# Las medidas de autotutela frente a amenazas cibernéticas en derecho internacional: Especial referencia a la posible adopción de contramedidas colectivas

# Self-help measures against cyber threats in international law: Special reference to the possible adoption of collective countermeasures

Juan Jorge Piernas López[*]
*Profesor Titular de Derecho internacional público y Relaciones internacionales en la Universidad de Murcia*
*Titular de una Cátedra Jean Monnet de la Comisión Europea (TEULP)*

Recibido: 14.12.2023 / Aceptado: 15.01.2024
DOI: 10.20318/cdt.2024.8412

**Resumen:** Este artículo analiza las medidas que pueden adoptar legítimamente los sujetos de Derecho internacional para responder ante actividades cibernéticas maliciosas. En particular, el artículo analiza las principales medidas de autotutela previstas por el Derecho internacional, a saber, la retorsión, las contramedidas y la legítima defensa en respuesta a ciberataques. Con este fin, se estudia en primer lugar el estado de la cuestión relativo a la retorsión en este ámbito. En segundo lugar, se aborda la cuestión de las contramedidas, con especial referencia a la posibilidad de adoptar contramedidas colectivas a la luz de posicionamientos recientes de Estados y de algunas instituciones y órganos de la Unión Europea. En tercer lugar, se estudia la posibilidad de actuar en legítima defensa en respuesta a un ciberataque. Finalmente se incluyen una serie de consideraciones a modo de conclusión.
**Palabras clave:** Autotutela, ciberespacio, Derecho internacional, retorsión, contramedidas, legítima defensa.

**Abstract:** This article analyses the measures that subjects of international law can legitimately take to respond to malicious cyber activities. In particular, the article examines the main measures of self-help provided for by International law, namely retorsion, countermeasures and self-defence in response to cyber-attacks. To this end, the article first studies the question of retorsion in this area. Secondly, the issue of countermeasures is analysed, with particular reference to the possibility of adopting collective countermeasures in the light of recent positions adopted by States and certain institutions and bodies of the European Union. Thirdly, the possibility of acting in self-defence in response to a cyber-attack is examined. Finally, a number of concluding remarks are included.
**Keywords:** Self-help, cyberspace, International law, retaliation, countermeasures, self-defence.

[*] Profesor Titular de Derecho Internacional Público y Relaciones Internacionales y titular de la Cátedra Jean Monnet (TEULP), Universidad de Murcia (España). Este trabajo ha sido realizado en el marco del proyecto de investigación titulado *La búsqueda de una regulación internacional para las actividades cibernéticas: ¿una ineludible necesidad? (CYBINREG),* ayudas a proyectos de I+D+i en el marco de los Programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de I+D+i orientada a los retos de la Sociedad (convocatoria 2020), Ref PID 2020 112577 RB-I00. El autor es IP2 del proyecto. Este artículo es fruto de la investigación realizada por el solicitante en la Universidad de Harvard en el marco de la estancia (21725/EE/22), financiada por la Fundación Séneca-Agencia de Ciencia y Tecnología de la Región de Murcia dentro del Programa Regional de Movilidad, Colaboración e Intercambio de Conocimientos "Jiménez de la Espada".

**Sumario:** I. Introducción. II. Las medidas de retorsión frente a ciberataques. III. Las contramedidas. Especial referencia a las contramedidas colectivas. IV. La legítima defensa en respuesta a ciberamenazas. V. Conclusiones.

## I. Introducción

**1.** El 7 de diciembre de 2023, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, realizó una declaración en nombre de la Unión Europea sobre la protección de los procesos democráticos contra las actividades cibernéticas malintencionadas. La declaración condenaba firmemente las actividades cibernéticas malintencionadas dirigidas contra las instituciones democráticas y los procesos electorales, y mostraba su solidaridad con el Reino Unido, que ese mismo día había acusado al Servicio de Seguridad ruso, el FSB, de una campaña sostenida de ciberhackeo dirigida a políticos y otros cargos públicos. La Unión Europea y sus Estados miembros, concluía la declaración, se muestran dispuestos a emprender cualquier acción necesaria de ciberdiplomacia, incluidas sanciones, para prevenir y responder a ciberataques inaceptables.[1]

**2.** La declaración es reveladora del contexto actual, en el que los ciberataques representan una creciente amenaza para la seguridad global, así como para los procesos electorales democráticos en todo el mundo. En la reunión de Davos celebrada a inicio de 2023 se presentó un informe del World Economic Forum que afirma que más del 93% de los expertos en ciberseguridad y el 86% de los líderes empresariales creen que "es probable que se produzca un acontecimiento cibernético catastrófico de gran alcance en los próximos dos años".[2] La situación previsiblemente se agravará con la creciente conexión de dispositivos a Internet a través del denominado Internet of Things (IoT), que prevé la conexión de más de 41 mil millones de dispositivos IoT para 2025.[3] Además, la situación de la Unión Europea es particularmente complicada, habida cuenta de que es un importador neto de productos y servicios de ciberseguridad, y depende en gran medida de proveedores no europeos,[4] lo que aumenta el riesgo de dependencia tecnológica y vulnerabilidad.

**3.** Los ciberataques han aumentado significativamente durante la reciente pandemia, habiendo sido dirigidos recientemente contra infraestructuras críticas, centros sanitarios, o instalaciones energéticas, como los ciberataques a gran escala que afectaron en Bélgica a la empresa de telecomunicaciones Belnet y al Departamento de Asuntos Internos responsable de la política de inmigración y el orden público en 2021, o el ciberataque contra Ucrania que precedió a la agresión rusa de febrero de 2022.[5] Cabe recordar también en este contexto las palabras del expresidente Juncker de la Comisión Europea en su discurso sobre el estado de la Unión de 2017: "Los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques"[6].

