las capacidades de planificación y los recursos de ésta[373], factor estructural que dificulta la sinergia entre organizaciones internacionales, en tanto la constante aspiración a reducir la dependencia obstaculiza la verdadera cooperación[374].

Ello conduce a la misma situación de "cooperación bajo rivalidad"[375] que lleva a la duplicación de recursos y retroalimenta el solapamiento, el cual a su vez impide el desarrollo de una división del trabajo eficiente entre la UE y la OTAN[376]. Sin embargo, como quiera que cierta superposición funcional es condición *sine qua non* de una verdadera cooperación[377], la clave está en alcanzar una duplicación efectiva, es decir, equilibrada de forma que no alcance un grado de solapamiento tal que disminuya la cooperación y aumente

[371] Forsberg, Tuomas y Herd, Graeme, *Divided West. European Security and the Transatlantic Relationship*, The Royal Institute of International Affairs, Londres, 2006, p. 130.

[372] Rutten, Maartje (coord.), "From St. Malo to Nice. European Defence: Core Documents", *Chaillot Paper 47*, Instituto de Estudios de Seguridad, Unión Europea Occidental, París, 2001, pp. 8-10.

[373] Marsal Muntala, *op. cit., supra* (nota 293), p. 188.

[374] Biermann, Rafael, "Towards a theory of inter-organizational networking. The Euro-Atlantic security institutions interacting", *The Review of International Organizations*, volumen 3, número 2, 2008, pp. 151-177, p. 171

[375] Biermann, *op. cit., supra* (nota 362), p. 32.

[376] Hofmann, Stephanie, "Overlapping Institutions in the Realm of International Security: The Case of NATO and ESDP", *Perspectives on Politics*, volumen 7, número 1, 2009, pp. 45-53, p. 46.

[377] Biermann, *op. cit., supra* (nota 156), p. 8.

la competencia[378]. Esto es especialmente evidente en el caso de dos organizaciones internacionales cuyas funciones en el ámbito de la seguridad se superponen, pero que presentan fortalezas y debilidades distintas de tal forma que pueden llegar a complementarse sobre la base o bien de un cierto reparto de tareas o bien de un intercambio de *know how* en lo que se refiere al desarrollo de las capacidades respectivas.

Por una parte, el principal factor restrictivo de la PCSD son sus limitaciones en lo que respecta a determinadas capacidades militares estratégicas[379], como son el transporte aéreo estratégico, el repostaje aire-aire o los sistemas de inteligencia, vigilancia y reconocimiento y supresión de defensas aéreas enemigas, hasta el punto en que no parece que ningún Estado miembro pueda reunir todas las capacidades necesarias para constar de una defensa integral[380]. De hecho, la gran brecha en materia de capacidades de defensa entre Estados Unidos y los aliados europeos no sólo es uno de los mayores impedimentos a la asunción de una mayor responsabilidad de la UE sobre la seguridad regional, sino que es además una importante fuente de tensión entre ambas orillas del Atlántico en el seno de la OTAN. Si bien Washington mantiene su liderazgo sobre la Alianza, el proceso de reducción de su presupuesto de defensa y reajuste de esfuerzo estratégico hacia una mayor eficiencia y recolocación geográfica en que se halla inmerso el gigante norteamericano lo han llevado a reclamar efusivamente de los socios europeos un reparto más equitativo de las cargas -*burden-sharing*- para evitar el tradicional *free-riding* de algunos Estados que se benefician de las externalidades positivas de la seguridad europea sin contribuir en consonancia[381].

Aunque ambas partes parecen cada vez más conscientes de la necesidad de llevar a cabo el desarrollo militar de Europa de forma cooperativa y no competitiva, el punto de partida fue la rivalidad entre ellas. De esta forma, el

[378] Kulich, *op. cit., supra* (nota 330), p. 23.

[379] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 3.

[380] Yaniz Velasco, *op. cit., supra* (nota 135), p. 11.

[381] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 2.

primer intento de colmar la brecha de capacidades se emprendió en el Consejo Europeo celebrado en diciembre de 1999 en Helsinki, en el que se proyectó la imagen de una Europa cuyo papel era el de pasar la aspiradora tras la intervención americana[382] para justificar el desarrollo de "una capacidad de decisión autónoma", así como, "en aquellas operaciones militares en las que no participe la OTAN en su conjunto, la capacidad de iniciar y llevar a cabo operaciones militares dirigidas por la UE en respuesta a crisis internacionales"[383]. La materialización práctica de este propósito fue el ya mencionado Objetivo de Helsinki consistente en la creación de una Fuerza Europea de Reacción Rápida, iniciativa que, aunque evitaría duplicaciones innecesarias y no implicaría la creación de un ejército europeo[384], fue criticada al otro del atlántico por duplicar los recursos y activos de la OTAN y vista por algunos como una tentativa de cuestionar el *status quo* transatlántico[385].

Por otra parte, también han sido llevadas al plano de la competencia entre las dos organizaciones de seguridad europeas, con el consiguiente riesgo de extensión de las duplicidades fuera del ámbito militar[386], las incursiones de la Alianza en el terreno del "poder suave" para incorporar capacidades civiles entre sus instrumentos de gestión de crisis bien porque las organizaciones que ofrecen servicios similares tienden a competir por su cuota en las relaciones internacionales[387] o bien por la toma de conciencia de la ineficiencia de los medios meramente militares para generar una paz duradera en la fase post-

[382] Garden, Timothy, "The future of ESDP-defence capabilities for Europe", *The International Spectator*, volume 38, número 3, 2003, pp. 7-14, p. 14.

[383] Consejo Europeo, *Conclusiones de la Presidencia del Consejo Europeo de 11 de diciembre de 1999*, Unión Europea, Helsinki, 1999 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/00300-r1.es9.htm, último acceso el 17 de julio de 2014], párrafo 27.

[384] *Ibid.*, párrafo 27.

[385] Pape, Robert, "Soft balancing against the United States", *International Security*, volume 30, número 1, 2005, pp. 7-45.

[386] Sturm, Paul, "NATO and the EU: Cooperation?", *European Security Review*, número 48, 2010 [disponible en http://www.isis-europe.eu/sites/default/files/programmes-downloads/2010_artrel_445_eu-nato-capabilities.pdf, último acceso el 5 de julio de 2014], p. 2.

[387] Biermann, *op. cit., supra* (nota 362), p. 15.

conflicto. Ello derivó en la mencionada propuesta estadounidense de un a modo de Berlín Plus inverso o "Bruselas Plus" que garantizara el acceso de la Alianza a las estructuras de planificación y mando civiles de la Unión y que no fue muy bien acogida en el Viejo Continente.

Para tratar de superar el *gap* de capacidades, así como la igualmente grave existencia de capacidades redundantes de los distintos Estados miembros provocada por la otra gran debilidad de la PCSD, la ausencia de una dirección estratégica que permita coordinar las planificaciones de defensa nacionales en función de determinadas prioridades identificadas claramente[388], se propuso a nivel de la UE el mecanismo conocido como *pooling and sharing*, que ya ha sido objeto de análisis. En el ámbito de la Alianza, se desarrolló el concepto paralelo de *Smart Defence*, referido al mencionar el énfasis de las conclusiones del Consejo Europeo de diciembre de 2013 en la necesidad de sinergia entre ambas iniciativas[389]. La OTAN, en su Declaración de Chicago de 2012, comparte esta vocación de complementariedad al afirmar que "la OTAN trabajará estrechamente con la UE, como se ha acordado, para garantizar que nuestra *Smart Defence* y el *Pooling and Sharing* de la UE sean iniciativas complementarias y mutuamente ventajosas"[390].

La filosofía subyacente a la "defensa inteligente" es la misma idea de "mancomunar y compartir" y de la UE, es decir, convertir a la Alianza en intermediaria o catalizadora de las soluciones multinacionales a los problemas comunes priorizando las capacidades más necesarias para la OTAN y propiciando un equilibrio en los gastos de defensa, de manera que se compaginen las prioridades de los distintos aliados en materia de defensa, que es ante todo una responsabilidad nacional, con las de la Alianza en su conjunto, en un escenario en el que la tecnología es cara, los presupuestos

[388] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 4.

[389] Ballesteros Martín, *op. cit., supra* (nota 266), pp. 9-10.

[390] Consejo del Atlántico Norte, *Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012* [Press Release (2012) 062], Organización del Tratado del Atlántico Norte, 2012 [disponible en http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease, ultimo acceso el 12 de Julio de 2014], párrafo 20.

militares se reducen y determinadas capacidades clave sólo pueden adquirirse y desarrollarse si los socios trabajan juntos, incluso concentrándose en sus puntos fuertes mediante la especialización por diseño[391].

Lo dicho para los miembros de cada una de estas organizaciones internacionales es válido también para las relaciones entre ellas, ya que la crisis económica y las políticas de austeridad, los cambios en el entorno de seguridad, el uso de armas cada vez más avanzadas y el desequilibrio entre Europa y Estados Unidos deben ser igualmente abordados en el plano de la interacción entre UE y OTAN. En este sentido, el Concepto Estratégico de 2010 declara que la UE es un socio único y esencial para la OTAN en la medida en que ambas comparten la mayoría de los miembros y todos los miembros de las dos comparten valores comunes[392]. Por su parte, la citada Declaración de Chicago de 2012 repite que la OTAN y la UE comparten valores comunes e intereses estratégicos y que la UE es un socio único y esencial de la OTAN, añadiendo que el refuerzo de esta asociación estratégica es particularmente importante en el entorno actual de austeridad, de modo que ambas organizaciones internacionales deben continuar trabajando para mejorar la cooperación práctica en operaciones, ampliar las consultas políticas y cooperar de forma más completa en el desarrollo de capacidades[393].

Además de las diferencias de capacidad, el más o menos patente reparto de tareas entre la UE y la OTAN se ve determinado, a la vez que cuestionado, por divergencias de cultura estratégica. Así, como se mencionó a propósito de la asociación transatlántica, los atentados del 11 de septiembre de 2001 constituyeron un momento histórico de profundos cambios que alteraron la dinámica tradicional de las relaciones internacionales[394] y sumieron el entorno de seguridad post-11 S en una crisis de multilateralismo[395], que también

[391] Yaniz Velasco, *op. cit., supra* (nota 135), p. 16.

[392] Consejo del Atlántico Norte, *op. cit., supra* (nota 228), párrafo 32.

[393] Consejo del Atlántico Norte, *op. cit., supra* (390), párrafo 20.

[394] Gärtner, Heinz y Cuthberson, Ian (eds.), *European Security and Transatlantic Relations after 9/11 and the Iraq War*, Nueva York, Palgrave Macmillan, 2005, p. 1.

[395] Newman, Edward, *A crisis of global institutions: multilateralism and international security*, Routledge, Nueva York, 2007.

sacudió la cooperación entre la Unión y la Alianza, así como el diálogo estratégico entre los Estados miembros de ambas organizaciones internacionales, y cuyo punto álgido se alcanzó con el desacuerdo sobre la invasión de Irak en 2003.

Algunos años después la crisis se superó gracias a los cambios en los gobiernos de los principales protagonistas de los enfrentamientos y, sobre todo, al acercamiento del nuevo presidente francés Nicolás Sarkozy, que llevó a la reintegración de Francia en la estructura de mandos de la OTAN en 2008 y al nombramiento de un general francés como comandante del Mando Aliado de Transformación de la Alianza. Sin embargo, la ruptura había puesto de manifiesto que, junto a las disparidades funcionales, existía una incompatibilidad ideológica entre Estados Unidos y la UE[396] que llevó a algunos a predecir una posible salida de aquél de la OTAN[397] o incluso la completa desintegración de la más efectiva organización de seguridad del mundo. La respuesta fue la reinvención de la Alianza para hacer frente a las nuevas amenazas a la seguridad en la Cumbre de Praga de 2002, en la que se adoptó el enfoque militar estadounidense de la lucha contra el terrorismo internacional[398], frente al carácter civil que se le atribuye en el Viejo Continente, en la línea de la división funcional del trabajo entre las dos organizaciones de seguridad europeas. Concretamente, se decidió la creación de la Fuerza de Respuesta de la OTAN, que, aunque anunciada como complemento de la Fuerza Europea de Reacción Rápida, debiendo ambas reforzarse mutuamente y respetar a la vez la autonomía de ambas organizaciones internacionales[399],

[396] Kulich, *op. cit., supra* (nota 330), p. 38.