---

[1] La declaración institucional puede consultarse (en inglés) en el siguiente enlace: https://www.consilium.europa.eu/es/press/press-releases/2023/12/07/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-the-protection-of-democratic-processes-against-malicious-cyber-activities/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cyber:+Statement+by+the+High+Representative+on+behalf+of+the+European+Union+on+the+protection+of+democratic+processes+against+malicious+cyber+activities

[2] Véase la noticia relativa a la publicación del informe, disponible en https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/ (traducción del autor).

[3] Véase a este respecto la información publicada por la Comisión Europea, disponible en el siguiente enlace: https://digital-strategy.ec.europa.eu/es/policies/internet-things-policy

[4] Véase sobre este punto la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación, Bruselas, 12.9.2018 COM(2018) 630 final 2018/0328 (COD), p. 1.

[5] Véase sobre estos ciberataques, entre otros, Y. Miadzvetskaya, and R.A. Wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, Vol. 7, 2021, No 1, pp. 413-438, p. 413.

[6] Discurso sobre el Estado de la Unión de 2017, disponible en el siguiente enlace: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_17_3165

**4.** Los ciberataques también se dirigen contra las instituciones europeas, y en respuesta a este fenómeno creciente, la Comisión presentó en marzo de 2022 una propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, basada en el artículo 298 TFUE, relativo a la administración europea "abierta, eficaz e independiente". El Reglamento prevé, entre otras medidas, la creación de Consejo Interinstitucional de Ciberseguridad. En relación con esta propuesta, el pasado 21 de noviembre de 2023, el Parlamento aprobó en primera lectura la misma, tras haber alcanzado un acuerdo con el Consejo en junio del mismo año.[7] Por otro lado, la implicación de agentes estatales, como Rusia, China y Corea del Norte, en actividades cibernéticas maliciosas, como ha señalado respecto de Rusia el Reino Unido en su declaración de 7 de diciembre de 2023, aumenta significativamente la gravedad de la situación.[8]

**5.** En este marco, el artículo analiza qué medidas pueden adoptar legítimamente los sujetos de Derecho internacional para responder, como señalaba la declaración del Alto Representante, a los ciberataques de los que cada vez con más frecuencia son víctimas. En particular, el artículo analiza las principales medidas de autotutela previstas por el Derecho internacional, a saber, la retorsión, las contramedidas y la legítima defensa en respuesta a ciberataques. Con este fin, se estudia en primer lugar el estado de la cuestión relativo a la retorsión en este ámbito. En segundo lugar, se aborda la cuestión de las contramedidas, con especial referencia a la posibilidad de adoptar contramedidas colectivas a la luz de posicionamientos recientes de Estados y de algunas instituciones y órganos de la Unión Europea. En tercer lugar, se estudia la posibilidad de actuar en legítima defensa en respuesta a un ciberataque. Finalmente se incluyen una serie de consideraciones a modo de conclusión.

## II. Las medidas de retorsión frente a ciberataques

**6.** La figura de la retorsión en Derecho internacional consiste en la adopción por un Estado u organización internacional de un acto inamistoso y perjudicial pero no ilícito contra otro Estado, como respuesta contra las actividades lesivas de ese Estado. Las medidas de retorsión no suponen por tanto la violación de ninguna obligación de Derecho internacional.

**7.** Como ha señalado la Comisión de Derecho Internacional, "Los actos de retorsión pueden incluir la prohibición o limitación de las relaciones diplomáticas normales u otros contactos, embargos de diversos tipos o retirada de los programas voluntarios de ayuda. Cualquiera que sea su motivación, en cuanto que esos actos no son incompatibles con las obligaciones internacionales de los Estados que toman esas medidas contra el Estado al que se dirigen, no son contramedidas y quedan fuera del ámbito de aplicación de los presentes artículos"[9].

**8.** En palabras de Shaw, la represión es un método legítimo de mostrar el descontento de un modo que perjudique al otro Estado (u organización internacional) pero dentro de los límites de la legalidad.[10] Este autor pone como ejemplo la ya derogada legislación estadounidense que exigía al Presidente de los Estados Unidos suspender la ayuda exterior a cualquier país que nacionalizara bienes estadounidenses sin compensación adecuada, aplicada en 1963 contra Ceilán (actual Sri Lanka).[11]

---

[7] Véase la noticia sobre el acuerdo alcanzado por los colegisladores de la Unión en el siguiente enlace: https://www.consilium.europa.eu/es/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/

[8] La declaración del Reino Unido puede consultarse en el siguiente enlace: https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes

[9] Documento A/56/10.–Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones cit., p. 137.

[10] M.S. Shaw, *International Law*, Oxford University Press (sixth edition), p. 1128.

[11] Id., p. 1129.

**9.** Las medidas de retorsión pueden tener también carácter cibernético. Como señala el comentario número 4 de la regla 20 del Manual de Tallin 2.0, un Estado puede emplear una lista de control de acceso para impedir las comunicaciones de otro Estado porque el primero goza de soberanía sobre la infraestructura cibernética en su territorio. La acción sería lícita incluso si fuera perjudicial para los intereses de este último, siempre que no viole ninguna obligación de tratado o norma de derecho consuetudinario aplicable.[12]

**10.** En los últimos años, numerosos Estados han avalado oficialmente la posibilidad de adoptar medidas de retorsión en respuesta a ciberataques con arreglo a Derecho internacional. Del análisis de estos documentos se desprenden algunas características relevantes de las medidas de retorsión en el ámbito cibernético, entre otras:

— Algunos Estados consideran que las medidas de retorsión se pueden adoptar en respuesta a operaciones cibernéticas ilícitas, o simplemente hostiles. Es decir, no se requiere que el acto previo por el que se responde vulnere una obligación de Derecho internacional.[13]
— Otros Estados, por ejemplo Alemania, parecen subordinar la adopción de medidas de retorsión frente a operaciones cibernéticas ilícita a la indisponibilidad por razones jurídicas o políticas. Además, Alemania considera que las medidas de retorsión pueden adoptarse como reacción a una operación cibernética ilícita en combinación con otros tipos de respuesta, como las contramedidas.[14]
— Entre los ejemplos de medidas de retorsión aportados por los Estados, junto a los ya mencionados de interrumpir relaciones diplomáticas, cabe destacar los siguientes: (a) un Estado puede limitar o cortar el acceso de un Estado a los servidores u otras infraestructuras digitales de su territorio, siempre que los países en cuestión no hayan celebrado un tratado de acceso mutuo a las infraestructuras digitales de sus respectivos territorios;[15] (b) declarar públicamente que otro Estado es responsable de una operación cibernética,[16] (c) abstenerse de firmar un acuerdo comercial que beneficiaría a ambas partes,[17] (d) exclusión de agrupaciones internacionales (cabe suponer en este sentido de grupos como el G8 o el G20 por ejemplo).[18]

---

[12] M.N. Schmitt, (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 112: "The fact that countermeasures involve acts that would otherwise be unlawful also distinguishes them from retorsion. Retorsion refers to the taking of measures that are lawful, albeit 'unfriendly'. A State may, for instance, employ an access control list to prevent communications from another State because the former enjoys sovereignty over the cyber infrastructure on its territory (Rule 2). The action would be lawful even if detrimental to the interests of the latter so long as it violates no treaty obligation or applicable customary law norm". Véase también en este sentido K. Härmä, y T. Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2017. Puede consultarse en el siguiente enlace: https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

[13] Véase a este respecto la postura, entre otros de Costa Rica, Ministerio de Relaciones Exteriores de Costa Rica, " Costa Rica's position on the application of International law in cyberspace" (21 de julio de 2023), p. 5, apartado 16 (traducción del autor). Véase también, inter alia, la posición nacional publicada por el Ministerio de Asuntos Exteriores de Polonia, 'The Republic of Poland's position on the application of international law in cyberspace, Ministry of Foreign Affairs of Poland, 29 Diciembre 2022, p. 8, apartado 9: "Retorsion is a response of the state to actions contrary to its interest or hostile actions of another state. Measures taken as a retorsion may be in reaction to both legal and illegal actions of another subject of international law, but in itself they must be in compliance with international law"

[14] Gobierno Federal de Alemania, 'On the Application of International Law in Cyberspace', Position Paper (March 2021), p. 13, apartado (1).

[15] Gobierno del Reino de los Países Bajos, Appendix: International law in cyberspace, 26 Septiembre 2019, p. 7.

[16] Posición nacional del Gobierno de Noruega, en 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, Agosto 2021, p. 72, apartado 5.1: "Publicly declaring that another State is responsible for a cyber operation is in itself an act of retorsion".

[17] Departamento Federal de Asuntos Exteriores de Suiza, 'Switzerland's position paper on the application of international law in cyberspace' (May 2021), p. 6, apartado 6.2.

[18] Discurso de la Fiscal General del Reino Unido Suella Braverman: 'International Law in Future Frontiers', 19 Mayo 2022, disponible en el siguiente enlace: https://www.gov.uk/government/speeches/international-law-in-future-frontiers

— Las medidas de retorsión pueden ser adoptadas también de manera colectiva, a través de una organización internacional. Destaca a este respecto la claridad con la que la posición nacional de Estonia se refiere al régimen de sanciones cibernéticas y a las medidas de ciberdiplomacia de la Unión Europea.[19] Esta postura corrobora la posición defendida por este autor en relación a la calificación como medidas de retorsión de las sanciones de la Unión Europea en respuesta a ciberataques, aunque desnaturalizando en parte la figura de la retorsión, habida cuenta de que no se dirigen contra sujetos de Derecho internacional, sino contra personas físicas.[20]
— La adopción de sanciones ha sido también mencionada por otros Estados en sus posiciones nacionales.[21] Conviene mencionar no obstante que las sanciones económicas, particularmente las que imponen congelaciones de activos a determinadas personas jurídicas residentes en Estados terceros, podrían vulnerar *prima facie* las obligaciones que numerosos Estados deben respetar con arreglo a los compromisos alcanzados en el marco de la Organización Mundial del Comercio (OMC). Sin embargo, las propias normas de la OMC prevén también excepciones por razones de seguridad nacional, en particular el artículo XXIII GATT.[22]

**11.** Por último, como expondremos en más detalle a continuación, las medidas de retorsión presentan ciertas ventajas respecto del resto de medidas de autotutela. En particular, al tratarse de medidas lícitas, no están sujetas a los requisitos procesales y sustantivos de las contramedidas, especialmente en lo tocante a la observancia del principio de proporcionalidad y a la ausencia de obligación de notificar al Estado que ha llevado a cabo el acto hostil o ilícito con carácter previo a su adopción.