[397] Heftendorn, Helga, "From an Alliance of Commitment to an Alliance of Choice: The Adaptation of NATO in a Time of Uncertainty", en Cottey, Andrew, *Security in the New Europe*, Nueva York, Palgrave Macmillan, 2007, pp. 161-180, p. 161.

[398] Reichard, *op. cit., supra* (nota 84), p. 108.

[399] Consejo del Atlántico Norte, *Prague Summit Declaration, the North Atlantic Council of 21 November 2002*, Organización del Tratado del Atlántico Norte, Praga, 2002 [disponible en http://www.nato.int/docu/pr/2002/p02-127e.htm, último acceso el 5 de julio de 2014], párrafo 4.a).

fue vista por algunos como un complot americano para contrarrestar esta iniciativa de la UE[400].

En cualquier caso, aunque lo avalen las fortalezas y debilidades de una y otra organización internacional[401] y las diferencias de cultura estratégica entre sus miembros, el reparto funcional de tareas *hard power-soft power*, conforme al cual las potencias regionales y locales europeas orquestan las operaciones militares a través de la OTAN con el apoyo estadounidense y la reconstrucción de las estructuras civiles a través de la UE, de manera que aquélla "hace el trabajo duro" y ésta "friega los platos"[402], quedó profundamente cuestionado como insatisfactorio, indeseable e insostenible en el futuro[403]. Sin embargo, hasta el momento, la ausencia de una estrategia comprensiva que sustituya el modelo "abajo-arriba" de conducción de la PESC y la PCSD por un enfoque "arriba-abajo" y la ausencia de acuerdo entre Estados miembros acerca del papel y la utilidad del instrumento militar en la acción exterior impiden recalibrar este equilibrio[404].

Sea como fuere, la ambigua definición de la división del trabajo entre ambas organizaciones internacionales ha llevado a la competencia y a la duplicidad en la medida en que la PESD fue alcanzando un éxito palpable e

[400] Laursen, Finn y otros, "The Institutional Dynamics of Euro-Atlnatic Integration", en Mouritzen, Hans y Wivel, Anders (eds.), *The Geopolitics of Euro-Atlantic Integration*, Londres, Routledge, 2005, pp. 43-69, p. 65.

[401] Ver Chafos, Timothy, *The European Union's Rapid Reaction Force and the North Atlantic Treaty Organization Response Force: A Rational Division of Labor for European Security*, Washington D. C., Storming Media, 2003, p.45, que afirma que la OTAN está mucho más capacitada para recurrir a la amenaza o a la proyección de la fuerza, y Lenzi, Guido, "The WEU between NATO and EU", *Studia Diplomatica*, volumen 51, 1998, pp. 167 y ss., que defiende que la UE, por su ADN y por su origen, es más eficaz desde la perspectiva humanitaria, cívico-económica y de prevención y rehabilitación post-conflicto.

[402] De Joop Scheffer, Jaap, *Speech by NATO Secretary General Jaap de Hoop Scheffer at the National Defense University on 29 January 2004*, Organización del Tratado del Atlántico Norte, Washington, 2004 [disponible en http://www.nato.int/docu/speech/2004/s040129a.htm, último acceso el 5 de julio de 2014].

[403] Kulich, *op. cit., supra* (nota 330), p. 39.

[404] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 3.

incorporando elementos de *hard power*, a la vez que la Alianza adquiría herramientas de *soft power*[405]. Por ello, una alternativa que algunos autores consideran incluso una necesidad[406] es un enfoque holístico en el cual no existen el poder "blando" o "duro", sino los instrumentos de poder "blando" o "duro" que deben estar igualmente representados en una capacidad estratégica cívico-militar que permita hacer uso de unos u otros en el momento oportuno. Este nuevo paradigma, que propugna un actor internacional de seguridad del siglo XXI cuyo éxito reside en su dominio del "poder inteligente" o *smart power*, es decir, en su habilidad para combinar los elementos "duro" y "suave" del poder[407], se plasmó con ocasión de la Cumbre de Riga de la Alianza de 2006 en la petición de un enfoque comprensivo por parte de la comunidad internacional que integrara un amplio espectro de instrumentos militares y civiles[408] y condujo al ex-Primer Ministro francés Hubert Védrine a afirmar que los americanos y los europeos están llamados a forjar una nueva alianza estratégica basada en la *realpolitik* "inteligente"[409].

Ello implica que la UE debería tener la capacidad para conducir todo el abanico de operaciones de gestión de crisis, incluso las más complejas y exigentes[410], y que la OTAN debería adquirir los componentes civiles que le faltan para un enfoque comprensivo de la defensa[411], haciendo posible un reparto de tareas caso por caso en el que, mientras persista la incapacidad militar de la UE, el papel de gestión de crisis se delegue en la OTAN[412] y asentando con el tiempo un enfoque integral de la política exterior de dos

[405] Kulich, *op. cit., supra* (nota 330), p. 50.

[406] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 4.

[407] Kulich, *op. cit., supra* (nota 330), p. 4.

[408] Consejo del Atlántico Norte, *Riga Summit Declaration of 29 November 2006*, Organización del Tratado del Atlántico Norte, Riga, 2006 [disponible en http://www.nato.int/docu/pr/2006/p06-150e.htm, último acceso el 5 de julio de 2014], párrafo 6.

[409] Védrine, Hubert, *History Strikes Back. How States, Nations and Conflicts Are Shaping the Twenty-First Century*, Washington D. C., Brookings Institution Press, 2008, p. 123.

[410] Tuomioja y Freivalds, Erkki y Freivalds, Laila, "We want a stronger EU security policy", *Dagens Nyheter*, 11 de noviembre, 2003, p. 430.

[411] Coelmont y De Langlois, *op. cit., supra* (nota 329), p. 5.

[412] Hofmann y Reynolds, *op. cit., supra* (nota 256), p. 8.

actores de seguridad plenamente dotados como son la Unión Europea y Estados Unidos[413], solución a la que éste no se opondría al no ver en una Europa fuerte un competidor de la Alianza, sino un socio esencial de la OTAN y de Washington[414].

A este respecto, Coelmont y De Langlois (2013, pp. 5-6) proponen tres recomendaciones sobre la redefinición de las relaciones entre la PCSD y la OTAN: (a) cooperación, mediante el establecimiento de un Pacto Estratégico de Seguridad transatlántico, en el que se codifique un concepto amplio de seguridad que ofrezca una solución conjunta y coordinada a los desafíos de un mundo multipolar, y la convocatoria regular y estructurada de reuniones entre la UE y Estados Unidos; (b) copropiedad, a través de la implementación de nuevas estructuras para el diálogo entre PCSD y OTAN, inspirado en la asociación transatlántica, la aplicación de un enfoque bidireccional en la transferencia de activos y capacidades colectivos de la UE y la OTAN cuando una u otra pongan en marcha una operación militar y la creación de sinergias en las capacidades cívico-militares de ambas organizaciones internacionales; y (c) capacidades, por medio del desarrollo de un nivel de autonomía estratégica apropiado para los Estados miembros de la UE respecto de los activos militares de Estados Unidos, la implementación de un proceso de decisión efectivo, así como acuerdos para el apoyo mutuo inmediato y equipos de enlace, que permitan la acción de emergencia coordinada entre la UE y la OTAN, la coordinación de las planificaciones de defensa nacionales, identificando y reduciendo las redundancias a nivel de la UE, la utilización de la Cooperación Estructurada Permanente por los Estados miembros dispuestos a asumir el liderazgo del desarrollo de la política de defensa y seguridad en Europa y la garantía de la interoperabilidad entre los socios de la UE y de la OTAN.

[413] Biscop, Sven (ed.), “The Value of Power, the Power of Values: A Call for an EU Grand Strategy”, *Egmont Paper 33*, Real Instituto Egmont de Relaciones Internacionales, 2009, p.11.

[414] Clinton, Hillary, *Remarks at the NATO Strategic Concept Seminar*, Washington D. C., 2010.

PARTE III: COOPERACIÓN ENTRE LA UE Y LA OTAN EN MATERIA DE CIBERDEFENSA:

8 LA CIBERDEFENSA DE EUROPA:

En este apartado se procede a la exposición de los marcos reguladores de la ciberdefensa en la UE y en la OTAN con el fin de compararlos y derivar conclusiones acerca de la compatibilidad y complementariedad de los enfoques que cada una adopta. En suma, el objetivo es contrastar las distintas actitudes de estas organizaciones internacionales hacia la legítima defensa colectiva, analizadas en detalle en la primera parte, con los documentos oficiales al respecto para determinar las perspectivas de cooperación entre ambas que dichos marcos ofrecen.

8.1 ESTRATEGIA DE LA UE EN MATERIA DE CIBERDEFENSA:

Como ya se ha apuntado, ante la imposibilidad de elaborar una nueva estrategia de seguridad que reemplace a la EES de 2003, se ha optado por la redacción de estrategias transversales en ámbitos clave como la seguridad marítima o el ciberespacio. Así surge el 7 de febrero de 2013 la Estrategia de ciberseguridad de la UE, bajo la rúbrica "un ciberespacio abierto, protegido y seguro" y acompañada de un propuesta legislativa técnica de la Dirección General de Redes de Comunicación, Contenido y Tecnologías de la Comisión Europea para reforzar la seguridad de los sistemas de información de la UE[415]. La adopción de estos dos documentos se inscribe dentro de la Agenda Digital para Europa, una de las siete iniciativas emblemáticas de la Estrategia Europa 2020, de manera que su ámbito se extiende tanto a la dimensión civil como a la militar y a las vertientes interna y externa de la ciberseguridad, la cual abarca

> "las salvaguardias y medidas que pueden utilizarse para proteger el ciberespacio, en los ámbitos tanto civil como militar, de las amenazas

[415] Comisión Europea, *Propuesta de 7 de febrero de 2013 de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión* [COM(2013) 48 final], Unión Europea, Bruselas, 2013.

inherentes a sus redes interdependientes e infraestructuras de información, o que pueden dañarlas"[416].

Esta vocación comprensiva se propone (a) "lograr la ciberresiliencia", (b) "reducir drásticamente la ciberdelincuencia", (c) "desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD)", (d) "desarrollar recursos industriales y tecnológicos de ciberseguridad" y (e) "establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE" como prioridades estratégicas, dentro de las cuales sólo la tercera se aborda propiamente desde la perspectiva de la defensa, nuevamente marginada en el planteamiento de seguridad de la UE, como prueba que no se le dedique ni una página completa de las veintidós que componen el texto.

En este reducido espacio, la Estrategia de ciberseguridad se limita a afirmar que "el desarrollo de capacidades de ciberdefensa debería concentrarse en la detección, respuesta y recuperación frente a complejas ciberamenazas", potenciando "las sinergias entre los enfoques civil y militar" y con el apoyo de "actividades de investigación y desarrollo y una mayor cooperación entre las administraciones públicas, el sector privado y la comunidad académica de la UE"[417]. Adicionalmente, se recalca la necesidad de aunar esfuerzos con la OTAN para evitar duplicaciones y "aumentar la resiliencia de infraestructuras críticas públicas, de defensa y de información de las que dependen los miembros de ambas organizaciones"[418].

Como acciones concretas que la Alta Representante se compromete a llevar a cabo en colaboración con los Estados miembros y la Agencia Europea de Defensa se encuentran (a) la evaluación de los requisitos operativos de ciberdefensa de la UE y la promoción del desarrollo de sus capacidades y tecnologías de ciberdefensa en sus aspectos de doctrina, liderazgo, organización, personal, formación, tecnología, infraestructuras, logística e

[416] Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *op. cit., supra* (nota 241), p. 3.