## III. Las contramedidas. Especial referencia a las contramedidas colectivas

**12.** De conformidad con el artículo 22 del Proyecto de Artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, adoptado por la Comisión de Derecho Internacional (CDI) de 12 de diciembre de 2001(en adelante también "el proyecto de artículos de la CDI"):[23] "La ilicitud del hecho de un Estado que no esté en conformidad con una obligación internacional suya para con otro Estado queda excluida en el caso y en la medida en que ese hecho constituya una contramedida tomada contra ese otro Estado de acuerdo con lo dispuesto en el capítulo II de la tercera parte." Con arreglo a la definición ofrecida por Alland, las contramedidas constituyen 'pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when

[19] Posición nacional del Gobierno de Estonia, en 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136', Agost0 2021, p. 29: "One example of such a mechanism would be the European Union's cyber sanctions regime and cyber diplomacy toolbox, which offer an array of measures that could be taken as a response to malicious cyber operations."

[20] J.J. Piernas López, *Ciberdiplomacia y ciberdefensa en la Unión Europea*, Aranzadi, Cizur Menor, 2020, pp. 133-135. Véase también sobre la calificación de las sanciones de la UE en respuesta a ciberataques como medidas de retorsion P. Pawlak, P. y T. biersteker (eds.), Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace, Chaillot Paper 155, cit., p. 43: "Due to their targeted nature, the measures applied as part of the EU sanctions regime are qualified as measures of retorsion (unfriendly but legal acts)". Véase también en un sentido similar K. Härmä y T. Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2017. Puede consultarse en el siguiente enlace: https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

[21] Véanse en particular las posiciones nacionales de Noruega, Reino Unido y Estados Unidos de América en 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, cit.', Agosto 2021, p. 72 (Noruega), 'Discurso de la Fiscal General Suella Braverman: International Law in Future Frontiers, cit.'(Reino Unido), y 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136', Agosto 2021, p. 142 (Estados Unidos).

[22] Véase a este respecto P. Pawlak, y T. Biersteker (eds.), *Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace*, Chaillot Paper 155, cit., p. 48.

[23] Proyecto de Artículos sobre responsabilidad del estado por hechos internacionalmente ilícitos, adoptado por la CDI en su 53º período de sesiones (A/56/10) y anexado por la Asamblea General en su Resolución 56/83, de 12 de diciembre de 2001.

the former consider that the latter has committed an internationally wrongful act which could justify such a reaction."[24]

**13.** Las contramedidas pueden, por tanto, ser adoptadas por los Estados y suponen una causa de exclusión de la ilicitud de su conducta, como confirma el artículo 49.1 del mismo proyecto de artículos de la CDI, siempre que el Estado que las lleva a cabo cumpla con sus requisitos sustantivos y procesales, que se desarrollan a continuación. Además, como ha señalado la doctrina, las contramedidas desencadenan la responsabilidad internacional del Estado contra el que se adoptan.[25]

**14.** Como indica el Manual de Tallin 2.0, un Estado puede tener derecho a adoptar contramedidas, ya sean de naturaleza cibernética o no, en respuesta al incumplimiento de una obligación de derecho internacional que incumbe a otro Estado.[26] El G7 también subrayó la posibilidad de que los Estados adopten contramedidas cibernéticas.[27] No obstante, como subraya Delereu, la práctica estatal indica que los Estados no parecen considerar los ciberataques como hechos internacionalmente ilícitos. Como resultado, hasta 2020 ningún Estado había tomado formalmente contramedidas contra otro Estado en respuesta a un ciberataque, lo que corrobora Segura Serrano en 2023.[28]

**15.** La regulación de las contramedidas por el Proyecto de artículos de la CDI representa un equilibrio entre posturas opuestas, y con válidos argumentos en ambas partes. Por un lado, tras la adopción de la Carta de Naciones Unidas y la creación de un sistema internacional que prohíbe el uso de la fuerza por los Estados, con la excepción de la legítima defensa, cabría argumentar que el sistema clásico de autotutela del Derecho internacional, y por tanto la adopción de contramedidas, ya no resulta apropiado. Por otro lado, la realidad es que el sistema creado por las Naciones Unidas es descentralizado y no establece un sistema de resolución inmediata y vinculante de todas las posibles diferencias entre sujetos de Derecho internacional. Se suele mencionar a este respecto que el tribunal arbitral creado en el caso del *Acuerdo sobre los servicios aéreos* entre Francia y Estados Unidos reafirmó la disponibilidad de las contramedidas en 1978, si bien recordando que están limitadas por las normas de la Carta sobre el uso de la fuerza, así como por el principio de proporcionalidad. Cabe destacar que el tribunal arbitral subrayó lo que puede parecer una obviedad, pero tiene efectos prácticos muy relevantes, a saber, que la determinación sobre si ha existido o no un ilícito previo corresponde al Estado que adopta las contramedidas ("in one State's view):

If a situation arises which, in one State's view, results in the violation of an international obligation by another State, the first State is entitled, within the limits set by the general rules of international law pertaining to the use of armed force, to affirm its rights through "counter-measures".[29]

---

[24] D. Alland, 'The Definition of Countermeasures' en J. Crawford et al. (eds), *The Law of International Responsibility*, Oxford University Press, 2010, 1127, 1135.

[25] H. LESAFFRE, 'Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Countermeasures' en J. Crawford et al. (eds), *The Law of International Responsibility*, Oxford University Press, 2010, 469, 469 y ss; A. Segura Serrano, *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023, p. 131.

[26] M. N. Schmitt (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 20, principio general, p. 112."

[27] Declaración del G7 sobre el comportamiento responsable de los Estados en el ciberespacio Lucca, 11 de abril de 2017, p. 2:" Observamos que, en aras de la prevención de conflictos y la solución pacífica de controversias, el derecho internacional también proporciona un marco para las respuestas de los Estados a los actos ilícitos que no equivalen a un ataque armado - estos pueden incluir actividades cibernéticas maliciosas. Entre otras respuestas lícitas, un Estado víctima de un hecho internacionalmente ilícito puede, en determinadas circunstancias, recurrir a contramedidas proporcionadas, incluidas medidas llevadas a cabo a través de las TIC, contra el Estado responsable del hecho ilícito con el fin de hacer que el Estado responsable cumpla con sus obligaciones internacionales".