[417] *Ibid.*, p. 12.

[418] *Ibid.*

interoperabilidad; (b) la elaboración de un marco político de ciberdefensa de la UE para proteger las redes dentro de las misiones y operaciones de la PCSD -compromiso al que, recuérdese, el Consejo Europeo de diciembre puso como plazo 2014- y la inclusión de aspectos de ciberdefensa en los actuales manuales de ejercicios ofreciendo mayores posibilidades al ejército para formarse y adiestrarse en la materia; (c) la promoción del diálogo entre las esferas civil y militar de la UE para el intercambio de buenas prácticas e información, la alerta temprana, la respuesta a incidentes, la evaluación de riesgos, la concienciación y la consideración de la ciberseguridad como objetivo prioritario; y (d) la garantía del diálogo con los socios internacionales, entre ellos la OTAN, otras organizaciones internacionales y centros de excelencia plurinacionales con el fin de conseguir auténticas capacidades de defensa, determinar las áreas de cooperación y evitar la duplicación de esfuerzos[419].

Además de estas directrices poco precisas en materia de ciberdefensa, interesa destacar los efectos del presente trabajo que en la Estrategia de ciberseguridad "la UE no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio", sino que por el contrario adopta una postura jurídica preventiva que exige que se respeten

> "las obligaciones jurídicas establecidas en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta de los Derechos Fundamentales de la Unión Europea. La UE examinará de qué modo puede garantizarse que esas disposiciones se aplican también en el ciberespacio"[420].

En esta línea, se añade que "en caso de que los conflictos armados se extiendan al ciberespacio, se aplicarán el Derecho humanitario internacional y, en su caso, el Derecho internacional en materia de derechos humanos"[421]. Por lo tanto, puede interpretarse que también respecto del *ius ad bellum* la UE mantiene un enfoque de *lege lata* en virtud del cual serían de aplicación a los

[419] *Ibid.*, pp. 12 y 13.

[420] *Ibid.*, p. 17.

[421] *Ibid.*, pp. 16-18.

ciberataques los planteamientos desarrollados en los tres primeros apartados de este trabajo. De este modo, parece quedar abierta la puerta al ejercicio de la legítima defensa ante ciberataques al amparo del artículo 42.7 del TUE, si se cumplen las condiciones ya examinadas en detalle, aunque la Estrategia de ciberseguridad aborda la cuestión sólo desde la perspectiva interna o de *law enforcement* propia del antiguo tercer pilar -ahora integrado en el Espacio de Libertad, Seguridad y Justicia- cuando reconoce que "un incidente o ataque cibernético de especial gravedad podría ser motivo suficiente para que un Estado miembro invocara la cláusula de solidaridad de la UE (artículo 222 del Tratado de Funcionamiento de la UE)"[422]. A este respecto, la Comisión de Asuntos Exteriores del Parlamento Europeo

> "opina asimismo que, aunque los ciberataques que ponen en peligro la seguridad nacional deben definirse con arreglo a una terminología común, podría aplicárseles la cláusula de defensa mutua (artículo 42, apartado 7, del TUE), sin perjuicio del principio de proporcionalidad"[423].

Otro aspecto digno de mención es la "integración de las cuestiones vinculadas al ciberespacio en las relaciones exteriores y la Política Exterior y de Seguridad Común de la UE", concretamente en lo que respecta a las consultas con socios internacionales sobre cuestiones referentes al ciberespacio como valor añadido en los diálogos bilaterales entre los Estados miembros y los terceros países, entre los cuales se menciona la especial importancia del mantenido con Estados Unidos en el marco del Grupo de Trabajo UE-Estados Unidos. En este contexto, la Comisión y la Alta Representante se comprometen a trabajar en una política internacional coherente de la UE en el ámbito del ciberespacio con el fin de estrechar su colaboración con los socios y organizaciones internacionales clave, integrar las cuestiones vinculadas al

[422] *Ibid.*, p. 21.

[423] Comisión de Asuntos Exteriores del Parlamento Europeo, *Informe de 17 de octubre de 2012 sobre ciberseguridad y ciberdefensa* [2012/2096(INI)], Unión Europea, Bruselas, 2012, párrafo 3.

ciberespacio en la PESC y mejorar la coordinación de las cuestiones de alcance mundial[424].

En conclusión, la Estrategia de ciberseguridad de la UE aborda las amenazas cibernéticas desde una perspectiva eminentemente de prevención, recuperación y, en lo que respecta a la respuesta, de *law enforcement*, sólo refiriéndose a la ciberdefensa de forma tangencial para posponer la elaboración de un verdadero marco político al respecto, aunque posteriormente el Consejo Europeo fijara 2014 como límite. Más significativo es el énfasis que se hace en la cooperación con la OTAN y con los Estados Unidos, considerados socios claves en materia de ciberseguridad, y la voluntad de hacer de ésta un asunto transversal integrado también en la PESC. Por último, es especialmente importante para el presente análisis el rechazo a la elaboración de un nuevo marco jurídico para el ciberespacio, confirmando la hipótesis de partida de este trabajo que postula la sujeción del uso de la fuerza cibernético al Derecho internacional consuetudinario y convencional del recurso a la fuerza, incluidas las cláusulas de asistencia mutua y de solidaridad, aunque sólo esta última es objeto de referencia expresa en el documento.

8.2 POLÍTICA DE CIBERDEFENSA DE LA OTAN:

Una vez definido el marco regulador de la ciberdefensa en la UE y antes de proceder al estudio de las relaciones entre ésta y la OTAN en dicho ámbito, es preciso exponer de forma breve las directrices políticas por las que el mismo se rige en la Alianza, mucho más influidas por la visión estadounidense de las nuevas amenazas a la seguridad como desafíos que deben ser afrontados desde la óptica militar sin que las soluciones civiles de *law enforcement* tengan tanto peso como en el caso de la Unión.

El punto de partida es el Concepto Estratégico de Lisboa de 2010[425], que menciona los ciberataques de ejércitos y servicios de inteligencia extranjeros, criminales organizados y grupos terroristas y extremistas como un fenómeno

[424] Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *op. cit., supra* (nota 241), p. 17.

[425] Consejo del Atlántico Norte, *op. cit., supra* (nota 228).

cada vez más frecuente, mejor organizado y más costoso en lo que respecta al daño que puede causar a los gobiernos, administraciones, negocios, economías e infraestructuras críticas hasta el punto de amenazar la prosperidad, seguridad y estabilidad euroatlánticas[426]. A ello añade que, con el fin de garantizar que la Alianza consta del conjunto de capacidades necesarias para disuadir y defenderse de cualquier amenaza a la seguridad de sus poblaciones, desarrollará su habilidad para prevenir, detectar, defenderse y recuperarse de los ciberataques, incluso usando el proceso de planificación de la OTAN para coordinar las capacidades nacionales de ciberdefensa, agrupando todos los órganos de la Alianza bajo una protección cibernética centralizada e integrando mejor la conciencia, alerta y respuesta cibernéticas de la OTAN con las de sus miembros[427].

La Política de CIberdefensa de la OTAN[428] desarrolla estas directrices generales partiendo para ello de la premisa, de tintes militares, de que la integridad y funcionamiento de los sistemas de información y comunicación de la Alianza son necesarios para que la misma pueda llevar a cabo sus tareas principales de defensa colectiva y gestión de crisis. Para ello adopta un enfoque comprensivo y coordinado que se propone integrar, por una parte, los aspectos de planificación y desarrollo de capacidades con los mecanismos de respuesta ante ciberataques y, por otra parte, los esfuerzos de la Alianza con los de los aliados, haciendo uso del Proceso de Planificación de Defensa de la OTAN para guiar la inclusión de la ciberdefensa en los marcos nacionales de defensa, centralizando la protección del conjunto de infraestructura segura utilizada por todos los órganos de la Alianza y estableciendo requisitos mínimos para las redes nacionales que están conectadas o procesan información de la OTAN. Todas estas acciones se rigen por los principios de prevención y resiliencia, que exige aumentar el grado de preparación y limitar las disfunciones y sus consecuencias, y no duplicación.

[426] *Ibid.*, párrafo 12.

[427] *Ibid.*, párrafo 19.

[428] División de Diplomacia Pública de la Organización del Tratado del Atlántico Norte, *op. cit., supra* (nota 230).

Sin embargo, como se anunció en el epígrafe relativo a la legítima defensa y los ciberataques, la Política de CIberdefensa de la OTAN rechaza expresamente prejuzgar ninguna respuesta en caso de ofensiva cibernética contra la Alianza o sus miembros, optando por "la ambigüedad estratégica así como la flexibilidad acerca de cómo responder a los diferentes tipos de crisis que incluyen un componente cibernético"[429], de manera que corresponde al CAN decidir discrecionalmente sobre la aplicación de la cláusula de asistencia mutua sobre la base del juicio de razonabilidad que ha sido extensamente detallado en la primera parte de este trabajo. En cambio, sí se afirma que la OTAN proporcionará asistencia coordinada a los aliados que sean víctimas de ciberataques mejorando los mecanismos de consulta, alerta temprana, conciencia de situación e intercambio de información entre ellos articulados en torno al memorando de entendimiento entre las autoridades nacionales de ciberdefensa y el Consejo de Gestión de Ciberdefensa de la OTAN. También se hace énfasis en la necesidad de lograr el compromiso de la comunidad internacional, como será analizado en el siguiente epígrafe.

Finalmente, se señala un conjunto de pasos prácticos a dar, tales como el desarrollo de requisitos mínimos para los sistemas nacionales de información que lleven a cabo tareas fundamentales de la OTAN, la asistencia a los aliados en la consecución de un nivel mínimo de ciberdefensa para la reducción las debilidades de las infraestructuras críticas nacionales, el apoyo de los aliados a otros aliados o a la Alianza en caso de ciberataque, la integración, identificación y priorización del desarrollo de capacidades de ciberdefensa dentro del Proceso de Planificación de Defensa de la OTAN, la evaluación por las autoridades militares de la Alianza del apoyo que la ciberdefensa supone para la conducción de las tareas fundamentales de la OTAN, la definición de requisitos para los Estados no miembros de la Alianza que contribuyen con tropas a las misiones de la misma, la aplicación de estrictos requisitos de autenticación, la mejora de la alerta temprana, la conciencia de situación y el análisis de capacidades, el desarrollo de programas de concienciación y de

[429] *Ibid.*, p. 2.

componentes cibernéticos en los ejercicios de la OTAN y el uso de la experiencia del Centro de Excelencia Cooperativo de Ciberdefensa de Talín.

En resumen, aunque la ciberdefensa se encuentra claramente en el primer plano político de la OTAN, la versión oficial evita pronunciarse sobre el tema central del uso de la fuerza frente a los ciberataques, seguramente por las discrepancias al respecto entre los aliados y por las trabas diplomáticas y de política internacional que supone el recurso al artículo 5 del TAN en el ciberespacio y que impidieron su activación con ocasión de los ataques de 2007 contra Estonia. Como quiera que, dado el escaso desarrollo del marco jurídico al respecto, no se ha considerado políticamente correcto "amenazar" públicamente con el uso de la fuerza, la Política de CIberdefensa de la OTAN opta por la prevención y la resiliencia, basadas en una combinación de desarrollo de capacidades y respuesta rápida, en lugar de la disuasión. Así, se difiere la decisión sobre la legítima defensa colectiva a la evaluación por el CAN del caso concreto, con lo que no sólo se pospone el consenso entre los aliados, sino que además se lanza una severa advertencia más o menos sutil a los posibles ciberagresores.

8.3 ¿SUPONDRÁ LA CIBERDEFENSA UNA NUEVA OPORTUNIDAD PARA LA COOPERACIÓN O UNA RUPTURA DEFINITIVA?

Para una auténtica comparación con las directrices sobre defensa cibernética de la UE y la OTAN será necesario esperar a que aquélla elabore un marco político propiamente de ciberdefensa a lo largo de 2014 -si se cumple el plazo marcado por el Consejo Europeo de diciembre de 2013-. Por ello, a los efectos de este trabajo es preciso atenerse a lo concluido sobre la Estrategia de Ciberseguridad de la Unión, un marco político mucho más amplio centrado en la coordinación de los esfuerzos nacionales de *law enforment* y dentro del cual la ciberdefensa es abordada tan sólo desde la perspectiva de *soft security* de la cláusula de solidaridad del artículo 222 del TFUE, evitándose cualquier referencia a la posible activación de la cláusula de asistencia mutua del artículo

42.7 del TUE, alternativa de *hard security* contemplada empero a nivel más informal por Comisión de Asuntos Exteriores del Parlamento Europeo[430].

No es de esperar que la futura política de ciberdefensa de la UE vaya más lejos que la de la OTAN, si acaso limitándose a dar soporte oficial a la mencionada opinión de dicha Comisión parlamentaria, que a semejanza de la Alianza pospone implícitamente la decisión sobre la legítima defensa colectiva ante ciberataques a una decisión caso por caso que requerirá la unanimidad de los Estados miembros. Sí parece clara la disposición de la Unión y la Alianza a que esta decisión sobre el uso de la fuerza no sólo se base en el consenso de sus respectivos miembros, sino también en el acuerdo entre ambas organizaciones internacionales, como pone de manifiesto el énfasis que sus correspondientes marcos políticos hacen sobre la cooperación y el refuerzo mutuo en el quinto dominio.

De este modo, la Declaración de Chicago 2012 afirma, para abordar las amenazas de ciberseguridad y para mejorar la seguridad común, el compromiso de la OTAN de incrementar la cooperación en este ámbito concreto con otras organizaciones internacionales entre las cuales existe acuerdo con la UE[431], que ocupa un papel privilegiado como socio único y esencial[432]. Por su parte, la Política de Ciberdefensa de la OTAN parte de la consideración del carácter global del ciberespacio y las amenazas que implica para afirmar el compromiso de la Alianza con socios, organizaciones internacionales, academia y sector privado con el objetivo de establecer una cooperación sobre la base de los riesgos compartidos y los valores comunes que incluya la toma de conciencia y la compartición de buenas prácticas[433].

También la UE se muestra muy proclive a cooperar con la OTAN en ciberdefensa, como muestra la voluntad de integrar las cuestiones vinculadas al ciberespacio en las relaciones exteriores y la PESC expresamente

[430] Comisión de Asuntos Exteriores del Parlamento Europeo, *op. cit., supra* (nota 423), párrafo 3.

[431] Consejo del Atlántico Norte, *op. cit., supra* (nota 390), párrafo 49.

[432] *Ibid.*, párrafo 20.

[433] División de Diplomacia Pública de la Organización del Atlántico Norte, *op. cit., supra* (nota 230), p. 2.

manifestada en su Estrategia de Ciberseguridad, en la que también se explicita el compromiso de la Comisión y la Alta Representante de trabajar en una política internacional coherente de la UE en el ámbito del ciberespacio con el fin de estrechar su colaboración con los socios y organizaciones internacionales clave, especialmente con Estados Unidos, en el marco del Grupo de Trabajo UE-Estados Unidos, y la Alianza[434]. Adicionalmente, la Comisión de Asuntos Exteriores del Parlamento Europeo, además de los cinco párrafos dedicados a la colaboración con los Estados Unidos[435], consagra otros tres a la cooperación con la OTAN[436], en los que invoca los valores e intereses estratégicos comunes para reiterar la necesidad de colaboración estrecha en la búsqueda de complementariedades, sin duplicación y respetando las competencias respectivas; de mayor coordinación en lo que respecta a la puesta en común de recursos relativos a la planificación, la tecnología, la formación y los equipos en lo que atañe a la ciberseguridad y la ciberdefensa; y de intercambio de experiencias en particular a efectos de dotar de resiliencia a los sistemas de la Unión.

Por lo tanto, los dos "proveedores de seguridad" europeos parecen coincidir no sólo en su disposición a afrontar el desafío cibernético -completamente nuevo y en menor medida determinado por la brecha de las capacidades militares preexistentes- desde una perspectiva distinta a su tradicional "cooperación bajo rivalidad" y fundada en un difuso reparto de tareas "blandas" y "duras", sino además en la ambigüedad estratégica que han preferido mantener acerca del recurso a la legítima defensa colectiva ante ciberataques, en aras de la flexibilidad y la corrección política y diplomática. De este modo, cuando el caso se plantee y la decisión deba ser tomada parece más posible que nunca que se funde sobre el diálogo previo entre la UE y la OTAN. No obstante, dicho diálogo presenta el riesgo de desvelar el gran punto

[434] Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *op. cit., supra* (nota 241), p. 17.

[435] Comisión de Asuntos Exteriores del Parlamento Europeo, *op. cit., supra* (nota 423), párrafos 52-56.

[436] *Ibid.*, párrafos 49-51.

de conflicto transatlántico y entre los miembros de una y otra organización internacional, su diferente concepción del marco regulatorio del uso cibernético de la fuerza. Efectivamente, mientras la Estrategia de CIberseguridad de la Unión anuncia su preferencia por aplicar el marco jurídico internacional general también en el ciberespacio[437] en una apuesta decidida por la *lege lata*, la Alianza, aunque no se pronuncia oficialmente al respecto, se ve influida por la doctrina militar estadounidense partidaria de una interpretación flexible de lege *ferenda* del Derecho internacional que permita su adaptación a las nuevas circunstancias de hecho, cuyo máximo exponente es el Manual de Talín, dirigido por el ex-teniente coronel de las fuerzas aéreas estadounidenses profesor Michael Schmitt.

Sin duda, la amenaza cibernética, como desafío postmoderno por excelencia y consiguientemente requerido de un enfoque de seguridad igualmente postmoderno y singularmente transversal, en el sentido externo-interno y cívico-militar, supone una gran oportunidad para que la UE explote la naturaleza comprensiva de su PESC y se convierta verdaderamente en el socio único y esencial que Estados Unidos y la OTAN esperan. De este modo, convirtiendo el desarrollo de capacidades militares innovadoras en uno de los pilares de una industria tecnológica llamada a impulsar la economía en tiempos de crisis y manteniendo su liderazgo en materia de instrumentos “blandos” y de *law enforcement*, se convertirá en el “poder inteligente” llamado a asumir una mayor parte de la responsabilidad de la Alianza sobre la defensa regional que la potencia norteamericana confía cada vez más a los aliados europeos.

Si bien no parece previsible que las diferencias ideológicas, de capacidades y presupuestarias entre Estados miembros, así como el carácter intergubernamental de la PCSD, permitan una definición clara de prioridades estratégicas, será necesario recurrir a una geometría variable articulada jurídicamente sobre la Cooperación Estructurada Permanente y políticamente sobre el mecanismo de *pooling and sharing* en la que los socios más capaces y dispuestos, como Reino Unido y Francia -que ya han firmado dos tratados de

[437] Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *op. cit., supra* (nota 241), p. 17.

Defensa y Seguridad el 2 de noviembre de 2010 en la cumbre de Lancaster House[438] - asuman el liderazgo de este proceso. Paralelamente, el mismo fenómeno se habrá de producir en la OTAN por medio de la *Smart Defence*, siendo crucial que los proyectos llevados a cabo en el marco de una u otra organización internacional estén coordinados, por ejemplo, a través de la iniciativa del Mando Aliado de Transformación de la Alianza denominada Marco para la Colaboración Interactiva o *Framework for Collaborative Interaction*[439].

[438] Gobierno del Reino Unido, "Announcement: UK-France Defence Co-operation Treaty announced", *www.gov.uk*, 2010 [disponible en https://www.gov.uk/government/news/uk-france-defence-co-operation-treaty-announced--2, último acceso el 13 de julio de 2014].

[439] Yaniz Velasco, *op. cit., supra* (nota 135), p. 19.

9 CONCLUSIONES:

Este último apartado de conclusiones está consagrado a recoger a modo de corolario mi opinión personal, forjada durante la investigación que ha dado como fruto este trabajo, sobre el futuro de las relaciones entre la UE y la OTAN en general y específicamente en materia de ciberdefensa, así como algunas recomendaciones acerca de la evolución de las mismas en el marco más amplio de la asociación estratégica transatlántica. Los tres primeros apartados se dedican a lo que he considerado los tres grandes desafíos a superar por ambas organizaciones internacionales para garantizar una cooperación fluida, seguidos de mis propuestas al respecto.

9.1 ACTITUDES ESTRATÉGICAS DIVERGENTES:

Partiendo de la premisa de que la competencia en materia de defensa es un componente tradicionalmente esencial de la soberanía estatal, incluso el grupo de Estados más integrado del planeta, como son los miembros de la UE, son muy reticentes a renunciar al control sobre la misma. De este modo, tanto la Unión como la Alianza son organizaciones internacionales de mera cooperación intergubernamental en este ámbito concreto y los principales obstáculos a la cooperación entre ellas derivan de las actitudes de sus respectivos miembros, tanto de los que comparten como de los que no. Así, el primer y acaso más evidente obstáculo a la asociación entre los dos "duopolistas" de la defensa europea, cada vez más conscientes a nivel institucional de la necesidad de sustituir la competencia leal por la colaboración mutuamente beneficiosa, es la distinta actitud de sus miembros hacia el uso de la fuerza, especialmente anticipatoria, el multilateralismo y el liderazgo de Estados Unidos en la seguridad mundial.

Aunque los distintos documentos oficiales de la una y de la otra traídos a colación en este trabajo se esfuerzan por destacar los valores compartidos y los intereses estratégicos comunes de ambas organizaciones internacionales, en una suerte de "dime de qué presumes y te diré de qué careces", lo cierto es que determinados planteamientos propios de la cultura geoestratégica anglo-americana, a menudo secundados por los países del Este como reacción a su

pasado soviético, encajan difícilmente con el deseo de un orden internacional multilateral y regulado jurídicamente que Habermas y Derrida (2003, p. 295) predicaban de la Europa continental e hicieron tambalearse la superestructura de seguridad euroatlántica y la misma recién nacida PESD en los momentos de predominio del neoconservadurismo en la otra orilla del Atlántico durante la administración Bush.

Superada la crisis que alcanzó su clímax con la invasión de Irak en 2003, Norteamérica y el Viejo Continente parecen, por una parte, nuevamente conscientes de que constituyen una "comunidad de seguridad" y que, a pesar de sus diferencias, comparten en lo esencial un mismo núcleo de valores e intereses frente a las potencias emergentes o reemergentes, a los Estados fallidos y a los actores no estatales que pueden ponerlos en peligro. Por otra parte, parecen por primera vez conscientes de la necesidad de repartirse de forma más equitativa la responsabilidad sobre la protección de esos valores e intereses en un escenario geoestratégico en el que la UE reclama un mayor protagonismo y Washington contrarresta la reducción de recursos con una concentración más eficiente de los mismos en sus áreas prioritarias de Oriente Medio y Asia-Pacífico.

En este sentido, la administración Obama, aunque mantiene en la Estrategia Nacional de Seguridad de 2010 el objetivo de asegurar el liderazgo estratégico global de Estados Unidos como único Estado capaz de llevar a cabo operaciones a gran escala en cualquier lugar del mundo, ha supuesto un giro hacia cierto multilateralismo eficaz y ha abandonado la doctrina de legítima defensa preventiva de su predecesor, propiciando un acercamiento a las potencias europeístas que fue correspondido por el Presidente francés Nicolás Sarkozy devolviendo a Francia a la estructura de mandos de la Alianza.

Más compleja es la cuestión en el ámbito de la ciberdefensa, donde surge el problema adicional de la aplicación del marco jurídico preexistente y de su adaptación a un medio esencialmente distinto del mundo físico para el que fue previsto o la marginación de esta regulación por obsoleta y su sustitución por nuevos estándares incluso políticos o meramente fácticos, como se plantea en el siguiente epígrafe.