[28] F. Delerue, *Cyber operations and international law*, Cambridge University Press, 2020, p. 431: "Curiosamente, dado que [los Estados] no califican las operaciones cibernéticas en cuestión de actos internacionalmente ilícitos, también parecen adoptar únicamente respuestas que adoptan la forma de medidas legales, al menos públicamente. Estas respuestas adoptan, en particular, la forma de nuevas sanciones contra individuos o entidades relacionados con la perpetración de las operaciones cibernéticas, o la deportación de diplomáticos. Hasta la fecha, ningún Estado ha enmarcado públicamente su respuesta en el mecanismo jurídico internacional de las contramedidas ni ha invocado el derecho de legítima defensa en respuesta a las operaciones cibernéticas" (traducción del autor). A. Segura Serrano, *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023, p. 113.

[29] Laudo de 9 de diciembre de 1978, párr. 91

**16.** En relación con lo anterior, un autor crítico con las medidas de autotutela llegó a afirmar que la autoayuda se distingue en principio de la anarquía sólo en que quienes la emprenden pueden alegar que actúan para hacer valer un derecho.[30] En este marco, las contramedidas fueron finalmente aceptadas por el proyecto de la CDI en 2001, pero con estrictos limites dirigidos a evitar abusos por parte de los Estados más poderosos, incluyendo ciertas obligaciones internacionales que no se pueden ver afectadas por las contramedidas.

**17.** Los requisitos sustantivos de las contramedidas, que deben ser observados también en el ciberespacio, son los siguientes:

(i) las contramedidas sólo se deben adoptar en respuesta a un hecho internacionalmente ilícito previo de otro Estado;
(ii) deben respetar el principio de proporcionalidad;
(iii) deben ser reversibles; y
(iv) no pueden afectar a ciertas obligaciones previstas por el artículo 50 del proyecto de artículos de la CDI.

**18.** En cuanto al primer requisito, de conformidad con el artículo 2 del proyecto de artículos de la CDI, hay hecho internacionalmente ilícito del Estado cuando un comportamiento consistente en una acción u omisión atribuible al Estado según el derecho internacional y que constituye una violación de una obligación internacional del Estado. A este respecto, como ha señalado CERVELL HORTAL, las actividades cibernéticas maliciosas atribuibles a Estados pueden suponer la violación del principio de soberanía o el de no intervención y constituir un hecho ilícito internacional.[31]Asimismo, la actividad cibernética maliciosa podría también suponer la violación de otras obligaciones internacionales, bien por acción, como la prohibición del uso de la fuerza, bien por omisión, como la del deber de debida diligencia.

**19.** En cuanto al principio de proporcionalidad, como se ha observado, la CDI exigió *expressis verbis* (art. 51 del Proyecto de 2001 y art. 54 del Proyecto de Organizaciones de 2011) tres criterios para medir la proporcionalidad: el perjuicio sufrido, la gravedad del hecho ilícito y el impacto de la contramedida sobre 'los derechos en cuestión', explicando (respecto a esta última expresión) que refleja los términos utilizados por el Tribunal en el asunto Gabcíkovo (1997) y que se refiere tanto a los derechos del Estado (u organización internacional) lesionado como a los del Estado (u organización internacional) lesionado. Gabcíkovo (1997) y que se refiere tanto a los derechos del Estado (u organización internacional) lesionado como a los del Estado (u organización) que cometió el hecho ilícito, y puede abarcar también los derechos de otros Estados (u organizaciones) que puedan verse afectados"[32].

**20.** En relación con la reversibilidad, de conformidad con el artículo 53 del Proyecto de artículos de la CDI, se pondrá fin a las contramedidas tan pronto como el Estado responsable haya cumplido sus obligaciones en relación con el hecho internacionalmente ilícito de conformidad con lo dispuesto en la segunda parte.

[30] P. Allott, 'State Responsibility and the Unmaking of International Law' (1988) 29 Harvard Intl LJ 1, 21: "self-help is distinguishable in principle from anarchy only in that those taking such action may claim that they are acting to assert a legal right; in other words, they acknowledge the existence of law. Self-help is indistinguishable from anarchy in practice if it is regarded by the subjects of the law as the normal sanction of the law." Véase sobre estas objeciones a la figura H. Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge University Press, 2020, p. 114.

[31] M.J. Cervell Hortal, 'Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)', *Revista electrónica de estudios internacionales* (REEI), Nº. 45, 2023, pp. 1-33, p. 27.

[32] C. Gutiérrez espada/ M. J. Cervell Hortal, *El Derecho Internacional (Corazón y Funciones),* Civitas-Thomson Reuters, Editorial Aranzadi, Cizur Menor (Navarra), 2022*,* p. 354, párrafo 27, A), b) del capítulo 7.