9.2 VISIONES DIFERENTES DEL MARCO JURÍDICO DEL USO DE LA FUERZA CIBERNÉTICO:

En este debate se manifiesta nuevamente la diferencia ideológica entre el mundo anglosajón y postsoviético, más proclive considerar el orden jurídico internacional un instrumento que debe servir a fines morales y políticos -como la paz y la seguridad globales- y consiguientemente debe considerarse una realidad dinámica que evoluciona para cumplir sus propósitos, y la Europa continental occidental , que concibe el ordenamiento internacional presidido por la CNU como el garante último de los valores en los que se basa la civilización y en consecuencia un fin en sí mismo merecedor de la mayor protección. En el ámbito cibernético, la diferente concepción del Derecho internacional se traduce en el predominio de una visión de *lege lata* en la UE frente a una perspectiva de *lege ferenda* preponderante en la doctrina de la Alianza influida de forma determinante por la literatura científica norteamericana elaborada por autores vinculados al ejército estadounidense.

Habrá que esperar a la política de ciberdefensa de la UE para determinar en qué medida puede hacerse uso de la cláusula de asistencia mutua en el ciberespacio, aunque no parece probable que los Estados miembros alcancen un acuerdo a este respecto. Hasta el momento, todo lo que tenernos son los artículos 42.7 del TUE y 5 del TAN, respetuosos de los artículos 2.4 y 51 de la CNU y modulados por el concepto de infraestructuras críticas cuyo daño, junto a la pérdida de vidas humanas o lesiones a personas, parece el único supuesto que aceptablemente puede justificar tanto para la Unión como para la Alianza el recurso a la fuerza en respuesta a una operación cibernética. La práctica ha mostrado con ocasión de los atentados contra Estonia de 2007 que la dificultad de establecer la responsabilidad y el coste político de una acusación en este sentido, en ausencia de un estándar claramente definido de lo que se considera ataque armado en el ciberespacio, son demasiado elevados como para ni siquiera plantearse el ejercicio de la legítima defensa.

9.3 FALTA DE VOLUNTAD POR PARTE DE LOS ESTADOS MIEMBROS DE LA UE:

No obstante, las diferencias de cultura estratégica y de concepción del orden jurídico internacional entre Estados que, al fin y al cabo, nadie discute que comparten un *ethos* común no es en realidad un obstáculo tan insalvable como la falta de voluntad de los Estados miembros de la UE de definir un conjunto de prioridades estratégicas y comprometerse con el desarrollo de capacidades militares que permitan postular a la PCSD como un candidato creíble a "proveedor de seguridad" internacional en pie de igualdad con la OTAN e incluso con Estados Unidos. Sin un compromiso interno fuerte a nivel de la Unión es inviable reclamar un reparto de la responsabilidad sobre la defensa de Europa y del mundo más equilibrado que garantice a la vez la supervivencia de la PCSD y de la Alianza y evite la competencia y las consiguientes duplicaciones entre ellas, maximizando de este modo la eficiencia de ambas.

El problema esencial de la cooperación entre UE y OTAN en materia de ciberdefensa es el mismo que aqueja a la PESC y particularmente a la propia PCSD desde su origen, esto es, la falta de implicación en una política exterior y de seguridad y defensa supranacional coherente por parte de unos Estados miembros que, por diferencias de cultura geoestratégica, tradición neutral, ambiciones de potencia regional o déficit de capacidades, priman su políticas exteriores y estrategias de seguridad y defensa nacionales y consideran a la Unión como un foro de coordinación de las mismas, función que además ya cumple la Alianza de manera prioritaria por su más largo recorrido histórico y por contar con Estados Unidos como miembro.

Las nuevas amenazas de seguridad como la ciberdefensa constituyen una oportunidad para superar este egoísmo nacionalista, impropio de la solidaridad sobre la que se asienta la Unión, porque, por una parte, son fenómenos globales que trascienden las fronteras estatales y sólo pueden ser combatidos a nivel supranacional, sin mencionar que la protección de las redes tiene que ser completa porque están interconectadas y el eslabón débil hace que se rompa la cadena, y, por otra parte, porque la tecnología necesaria requiere un

esfuerzo de investigación y desarrollo demasiado elevado como para ser afrontado por los Estados individualmente y las posibilidades de alcanzar sinergias son casi ilimitadas.

9.4 PROPUESTAS:

En consecuencia, los Estados miembros no pueden conformarse con una Venus europea autolimitada al ámbito civil, de manera que la PCSD acabe constituyendo un mero apéndice de la OTAN liderada por el Marte norteamericano. Ya ha quedado claro que una apuesta excesiva por los instrumentos de *soft power* condenaría a Europa a ser el "descanso del guerrero" de su socio transatlántico, restringiéndose a la lavar los platos que éste ensucie en sus despliegues de fuerza bruta, orquestados a través de la OTAN o prescindiendo de sus aliados europeos en un alarde de unilateralismo. Por ello, es vital que los Estados miembros se comprometan con una PCSD fuerte construida a través del método de los pequeños pasos, la geometría variable que ha demostrado ser el cauce más fructífero para la integración y que en el ámbito de la defensa se vea dotado de una vía específica en la forma de una Cooperación estructurada Permanente. Así Reino Unido y Francia deben asumir el liderazgo y esforzarse por lograr un desarrollo de capacidades lo más eficiente posible.

También es evidente que este proceso en ningún caso debe implicar la ruptura con el otro lado del Atlántico, ya que ambas orillas tienen la responsabilidad de colaborar en la protección de un conjunto de valores compartidos merecedores de la mayor protección en las relaciones internacionales para el bien de la comunidad internacional. En este sentido, la UE puede apelar a su mayor autoridad moral para modular e incluso contrapesar el paroxismo militar americano, siendo para ello condición previa necesaria ganarse el respeto y la credibilidad de su aliado convirtiéndose realmente en un socio único y esencial. Sólo de este modo será posible construir una nueva asociación estratégica transatlántica mucho más equilibrada entre iguales de la cual las relaciones entre la UE y la OTAN

constituyan el núcleo y que conduzca al establecimiento de una “pax euroamericana” beneficiosa para el mundo en su conjunto.

El ámbito cibernético es idóneo para esta evolución, ya que se trata de un dominio nuevo en el que no es posible establecer áreas de influencia geoestratégica ni fronteras nacionales, que aún está por regular plenamente y en el que el progreso tecnológico presenta unas posibilidades casi ilimitadas para el desarrollo de nuevas capacidades de defensa por actores que no son potencias militares en el mundo físico, como por ejemplo China, concediendo a la oportunidad y a la vez imponiendo la responsabilidad a Europa de tomar el carril cibernético para seguir el ritmo a Estados Unidos en la carrera de la seguridad mundial.

Sin embargo, a falta de conocer los términos en los que la futura política de ciberdefensa de la UE aborde el asunto pendiente de la legítima defensa colectiva frente a ciberataques, principal fuente de potenciales rupturas llegado el caso de tener que adoptar una decisión, tan esencial como el desarrollo de capacidades civiles y militares es que los Estados miembros y los aliados fomenten un consenso a nivel europeo y, de forma más ambiciosa, a nivel de las Naciones Unidas sobre la interpretación de los artículos 2.4 y 51 de la CNU en el quinto dominio. Consciente de lo utópico de esta afirmación y de que será la práctica la que determine el marco aplicable en un orden internacional cada vez más político que jurídico, Europa está llamada a defender el “multilateralismo eficaz” que Solana convirtió en enseña de la PESC y lograr que aquella determinación se realice con la mayor participación posible del conjunto de la comunidad internacional.

10 BIBLIOGRAFÍA:

Agencia de Normalización de la Organización del Tratado del Atlántico Norte, "Glosario de la OTAN de términos y definiciones", *Documento AAP-6(2012)(2)*, Organización del Tratado del Atlántico Norte, Bruselas, 2012.

Ago, Roberto, "Adición al octavo informe sobre la responsabilidad de los Estados", *Anuario de la Comisión de Derecho Internacional* [Doc. A/CN.4/318/Add. 5 a 7], volumen II, 1980.

Albright, Madeleine, "The Right Balance Will Secure NATO's Future", *Financial Times*, 7 de diciembre, 1998.

Alexandrov, Stanimir, *Self-Defence Against the Use of Force in International Law*, Leiden, Martinus Nijhoff Publishers,1996.

Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *Comunicación conjunta de 7 de febrero de 2013 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro* [JOIN(2013) 1 final], Unión Europea, Bruselas, 2013.

Arpagian, Nicolas, "La cyberattaque, nouvelle arme de guerre des États", *www.franceinfo.fr*, 2013 [disponible en http://www.franceinfo.fr/high-tech/vie-quotidienne/article/la-cyberattaque-nouvelle-arme-de-guerre-des-etats-239231, último acceso el 22 de junio de 2014].

Arteaga Martín, Félix, "La Política Europea de Seguridad y Defensa", en Instituto Español de Estudios Estratégicos, "La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa", *Cuadernos de Estrategia*, volumen 145, número de marzo, 2010, pp. 31-67.

Asamblea de Defensa y Seguridad de la Unión Europea Occidental, “The EU-NATO Berlin plus agreements”, *Assembly Facts Sheet 14*, Unión Europea Occidental, París, 2009.

Asamblea General de las Naciones Unidas, *Documento Final de la Cumbre Mundial, Organización de las Naciones Unidas*, Nueva York, 2005.

Asamblea General de las Naciones Unidas, *Documentos 1123 (I/8, 6 UNCIO), 65 (1945), 784 (I/1/27, 6 UNCIO), 336 (1945), 885 (I/1/34, 6 UNCIO) y 387 (1945)*, Organización de las Naciones Unidas, San Francisco, 1945.

Asamblea General de las Naciones Unidas, *Resolución 2625 (XXV)*, Organización de las Naciones Unidas, Nueva York, 1970.

Asamblea General de las Naciones Unidas, Resolución 3314 (XXIX) sobre la definición de la agresión, Organización de las Naciones Unidas, Nueva York, 1974.

Asamblea General de las Naciones Unidas, *Resolución de 30 de enero de 2004 sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales*, Organización de las Naciones Unidas, Nueva York, 2004.

Asmus, Ronald, Blackwill, Robert y Larrabee, Stephen, “Can NATO Survive?”, *The Washington Quarterly*, volumen 19, número 2, 1996, p. 79 y ss.

Ballesteros Martín, Miguel Ángel, “La Política Común de Seguridad y Defensa tras el Consejo Europeo de Diciembre de 2013”, *Documento de Análisis 03/2014*, Instituto Español de Estudios Estratégicos, Madrid, 2014 [disponible en http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA03-2014_PoliticaComunSegyDef_MABM.pdf, último acceso el 26 de junio de 2014].

Barnier, Michel, *WEU Assembly Press Release 3/2003 of 12 February 2003: Eurozone for Defence*, Asamblea Parlamentaria de la Unión Europea Occidental, París, 2003.

Baud, Michel, "La cyberguerre n'aura pas lieu mais il faut s'y préparer", *Politique étrangère*, volumen 77, número 2, 2012, pp. 305-314.

Baudin, Laura, *Les cyber-attaques dans les conflits armées. Qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire*, París, L'Harmattan, 2014.

Biermann, Rafael, "Inter-Organizationalism in Theory and Practice, Military Crisis Management: The Challenge of Inter-Organizationalism", *Studia Diplomatica*, volumen 62, número 3, 2009, pp. 7-13.

Biermann, Rafael, "Rivalry Among International Organizations Bringing Power Back In", *Paper for the Panel The European Union and Transatlantic Relations of 14 September 2007*, Turín, 2007 [disponible en http://www.ies.be/files/documents/JMCdepository/Rafael%20Biermann,%20Rivalry%20Among%20International%20Organizations.%20Bringing%20Power%20Back%20In.pdf, ultimo acceso el 5 de Julio de 2014].

Biermann, Rafael, "Towards a theory of inter-organizational networking. The Euro-Atlantic security institutions interacting", *The Review of International Organizations*, volumen 3, número 2, 2008, pp. 151-177.

Biscop, Sven (ed.), "The Value of Power, the Power of Values: A Call for an EU Grand Strategy", *Egmont Paper 33*, Real Instituto Egmont de Relaciones Internacionales, 2009.

Biscop, Sven y Coelmont, Jo, "Defence, The European Council Matters", *Security Policy Brief 51*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013.

Biscop, Sven, “And What Will Europe Do? The European Council and Military Strategy”, *Security Policy Brief 46*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013.

Biscop, Sven, “Pool it, Share it, Use it: The European Council on Defence”, *Security Policy Brief 44*, Real Instituto Egmont de Relaciones Internacionales, Bruselas, 2013b.

Biscop, Sven, NATO, “ESDP and The Riga Summit: No Transformation Without Re-Equilibration”, *Egmont Paper 11*, Real Instituto Egmont de Relciones Internacionales, Bruselas, 2006.

Blum, Yehuda, “State Response to Acts of Terrorism”, *German Yearbook of International Law*, volumen 19, 1976, pp. 223-237.

Bowett, Derek, *Self-defence in International Law*, Praeger, Nueva York, 1958.

Brownlie, Ian, *Principles of Public International Law*, Oxford, Oxford Press University, 1990.

Buzan, Barry y Waeber, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003.

Bweless, Charles, “Peut-on dissuader dans le cyberespace? ”, *Revue de la défense nationale*, número 731, 2010, pp. 25 a 30.

Calduch Cervera, Rafael, “El Tratado de Lisboa y la amenaza terrorista en Europa”, en Martín y Pérez de Nanclares, José (coord.), *El Tratado de Lisboa. La salida de la crisis constituciona*l, Madrid, Iustel, 2008, pp. 451-468.

Cameron, Fraser y Quille, Gérard, “The Future of ESDP”, *European Policy Centre Working Paper*, Centro Político Europeo, Bruselas, 2004.

Cannizzaro, Enzo, “NATO’s New Strategic Concept and the Evolving Legal Regulation of the Use of Force”, *The International Spectator*, volume 36, número 1, 2001, p. 67-74.

Carrillo Salcedo, Juan Antonio, *Curso de Derecho internacional Público*, Madrid, Tecnos, 1991.

Centro Superior de Estudios de la Defensa Nacional, “Guerra cibernética: Aspectos organizativos”, *Documento del Grupo de Trabajo nº 3 del XXXIII Curso de Defensa Nacional*, Ministerio de Defensa, Reino de España, Madrid, 2013.

Chafos, Timothy, *The European Union’s Rapid Reaction Force and the North Atlantic Treaty Organization Response Force: A Rational Division of Labor for European Security*, Washington D. C., Storming Media, 2003.

Chivvis, Christopher, “Recasting NATO’s Strategic Concept, Possible Directions for the United States”, *Occasional Paper*, RAND Corporation, Santa Mónica, California, 2009 [disponible en http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP280.pdf, ultimo acceso el 5 de julio de 2014].

Clinton, Hillary, *Remarks at the NATO Strategic Concept Seminar*, Washington D. C., 2010.

Coelmont, Jo y De Langlois, Maurice, “Recalibrating CSDP-NATO Relations : The Real Pivot”, *Security Policy Brief 47*, Real Instituto Egmont de Relaciones Internacionales, 2013.

Colom Piella, Guillem, “Los Límites de la Política Común de Seguridad y Defensa”, *Revista General de la Marina*, número de abril, 2014, pp. 447-454.

Comisión de Asuntos Constitucionales del Parlamento Europeo, *Opinión de 10 de octubre de 2012 para la Comisión de Asuntos Exteriores sobre las*

cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa, Unión Europea, Bruselas, 2012.

Comisión de Asuntos Exteriores del Parlamento Europeo, *Informe de 17 de octubre de 2012 sobre ciberseguridad y ciberdefensa* [2012/2096(INI)], Unión Europea, Bruselas, 2012.

Comisión de Asuntos Exteriores del Parlamento Europeo, *Informe de 31 de octubre de 2012 sobre las cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa* [2012/2223(INI)], Unión Europea, Estrasburgo, 2012.

Comisión Europea, *Documento de 10 de julio de 2007 sobre la reforma de Europa para el siglo XXI* [COM (2007) 412 final], Comunidades Europeas, Bruselas, 2007.

Comisión Europea, *Propuesta de 7 de febrero de 2013 de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión* [COM(2013) 48 final], Unión Europea, Bruselas, 2013.

Condorelli, Luigi, "Les attentats du 11 septembre et leurs suites: où va le droit international", *Revue Générale de Droit International Public*, número 105, 2001, pp. 829-848.

Condron, Sean, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law and Technology*, volumen 20, 2007, pp. 404 y ss.

Congreso de los Estados Unidos, *Joint Resolution number 114 Authorizing the Use of Force Against Iraq, publication 107-243, 16 October 2002*, Estados Unidos de América, Washington D. C., 2002.

Congreso de los Estados Unidos, *US Patriot Act of 26 October 2001* [42 U.S.C. 5195c(e)], Estados Unidos de América, Washington D. C., 2001.

Consejo de la Unión Europea, “Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección”, *Diario Oficial de las Comunidades Europeas número L 345/75 de 23 de diciembre de 2008*, Unión Europea, Bruselas, 2008.

Consejo de la Unión Europea, *Comunicado de Prensa de la Sesión número 3157 del Consejo de Asuntos Exteriores, 22 y 23 de marzo de 2012* [7849/12 PRESSE 117 PR CO 18], Unión Europea, Bruselas, 2012.

Consejo de la Unión Europea, *Estrategia Europea de Seguridad de 12 de diciembre de 2003: Una Europa más segura en un mundo mejor*, Unión Europea, Bruselas, 2003 [disponible en http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf, último acceso el 26 de junio de 2014].

Consejo de la Unión Europea, *EU-US Summit Joint Statement of 20 November 2010* [16726/10 PRESSE 315], Unión Europea, Lisboa, 2010 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/117897.pdf, último acceso el 1 de julio de 2014].

Consejo de la Unión Europea, *German Presidency Paper of 24 February 1999: Informal Reflection at WEU on Europe’s Security and Defence*, Unión Europea, Bonn, 1999.

Consejo de la Unión Europea, *Ofrecer seguridad en un mundo en evolución. Informe de 11 de diciembre de 2008 sobre la aplicación de la Estrategia Europea de Seguridad* [S407/08], Unión Europea, Bruselas, 2008 [disponible en http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf, último acceso el 26 de junio de 2014].

Consejo de Ministros de la Unión Europea Occidental, *Pertersberg Declaration of 19 June 1992*, Unión Europea Occidental, Bonn, 1992. 101

Consejo de Seguridad de las Naciones Unidas, *Resolución 611 de 25 de abril 1988 sobre Israel-Túnez*, Organización de las Naciones Unidas, Nueva York, 1988.

Consejo de Seguridad, *Documentos S/RES/1368, de 12 de septiembre de 2001, y S/RES/1373, de 28 de septiembre de 2001*, Organización de las Naciones Unidas, Nueva York, 2001.

Consejo del Atlántico Norte, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the Northern Treaty Organisation of 19 November 2010*, Organización del Tratado del Atlántico Norte, Lisboa, 2010.

Consejo del Atlántico Norte, *Bucharest Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008*, Organización del Tratado del Atlántico Norte, Bucarest, 2008.

Consejo del Atlántico Norte, *Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012* [Press Release (2012) 062], Organización del Tratado del Atlántico Norte, 2012 [disponible en http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease, ultimo acceso el 12 de Julio de 2014].

Consejo del Atlántico Norte, *Final Communiqué of the North Atlantic Council Summit of 24 April 1999*, Organización del Tratado del Atlántico Norte, Washington, D. C., 1999.

Consejo del Atlántico Norte, *Prague Summit Declaration, the North Atlantic Council of 21 November 2002*, Organización del Tratado del Atlántico Norte, Praga, 2002 [disponible en http://www.nato.int/docu/pr/2002/p02-127e.htm, último acceso el 5 de julio de 2014].

Consejo del Atlántico Norte, *Riga Summit Declaration of 29 November 2006*, Organización del Tratado del Atlántico Norte, Riga, 2006 [disponible en http://www.nato.int/docu/pr/2006/p06-150e.htm, último acceso el 5 de julio de 2014].

Consejo Europeo, *Annex III to the European Council of Cologne: Presidency Report on Strengthening the Common European Policy on Security and Defence*, Unión Europea, Colonia, 1999.

Consejo Europeo, *Conclusiones de la Presidencia del Consejo Europeo de 11 de diciembre de 1999*, Unión Europea, Helsinki, 1999 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/00300-r1.es9.htm, último acceso el 17 de julio de 2014].

Consejo Europeo, *Conclusiones del Consejo Europeo de Bruselas del 13 y 14 de diciembre de 2012* [EUCO 205/12], Unión Europea, Bruselas, 2012 [disponible en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/134371.pdf, último acceso el 28 de junio de 2014].

Consejo Europeo, *Conclusiones del Consejo Europeo de Bruselas del 19 y 20 de diciembre de 2013* [EUCO 217/13], Unión Europea, Bruselas, 2013 [disponible en http://consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/140263.pdf, último acceso el 28 de junio de 2014].

Corte Internacional de Justicia, *Opinión consultiva de 8 de julio de 1996 sobre legalidad de la amenaza o el uso de las armas nucleares*, Organización de las Naciones Unidas, La Haya, 1996.

Corte Internacional de Justicia, *Sentencia de 12 de diciembre de 1996 en el asunto de las plataformas petrolíferas*, Organización de las Naciones Unidas, La Haya, 1996.

Corte Internacional de Justicia, *Sentencia de 17 de junio de 1986 en el asunto de las actividades militares y paramilitares en y contra Nicaragua*, Organización de las Naciones Unidas, La Haya, 1986.

Corte Internacional de Justicia, *Sentencia de 19 de diciembre de 2005 en el asunto de las actividades armadas en el territorio del Congo*, Organización de las Naciones Unidas, La Haya, 2005.

Corte Internacional de Justicia, *Sentencia de 6 de noviembre de 2003 en el asunto de las plataformas petrolíferas*, Organización de las Naciones Unidas, La Haya, 2003.

Corte Internacional de Justicia, *Sentencia de 9 de abril de 1949 en el asunto del estrecho de Corfú*, Organización de las Naciones Unidas, La Haya, 1949.

Cortes del Reino de España, "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas", *Boletín Oficial del Estado número 102 de 29 de abril de 2011 páginas 43.370-43.380*, Reino de España, 2011.

Coşkun, Bezen Balamir, "Does <<strategic culture>> matter? Old Europe, New Europe and the transatlantic security", *Perceptions*, número de verano-otoño, 2007, pp. 71-90.

Crawford, James, *The International Law Commission´s Articles on State Responsibility*, Cambridge, Cambridge University Press, 2002.

D'Oléon, Michel y Jopp, Mathias, "The way ahead for European defence cooperation", en Martin, Lawrence y Roper, J. (eds.), *Towards a common defence policy*, París, Instituto de Estudios Estratégicos de la Unión Europea Occidental, 1995, pp. 98 y ss.

De Joop Scheffer, Jaap, *Speech by NATO Secretary General Jaap de Hoop Scheffer at the National Defense University on 29 January 2004*, Organización del Tratado del Atlántico Norte, Washington, 2004 [disponible

en http://www.nato.int/docu/speech/2004/s040129a.htm, último acceso el 5 de julio de 2014].

Dehousse, Franklin y Galer, Benoît, “De Saint-Malo a Feira: les enjeux de la renaissance du projet de defense européenne”, *Studia Diplomatica*, volumen 52, número 4, Bruselas, 1999.