**21.** Finalmente, como establece el artículo 50, y se deriva también de la jurisprudencia internacional,[33] ciertas obligaciones internacionales no pueden ser afectadas por las contramedidas, en particular la obligación de abstenerse de recurrir a la amenaza o al uso de la fuerza, la protección de los derechos humanos fundamentales, las obligaciones de carácter humanitario que prohíben las represalias, y otras obligaciones que emanan de normas imperativas del derecho internacional general, lo que se aplicaría de la misma forma a las contramedidas cibernéticas. A este respecto, desde la esfera de la Unión Europea sea ha matizado que la "protección de los derechos humanos fundamentales" del artículo 50.1.b, por obra del calificativo "fundamentales" indica que sólo los derechos humanos que no admiten excepciones están protegidos de las contramedidas. En este sentido, y tomando como referencia el apartado 2 del artículo 15 del Convenio Europeo de Derechos Humanos, se trataría del derecho a la vida, la prohibición de la tortura y la esclavitud y la prohibición de la retroactividad penal.[34]

**22.** Respecto de los requisitos procesales de las contramedidas, de conformidad con el proyecto de artículos sobre la responsabilidad internacional de los Estados (2001) y la de las organizaciones internacionales (2011) de la Comisión de Derecho Internacional, así como con la jurisprudencia internacional, las contramedidas deben ir precedidas, *inter alia,* de un requerimiento al Estado responsable para que modifique su comportamiento[35].

**23.** En particular, el artículo 52 del proyecto de artículos de la CDI, establece lo siguiente en relación con la adopción de contramedidas bilaterales de un Estado respecto de otro:

> "1. Antes de tomar contramedidas, el Estado lesionado:
> a) Requerirá al Estado responsable, de conformidad con el artículo 43, que cumpla las obligaciones que le incumben en virtud de la segunda parte; y b) Notificará al Estado responsable cualquier decisión de tomar contramedidas y ofrecerá negociar con ese Estado.
> 2. No obstante lo dispuesto en el apartado b del párrafo 1, el Estado lesionado podrá tomar las contramedidas urgentes que sean necesarias para preservar sus derechos.
> 3. Las contramedidas no podrán tomarse y, caso de haberse tomado, deberán suspenderse sin retardo injustificado si:
> a) El hecho internacionalmente ilícito ha cesado; y
> b) La controversia está sometida a una corte o un tribunal facultados para dictar decisiones vinculantes para las partes.
> 4. No se aplicará el párrafo 3 si el Estado responsable no aplica de buena fe los procedimientos de solución de controversias."[36]

**24.** El primer requisito, relativo al requerimiento o conminación al Estado responsable para que cumpla con sus obligaciones internacionales tiene carácter de norma consuetudinaria, como señaló el Tribunal de Arbitraje establecido en 1928 para resolver la disputa entre Alemania y Portugal en el asunto *Nauliaa*,[37]y posteriormente el Tribunal Internacional de Justicia en el asunto *Gabcíkovo*.[38]Este hecho, como ha señalado recientemente el Servicio Europeo de Acción Exterior (SEAE) con referencia a la jurisprudencia del Tribunal Internacional de Justicia, es coherente con la naturaleza instrumental y

[33] Véase, por ejemplo, Comisión de Reclamaciones entre Etiopía y Eritrea, Laudo parcial de 1 de julio de 2003, Prisioners of War. Eritrea's claim 17, párr. 159), o s. del TPIY de 14 de enero de 2000 de la Sala de Primeras Instancia, Prosecutor v. Zoran Kupresic, Mirjian Kupresic, Vlatko Kupresic, Drago Jasipovic, Dragan Papic, Vladimirr Cantic /"Lasva Valley"), causa N.IT-95-16-T, párr. 529).

[34] Servicio Europeo de Acción Exterior (Consejo de la Unión Europea [Secretaría General]) Third-party Countermeasures under International Law, cit., pp. 29-30.

[35] Para las condiciones exigidas por el Derecho internacional, véase la sentencia de la Corte Internacional de Justicia de 25 de septiembre de 1997 en el asunto Gabcíkovo-Nagymaros, ICJ Reports-CIJ Reports 1997, pp. 55-57.

[36] Documento A/56/10.—Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones (23 de abril a 1.º de junio y 2 de julio a 10 de agosto de 2001), p. 145.

[37] Laudo de 31 de julio de 1928, asunto "Nauliaa", RIAA/RSA, II, pp. 1026-1029.

[38] CIJ Recueil 1997, p. 56 y comentario 3 al art. 52 del Proyecto de 2001, también en el Proyecto de 2011 sobre las Organizaciones [art. 54.1 y comentario 2 al mismo.

no punitiva de las contramedidas, que deben estar dirigidas a la cesación del acto ilícito.[39] En el caso de respuestas a ciberataques, la conminación se puede encontrar en las declaraciones políticas que realizan los Estados, como la mencionada *supra* del Reino Unido el 7 de diciembre, condenando una determinada actividad cibernética maliciosa e instando al Estado responsable, en aquel caso Rusia, a ponerle fin.[40]

**25.** El segundo requisito incluido en el artículo 52.1, relativo a la notificación de cualquier decisión de tomar contramedidas, que figuraba ya en el asunto *Nauliaa* y está consolidado en Derecho internacional,[41] y a ofrecer negociar con ese Estado, el SEAE ha reconocido recientemente que, en la práctica, lo más frecuente es que no haya notificación previa, en particular cuando la contramedida adopta la forma de legislación. El documento del SEAE aporta como ejemplo las sanciones de la UE mediante Decisiones del Consejo o Reglamentos, lo que podría incluir también las decisiones adoptadas en respuesta a ciberataques, aunque ya hemos expresado previamente nuestras reservas a esa calificación jurídica, considerando más apropiada la de retorsión en ese caso.[42]

**26.** En este sentido, como ha señalado Cervel Hortal en relación con los ciberataques, "[…] también la notificación previa, que exige el artículo 52 del Proyecto de artículos de la CDI, es puesta en duda ya por algunos Estados (Finlandia, Francia, Holanda, Italia…), que son de la opinión de que en un entorno como el ciberespacio sólo las respuestas rápidas pueden evitar males mayores. Y no dejan de estar en lo cierto: si un Estado constata, digamos, que en el día de unas elecciones las máquinas de voto están siendo hackeadas… y está seguro de esa acción proviene de un Estado concreto ¿de veras ha de cumplir con el requisito de notificación previa para que su respuesta se ajuste a los parámetros de legalidad establecidos?".[43] En todo caso, el artículo 52.2 permitiría, no obstante, adoptar contramedidas sin notificación previa ni oferta de negociaciones, en caso de que estas sean urgentes y "necesarias para preservar sus derechos", lo que se cabría invocar en el caso de ciberataques graves.