Deighton, Anne, “The European Security and Defence Policy”, *Journal of Common Market Studies*, volume 40, número 4, 2002, pp. 719-741.

Deutsch, Karl, *Political community and the North Atlantic area*, Princeton, Nueva Jersey, Princeton University Press, 1957.

Díez de Velasco, Manuel, *Instituciones de Derecho Internacional Público*, Madrid, Tecnos, 2013.

Dinstein, Yoram, *War, Aggression and Self-Defence*, Cambridge, Cambridge University Press, 2001.

Dirección General de Políticas Externas de la Unión del Parlamento Europeo, *Note of 12 September 2006 on the European Security and Defence Policy. From the Helsinki Headline Goal to the EU Battlegroups*, Parlamento Europeo, Unión Europea, Bruselas, 2006 [disponible en http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede030909noteesdp_/sede030909noteesdp_en.pdf, ultimo acceso el 28 de junio de 2014].

División de Diplomacia Pública de la Organización del Tratado del Atlántico Norte, *Defending the Networks. The NATO Policy on Cyber Defence 2011*, Organización del Tratado del Atlántico Norte, Bruselas, 2011 [disponible en http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf, ultimo acceso el 25 de junio de 2014].

Fernández Tomás, Antonio, “El recurso al artículo quinto del Tratado de Washington tras los acontecimientos del 11 de septiembre: mucho ruido y

pocas nueces", *Revista Española de Derecho Internacional*, volumen 53, 2001, pp. 205-226.

Forsberg, Tuomas y Herd, Graeme, *Divided West. European Security and the Transatlantic Relationship*, The Royal Institute of International Affairs, Londres, 2006.

Franck, Thomas, "When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?", *Washington Journal of Law and Policy*, volumen 5, 2001, pp. 51 y ss.

Franck, Thomas, *Recourse to Force: State Action Against Threats and Armed Attacks*, Cambridge, Hersch Lauterpatch Memorial Lectures, 2002.

Garden, Timothy, "The future of ESDP-defence capabilities for Europe", *The International Spectator*, volume 38, número 3, 2003, pp. 7-14.

Gärtner, Heinz y Cuthberson, Ian (eds.), *European Security and Transatlantic Relations after 9/11 and the Iraq War*, Nueva York, Palgrave Macmillan, 2005.

Garwood-Gowers, Andrew, "Israel's Airstrike on Syria's Al-Kibar Facility: A Test Case for the Doctrine of Pre-Emptive Self-Defence?", *Journal of Conflct and Security Law*, volumen 16, 2011, pp. 263-291.

Gill, Terry y Ducheine, Paul, "Anticipatory Self-Defense in the Cyber Context", *International Law Studies of the US Naval War College*, volumen 89, 2013, pp. 438-471.

Glennon, Michael, "Preempting Terrorism: The Case for Anticipatory Self-Defense", *The Weekly Standard*, 28 de enero, 2002, pp. 24 y ss.

Gnesotto, Nicole (ed.), *Política de Seguridad y Defensa de la Unión Europea*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2004.

Gnesotto, Nicole, “Visions of the other”, en Lindstrom, Gustav (ed.), *Shift or Rift: Assessing US-EU relationships after Iraq*, París, Instituto de Estudios de Seguridad de la Unión Europea, 2003, pp. 7 y ss.

Gobierno de la República Federal Alemana y Gobierno del Reino de Suecia, “European Imperative, Intensifying Military Cooperation in Europe”, *Food for Thought of November 2010*, República Federal Alemana y Reino de Suecia, Berlín y Estocolmo, 2010 [disponible en http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260511deseinitiative_/sede260511deseinitiative_en.pdf, ultimo acceso el 28 de junio de 2014].

Gobierno del Reino de los Países Bajos, *Government response of 6 April 2012 to the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law on cyber warfare*, Reino de los Países Bajos, La Haya, 2012.

Gobierno del Reino Unido, “Announcement: UK-France Defence Co-operation Treaty announced”, *www.gov.uk*, 2010 [disponible en https://www.gov.uk/government/news/uk-france-defence-co-operation-treaty-announced--2, último acceso el 13 de julio de 2014].

Gobierno del Reino Unido, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review of 19 October 2010*, Reino Unido de la Gran Bretaña e Irlanda del Norte, 2010 [disponible en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf, ultimo acceso el 16 de julio de 2014].

Gompert, David, “What does America want of Europe?” , en Lindstrom, Gustav (ed.), Shift or Rift: *Assessing US-EU relationships after Iraq*, París, Instituto de Estudios de Seguridad de la Unión Europea, 2003, p. 56 y ss.

González Campos, Julio Diego, Sánchez Rodríguez, Luis Ignacio y Andrés Sáenz de Santa María, María Paz, *Curso de Derecho Internacional Público*, Madrid, Aranzadi, 2002.

Grupo de Expertos sobre el Nuevo Concepto Estratégico de la OTAN, *NATO 2020: assured security; dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO of 17 May 2010*, Organización del Tratado del Atlántico Norte, Bruselas, 2010.

Habermas, Jürgen y Derrida, Jacques, "February 15, or What Binds Europeans Together: A Plea for a Common Foreign Policy, Beginning in the Core of Europe", *Constellations*, volumen 10, número 3, 2003, pp. 291-296 [disponible en http://platypus1917.org/wp-content/uploads/archive/rgroups/2006-chicago/habermasderrida_europe.pdf, ultimo acceso el 13 de Julio de 2014].

Haine, Jean-Yves y Gnesotto, Nicole (eds.), *ESDP - The first five years (1999-2004)*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2004.

Harrison Dinniss, Heather, *Cyber Warfare and the Laws of War*, Cambridge, Cambridge University Press, 2012.

Häußler, Ulf, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty", *International Cyber Security Legal & Policy Proceedings 2010*, Centro de Excelencia Cooperativo de Ciberdefensa, Talín, 2010, pp. 100–126.

Heftendorn, Helga, "From an Alliance of Commitment to an Alliance of Choice: The Adaptation of NATO in a Time of Uncertainty", en Cottey, Andrew, *Security in the New Europe*, Nueva York, Palgrave Macmillan, 2007, pp. 161-180.

Heisbourg, François, “The European Security Strategy is not a Security Strategy” en Everts, Stevens y otros, *A European Way of War*, Londres, Centre for Economic Reform, 2004, pp. 27-39.

Herdegen, Matthias, “Military intervention matter of dispute in transatlantic relations”, *Revista Colombiana de Derecho Internacional*, número 10, 2007, pp. 199-208.

Hofmann, Stephanie y Reynolds, Christopher, “EU-NATO Relations: Time to Thaw the <<Frozen Conflict>>”, *Stiftung Wissenschaft und Politik Comments 12*, Stiftung Wissenschaft und Politik, Berlín, 2007.

Hofmann, Stephanie, “Overlapping Institutions in the Realm of International Security: The Case of NATO and ESDP”, *Perspectives on Politics*, volumen 7, número 1, 2009, pp. 45-53.

Hoge, Warren, “NATO Chief criticizes terror <<gap>>”, *International Herald Tribune*, 12 de noviembre, 2004.

Hollis, Duncan, “Why States need and International Law for information operations”, *Lewis and Clark Law Review*, volumen 11, 2007, p. 1023.

Howorth, Jolyon, “NATO and ESDP: Institutional Complexities and Political Realities”, *Politique Étrangère*, número 4, 2009, pp. 95-107.

Howorth, Jolyon, *European integration defence: the ultimate challenge?*, París, Instituto de Estudios de Seguridad de la Unión Europea Occidental, 2000.

Ipsen, Knut, *Rechtsgrundlagen und Institutionalisierung der atlantisch-westeuropäischen Verteidigung*, Hamburg, Hansischer Gildenverlag Heitmann, 1967.

Ismay, Hastings, *NATO: the first five years, 1949-1954*, Utrecht, Bosch, 1954.

Jefes de Estado y de Gobierno de la Unión Europea y Organización del Tratado del Atlántico Norte, *EU-NATO declaration of 16 December 2002 on ESDP*,

Unión Europea y Organización del Tratado del Atlántico Norte, Bruselas, 2002 [disponible en http://www.consilium.europa.eu/uedocs/cmsUpload/73803%20-%20Solana%20-%20Permanent%20arrangements%20+%20NATO%20declaration.pdf, último acceso el 9 de julio de 2014].

Jefes de Estado y de Gobierno de la Unión Europea*, Agreement between the Member States of the European Union of 17 November 2003 concerning the status of military and civilian staff seconded to the institutions of the European Union, of the headquarters and forces which may be made available to the European Union in the context of the preparation and execution of the tasks referred to in Article 17(2) of the Treaty on European Union, including exercises, and of the military and civilian staff of the Member States put at the disposal of the European Union to act in this context* [OJ C 321/6], Unión Europea, Bruselas, 2003.

Jessup, Philip, *A Modern Law of Nations, North Haven*, Archon Books, 1968.

Kagan, Robert, "Power and Weakness", *Policy Review*, número 113, 2002 [disponible en https://www.mtholyoke.edu/acad/intrel/bush/kagan.htm, ultimo acceso el 17 de julio de 2014].

Kagan, Robert, *Of Paradise and Power: America and Europe in the New World Order*, Nueva York, Ramdom House, 2003.

Kay, Sean, *NATO and the Future of European Security. Europe Today*, Washinton D. C., Rowman and Littlefield, 1998.

Kovacs, Charles, "US-European Relations from the Twentieth to the Twenty-First Century", *European Foreign Affairs Journal*, volumen 8, 2003, pp. 435 y ss.

Krenzler, Horst y Schomaker, Astrid, “A new Transatlantic Agenda, European Foreign Affairs Review”, *European Foreign Affairs Review*, número 1, 1996, pp. 9-28.

Kulich, Stanislav, “The concept of division of labour between the EU and NATO: An elusive search for an optimal partition of security tasks”, Trabajo de Fin de Máster, King’s College, Universidad de Londres, Reino Unido, 2010.

La Casa Blanca, *The National Security Strategy of the United States*, Estados Unidos de América, Washington D. C., 2002 [disponible en http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/, ultimo acceso el 30 de junio de 2014].

Laursen, Finn y otros, “The Institutional Dynamics of Euro-Atlnatic Integration”, en Mouritzen, Hans y Wivel, Anders (eds.), *The Geopolitics of Euro-Atlantic Integration*, Londres, Routledge, 2005, pp. 43-69.

Lenzi, Guido, “The WEU between NATO and EU”, *Studia Diplomatica*, volumen 51, 1998, pp. 167 y ss.

Levasseur, Alain y Scott, Richard, *The Law of the European Union: A New Constitutional Order: Materials and Cases*, Durham, Carolina del Norte, Carolina Academic Press, 2001.

Link, Werner, “Die NATO im Gefl echt internationaler Organisationen“, *Aus Politik und Zeitgeschichte*, volumen 49, número 11, 1999, p. 9 y ss.

Marsal Muntala, Jordi, “Las relaciones transatlánticas”, en Instituto Español de Estudios Estratégicos, *La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa*, Cuadernos de Estrategia, volumen 145, número de marzo, 2010, pp. 174-204.

Martín y Pérez de Nanclares, José y Urrea Corres, Mariola: *Tratado de Lisboa - Textos consolidados del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea*, Madrid, Marcial Pons, 2010.

Martín y Pérez de Nanclares, José, "Seguridad y acción exterior de la Unión Europea: La creciente relevancia de la dimensión exterior del espacio de Libertad, Seguridad y Justicia", *Revista Electrónica del Instituto Español de Estudios Estratégicos*, número 0, 2012, pp. 135-154 [disponible en http://revista.ieee.es/index.php/ieee/article/view/13/14, último acceso el 18 de junio de 2014].

Melzer, Nils, *Cyberwarfare and International Law*, Instituto de las Naciones Unidas de Investigación para el Desarme, Ginebra, 2011.

Menon, Anand, "Defence policy and integration in Western Europe", *Contemporary Security Policy*, volumen 17, número 2, 1996, p. 264 y ss.