**27.** Asimismo, como ha señalado Segura Serrano recientemente, "el Reino Unido ha proclamado públicamente su posición, en el sentido de que la notificación previa no es un requisito derivado del derecho internacional consuetudinario, una posición que no ha sido secundada hasta la fecha por otros Estados, aunque cierta doctrina la considera razonable."[44]

**28.** El tercer requisito, previsto en el artículo 52.3, establece el deber de respetar los procedimientos vinculantes de solución de controversias en curso. La mera existencia de negociaciones no exige el cese de las contramedidas hasta la adopción de medidas vinculantes provisionales o finales por parte de la corte o tribunal a los que se haya sometido la controversia.[45] (s. de 9 de diciembre de 1978, párr. 91). Resulta interesante a este respecto la aclaración formulada en el documento del SEAE,

---

[39] Servicio Europeo de Acción Exterior (Consejo de la Unión Europea [Secretaría General]), Third-party Countermeasures under International Law, cit., p. 27. El SEAE se refiere en particular al asunto TIJ, Acuerdo Provisional (Antigua República Yugoslava de Macedonia c. Grecia), Sentencia de 5 de diciembre de 2011, Informes de la CIJ 2011, p. 644, en § 165, en la que se concluyó que la objeción de Grecia a la adhesión a la OTAN no se podía calificar como contramedida ya que no tenía por objeto el cese de un acto ilícito.

[40] Véase a este respecto también sobre la validez de las declaraciones políticas para cumplir el requisito de requerimiento o conminación Servicio Europeo de Acción Exterior (Consejo de la Unión Europea [Secretaría General]), Third-party Countermeasures under International Law, cit., p. 27.

[41] H. Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge University Press, 2020, p. 121. Véase también Y. Iwasawa y N. Iwatsuki, 'Procedural Conditions' en J. CRAWFORD ET AL. (eds), The Law of International Responsibility, Oxford University Press, 2010 1149, p. 1151.

[42] Véase a este respecto también sobre la validez de las declaraciones políticas para cumplir el requisito de requerimiento o conminación Servicio Europeo de Acción Exterior (Consejo de la Unión Europea [Secretaría General]), Third-party Countermeasures under International Law, cit., p. 27.

[43] M.J. Cervell Hortal, 'Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)', cit., p. 29.

[44] A. Segura Serrano, *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023, p. 140.

[45] Véase a este respecto la decisión del tribunal arbitral en el caso del Acuerdo sobre los servicios aéreos de 9 de diciembre de 1978, párrafo 91.

relativa a la posible implicación del Consejo de Seguridad de Naciones Unidas, en el sentido de que la misma no impide que los Estados puedan tomar medidas. Como explica el documento, a diferencia del artículo 51 de la Carta de las Naciones Unidas, según el cual la legítima defensa debe cesar cuando el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales, no existe la correspondiente limitación de los derechos de los Estados a utilizar contramedidas pacíficas en caso de conflicto armado, conclusión que se ve corroborada por la práctica reciente en materia de contramedidas.[46]

*Las contramedidas colectivas*

**29.** En el estado actual de desarrollo del Derecho internacional, en principio sólo el Estado perjudicado por una actividad informática malintencionada tiene derecho a recurrir a contramedidas, tal y como declaró la Comisión de Derecho Internacional (CDI) en 2001[47]. La CDI consideró la posibilidad de adoptar contramedidas colectivas como "embrionaria" y no la reguló en su informe final, aunque un proyecto anterior había previsto esa posibilidad.[48]

**30.** En el contexto de la Unión Europea, la falta de contramedidas colectivas se ha considerado una limitación significativa para la acción de la Unión.[49] Las directrices de aplicación del Marco de para una respuesta diplomática conjunta de la UE a las actividades cibernéticas maliciosas ("Cyber Diplomacy Toolbox") se referían a la posibilidad de que un Estado miembro adoptara *contramedidas no forzosas* contra un Estado que hubiera cometido un hecho internacionalmente ilícito mediante un ciberataque con el fin de poner fin a la actividad cibernética maliciosa,[50] confirmando el carácter "instrumental" y no punitivo de las "contramedidas". [51]

**31.** Las directrices del *Cyber Diplomacy Toolbox* no contemplaban la posibilidad de que otros Estados miembros participaran en las contramedidas, ni de que éstas se adoptaran de forma colectiva[52]

[46] Servicio Europeo de Acción Exterior (Consejo dela Unión Europea [Secretaría General]), Third-party Countermeasures under International Law, cit., p. 28.

[47] Párrafos 1 y 8 del Comentario introductorio al capítulo II de la tercera parte del Proyecto sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, responsabilidad del Estado por hechos internacionalmente ilícitos, Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones Informe de la Comisión de Derecho Internacional, quincuagésimo tercer período de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto de 2001), Suplemento No. 1 (A/53/40), Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto de 2001), Suplemento núm. 10 (A/56/10), Naciones Unidas, Nueva York, 2001, pp. 1-591, en pp. 309-316 (en adelante también CDI 2021). Véase también J.A. Frowein "Reactions by not directly affected States to breaches of public international law", *Recueil des cours....* 1994-IV (Dordrecht), Martinus Nijhoff, vol. 248 (1995), p. 345.