Menon, Arnand, "Why ESDP is Misguided and Dangerous for the Alliance?", en Howorth, Jolyon y Keeler, John (eds.), *Defending Europe*, London, Macmillan, 2003, pp. 203-219.

Ministerio de Asuntos Exteriores del Reino Unido, *British and foreign State papers, volume 30, 1841-1842*, Reino Unido de la Gran Bretaña e Irlanda del Norte, Londres, 1842.

Ministerio de Defensa del Reino de España, "Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas", *Boletín Oficial del Ministerio de Defensa*, número 40, pp. 4154-4156, Reino de España, Madrid, 2013.

Missiroli, Antonio (ed.), "From Copenhagen to Brussels. European defence: core documents", *Chaillot Paper 47*, Instituto de Estudios de Seguridad de la Unión Europea, París, 2003.

Missiroli, Antonio, "EU-NATO Cooperation in Crisis Management: No Turkish Delight for ESDP", *Security Dialogue*, volume 33, número 1, 2002, pp. 9-26.

Mongin, Dominique, "Les cyber-attaques, arme de guerre en temps de paix", *Revue Esprit*, número de enero, 2013, pp. 32 y ss.

Moore, John Bassett, *A digest of international law, volume 217*, Washington D. C., Government Printing Office, 1906.

Mora Benavente, Enrique, "Introducción", en Instituto Español de Estudios Estratégicos, "La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa", *Cuadernos de Estrategia*, volumen 145, número de marzo, 2010, pp. 11-27.

Möttölä, Kari, "Collective and co-operative security arrangements in Europe", en Koskenniemi, Martti (ed.), *International Law Aspects of the European Union*, La Haya, Kluwer Law International, 1998, pp. 87-98.

Murphy, Sean, "The Doctrine of Preemptive Self-Defense", *Villanova Law Review*, volumen 50, 2005, pp. 699 y ss.

Nakashima, Ellen, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace", *The Washington Post*, 30 de mayo, 2012 [disponible en http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html, ultimo acceso el 1 de julio de 2014].

Nerlich, Uwe, "The relationship between a European common defence and NATO, the OSCE and the United Nations", Martin, Lawrence y Roper, John (eds.), *Towards a common defence policy*, París, Instituto de Estudios Estratégicos de la Unión Europea Occidental, 1995, pp. 69-97.

Newman, Edward, *A crisis of global institutions: multilateralism and international security*, Routledge, Nueva York, 2007.

Noah, Timothy, "Birth of a Washington Word", *www.slate.com*, 2002 [disponible en http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html, ultimo acceso el 16 de julio de 2014].

Organización de las Naciones Unidas, *Carta de las Naciones Unidas de 24 de octubre de 1945* [1 UNTS XVI], San Francisco, 1945 [disponible en http://www.un.org/es/documents/charter, último acceso el 1 de julio de 2014].

Organización de las Naciones Unidas, *Convención de 23 de mayo de 1969 sobre el Derecho de los Tratados* [1155 UNTS. 331], Viena, 1969.

Organización del Tratado del Atlántico Norte, "NATO and cyber defence", *www.nato.int*, 2013 [disponible en http://www.nato.int/cps/en/natolive/topics_78170.htm, último acceso el 25 de junio de 2013].

Organización del Tratado del Atlántico Norte, "NATO and Estonia conclude agreement on cyber Defence", *www. nato.int*, 2010 [disponible en http://www.nato.int/cps/en/natolive/news_62894.htm, último acceso el 17 de julio de 2014].

Ortega Carcelén, Martín, *La legítima defensa del territorio del Estado. Requisitos para su ejercicio*, Madrid, Tecnos, 1991.

Ortega, Andrés, "Año de siembra en un cruce de siglos", *Anuario Internacional del Centro de Información y Documentación Internacionales en Barcelona*, 1997, pp. 15-26.

Oswald, Franz, *Europe and the United States. The Emerging Security Partnership*, Londres, Praeger Security International, 2006.

Pape, Robert, "Soft balancing against the United States", *International Security*, volume 30, número 1, 2005, pp. 7-45.

Parlamento Europeo, *Resolution of the European Parliament of 14 May 1998 on the gradual establishment of a common defence policy for the European Union* [A4–0171/98], Comunidades Europeas, Estrasburgo, 1998.

Patomäki, Heikki, “Cultivating the Mood of <<Grieving Delight>> The Moral Lessons of the Study of Narratives and Methaphors in the 1990-1991 Gulf War”, *Paper by the second EuPRA Conference of 12-14 November 1993*, Budapest, 1993.

Presidente de los Estados Unidos, *Presidential Policy Directive 20 on US Cyber Operations Policy*, Estados Unidos de América, Washington D. C., 2012 [disponible en http://fas.org/irp/offdocs/ppd/ppd-20.pdf, último acceso el 16 de julio de 2014].

Presidente de los Estados Unidos, *US Presidential Decision Directive 63 of 22 May 1998 on Critical Infrastructure Protection*, Estados Unidos de América, Washington D. C., 1998.

Quermonne, Jean-Louis, "Existe-t-il un modèle politique européen?", *Revue Française de Science Politique*, volumen 40, número 2, 1990, p. 192-211.

Randelzhofer, Albrecht, “Article 2(4)”, en Simma, Bruno, *The Charter of the United Nations: A commentary*, Oxford, Oxford University Press, 2002, pp. 117 y ss.

Reichard, Martin, *The EU-NATO Relationship: A Legal and Political Perspective*, Hampshire, Ashgate Publishing Limited, 2006.

Remiro Brotóns, Antonio (coord.), *Derecho Internacional*, Madrid, Tirant lo Blanch, 2010.

Roscini, Marco, *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014.

Rubio García, Dolores, “Las cláusulas de asistencia mutua y solidaridad introducidas por el Tratado de Lisboa: el refuerzo de la seguridad y la defensa en la Unión Europea”, *Documento de trabajo 57/2011*, Observatorio de Política Exterior Española, Madrid, 2011.

Rutten, Maartje (coord.), “From St. Malo to Nice. European Defence: Core Documents”, *Chaillot Paper 47*, Instituto de Estudios de Seguridad, Unión Europea Occidental, París, 2001.

Salmon, Trevor y Shepherd, Alistair, *Towards a European Army - A Military Power in the Making?*, Boulder, Colorado, Lynne Rienner Publishers, 2003.

Sánchez Pereyra, Antonio, *Geopolítica de la expansión de la OTAN*, México D.F., Plaza y Valdés, 2003.

Sanger, David y Shanker, Thom, “Broad Powers Seen for Obama in Cyberstrikes”, *The New York Times*, 3 de febrero, 2013 [disponible en http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0, ultimo acceso el 1 de julio de 2014].

Schaap, Arie, “Cyber Warfare operations: developments and use under international law”, *Air Force Law Review*, volumen 64, 2009, p. 121 y ss.

Schifferes, Steve, “US names <<coalition of the willing>>”, *BBC News Online*, 18 de marzo, 2003 [disponible en http://news.bbc.co.uk/2/hi/americas/2862343.stm, último acceso el 30 de junio de 2014].

Schmitt, Michael (coord.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013.

Schmitt, Michael, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, *Columbia Journal of Transnational Law*, volumen 37, 1999, pp. 885-937.

Schmitt, Michael, “Cyber operations and the jus ad bellum revisted”, *Villanova Law Review*, volumen 56, 2011, pp. 569-606.

Schmitt, Michael, “Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts”, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy*, Consejo Nacional de Investigación de Estados Unidos, 2010, pp. 151-178 [disponible en http://sites.nationalacademies.org/CSTB/cs/groups/cstbsite/documents/webpage/cstb_059439.pdf, último acceso el 16 de julio de 2013].

Secretario General de las Naciones Unidas, *Informe sobre un concepto más amplio de libertad*, Organización de las Naciones Unidas, Nueva York, 2005 [disponible en http://www.un.org/spanish/largerfreedom/chap3.htm, último acceso el 15 de julio de 2014].

Seibert, Bjoern, “When great powers compete, the pirates win”, *Foreign Policy*, 30 de marzo, 2009.

Servicio Europeo de Acción Exterior, *EU-US Summit Joint Statement of 26 March 2014* [140326/02], Unión Europea, Bruselas, 2014 [disponible en http://www.eeas.europa.eu/statements/docs/2014/140326_02_en.pdf, último acceso el 1 de julio de 2014].

Shapiro, Jeremy y Witney, Nick, *Towards a Post-American Europe: a power audit of EU-US Relations*, European Council on Foreign Relations, 2009.

Simma, Bruno, *The Charter of the United Nations: A Commentary*, Oxford, Oxford University Press, 2013.

Skubiszewski, Krzysztof, “Use of Force by States, Collective Security, Law of War and Neutrality”, en Sørensen, Maximilian (ed.), *Manual of Public International Law*, Londres, Macmillan, 1968, pp. 745 y ss.

Sofaer, Abraham, “On the Necessity of Preemption”, *European Journal of International Law*, volumen 14, 2003, pp. 209 y ss.

Stevens, Sharon, “Internet War Crimes Tribunals and Security in an Interconnected World”, *Transnational Law and Contemporary Problems*, volumen 18, 2009, pp. 676 y ss.

Stevenson, Richard, “Remember <<Weapons of Mass Destruction>>? For Bush, They Are a Nonissue”, *The New York Times*, 18 de diciembre, 2003.

Sturm, Paul, “NATO and the EU: Cooperation?”, *European Security Review*, número 48, 2010 [disponible en http://www.isis-europe.eu/sites/default/files/programmes-downloads/2010_artrel_445_eu-nato-capabilities.pdf, último acceso el 5 de julio de 2014].

The Economist, “Berlin Minus. There is no excuse for the failure of NATO and the EU to talk to each other”, *www.economist.com*, 2007 [disponible en http://www.economist.com/node/8669193, ultimo acceso el 17 de julio de 2014].

Traynor, Ian, “Russia accused of unleashing cyberwar to disable Estonia”, The Guardian, jueves 17 de mayo, 2007.

Tsang, Rose, “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks 21, University of California”, *Working Paper*, Goldmand School of Public Policy, Berkeley, 2009.

Tuomioja, Erkki y Freivalds, Laila, “We want a stronger EU security policy”, *Dagens Nyheter*, 11 de noviembre, 2003.

Unión Europea, “Síntesis de la Legislación de la UE. Política Exterior y de Seguridad”, *europa.eu*, 2007 [disponible en http://europa.eu/legislation_summaries/foreign_and_security_policy/cfsp_and_esdp_implementation/l33243_es.htm último acceso el 11 de julio de 2007].

Unión Europea, *Versión consolidada del Tratado de Funcionamiento de la Unión Europea* [2010/C 83/01], Lisboa, 2007, Artículo 222.3 del TFUE.

Unión Europea, *Versión consolidada del Tratado de la Unión Europea de 7 de febrero de 1992* [2010/C 83/01], Maastricht, 1992 [disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:FULL:ES:PDF , último acceso el 1 de julio de 2014].

Van der Vleuten, Anna, "Two-level interaction as source of influence. The European Union and equal treatment policies", en Reinalda, Bob y Verbeek, Bertjian (eds.), *Autonomous Policy Making by International Organizations*, London, Routledge, 1998, p. 62-79.

Védrine, Hubert, *History Strikes Back. How States, Nations and Conflicts Are Shaping the Twenty-First Century*, Washington D. C., Brookings Institution Press, 2008.

Ventre, Daniel, *Ciberattaque et cyberdéfense*, París, Lavoisier, 2011.

Yaniz Velasco, Federico, "La Alianza Atlántica y la Unión Europea. La evolución de unas relaciones complejas", *Documento marco 09/2013*, Instituto Español de Estudios Estratégicos, Madrid, 2013.

Zemanek, Karl, "Armed attack", en Rüdiger Wolfrum (ed.), *Encyclopedia of Public International Law*, Max Planck, 2010, entrada 21.