[48] CDI 2001, párrafo 8: "En la práctica se han dado casos de contramedidas adoptadas por otros Estados, en particular los mencionados en el artículo 48, cuando ningún Estado ha resultado lesionado o en nombre y a petición de un Estado lesionado. Estos casos son controvertidos y la práctica es embrionaria. Este capítulo no pretende regular la adopción de contramedidas por Estados distintos del Estado lesionado".

[49] Véase a este respecto K. Härmä y T. Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", The NATO Cooperative Cyber Defence Centre of Excellence: "existen dos obstáculos importantes para calificar una respuesta de contramedida: en primer lugar, la ciberactividad maliciosa original tiene que atribuirse a un Estado, no simplemente a un actor no estatal que opere desde el territorio del Estado; y en segundo lugar, sólo el Estado afectado por la ciberactividad maliciosa tiene derecho a recurrir a contramedidas, lo que limita la posibilidad de que otros Estados miembros de la UE ayuden al Estado afectado, ya que su respuesta no debe alcanzar el nivel de contramedida" (traducción del autor).

[50] Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades cibernéticas maliciosas ("Cyber Diplomacy Toolbox"), 7 de junio de 2017, CYBER 91 RELEX 482 POLMIL 58 CFSP/CFSP 476.

[51] Véase al respecto lo señalado por la CDI, en palabras de C. Gutiérrez Espada y M.J. Cervell Hortal, *El Derecho Internacional (Corazón y Funciones),* cit. p. 351, párrafo 27 del capítulo 7: Ya en 1996, al aprobar en primera lectura su Proyecto sobre la responsabilidad del Estado, la CDI optó por una concepción "instrumental" y no "punitiva" de las contramedidas (comentario 2 al art. 47, Anuario de la CDI 1996, II, Segunda Parte); y un año más tarde (as. Gabcíkovo-Nagymaros) la CIJ reafirmó la idea al darla por sentada en la regulación de las contramedidas en el derecho vigente (Informes de la CIJ 1997, pp. 56-57).

[52] Directrices de aplicación del Marco de respuesta diplomática conjunta de la UE a las actividades cibernéticas malintencionadas, Bruselas, 9 de octubre de 2017, p. 10: " Un Estado miembro que sea víctima de una actividad cibernética ma-

, como sí ocurría con el derecho de legítima defensa garantizado por el artículo 51 de la Carta de las Naciones Unidas en los casos graves en que las actividades cibernéticas malintencionadas pudieran equivaler al uso de la fuerza o a un ataque armado en el sentido de la Carta.

**32.** La posición de la Unión Europea parece coherente con la conclusión alcanzada por la CDI en 2001, así como con el Derecho internacional vigente. En efecto, a diferencia de la legítima defensa, que puede ser individual o colectiva, las contramedidas colectivas no se consideran aceptables. Esta fue al menos la posición adoptada por la Corte Internacional de Justicia en el caso de las actividades militares y paramilitares en y contra Nicaragua (1986):

> "While an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot. as the Court has already observed (paragraph 21 1 above). produce any entitlement to take collective countermeasures involving the use of force. The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force"[53].

**33.** La adopción de contramedidas colectivas parece más plausible en caso de incumplimiento de obligaciones internacionales *erga omnes* o en caso de obligaciones colectivas debidas a un grupo de Estados.

**34.** En relación con lo anterior, ya el proyecto de Informe de la CDI de 2000 establecía en su artículo 54.1 que "1. Todo Estado facultado en virtud del párrafo 1 del artículo 49 para invocar la responsabilidad de un Estado podrá tomar contramedidas a petición y en nombre de cualquier Estado lesionado por la violación, en la medida en que ese Estado pueda tomar a su vez contramedidas en virtud del presente Capítulo."[54] Esta disposición fue muy objetada por los Estados y finalmente se retiró del texto final.

**35.** La versión aprobada del artículo 54 en el informe de la CDI de 2001 no prejuzga la adopción de contramedidas colectivas en caso de violación de obligaciones debidas a la comunidad internacional en su conjunto o a un grupo de Estados para la protección de un interés colectivo, aplazando de hecho el debate de la cuestión incluso para este tipo de obligaciones. Dice así: "Este capítulo no prejuzga acerca del derecho de cualquier Estado, facultado por el párrafo 1 del artículo 48 para invocar la responsabilidad de otro Estado, a tomar medidas lícitas contra este Estado para asegurar la cesación de la violación y la reparación en interés del Estado lesionado o de los beneficiarios de la obligación violada".[55]

**36.** La misma solución se adoptó en el artículo 57 del proyecto de artículos de 2011 sobre la responsabilidad de las organizaciones internacionales, habida cuenta de la ausencia aún más notoria de práctica en la que estuvieran implicadas organizaciones internacionales. No obstante, la CDI señaló que la práctica existente en ese momento ya incluía ejemplos de una organización internacional no lesionada que adoptaba contramedidas contra un Estado presuntamente responsable, y citó en particular

---

lintencionada que constituya un hecho internacionalmente ilícito podrá, en determinadas condiciones, recurrir legalmente a contramedidas no forzosas y proporcionadas. Estas contramedidas constituyen acciones dirigidas a otro Estado responsable del hecho internacionalmente ilícito, que de otro modo violaría una obligación debida a ese Estado. Tales contramedidas no forzosas se llevan a cabo para obligar o convencer a este último de que cese la ciberactividad maliciosa, en cumplimiento de sus obligaciones internacionales".

[53] Sentencia de 27 de junio de 1986, ICJ Reports/CIJ Reports 1986, p. 117, párr. 249.

[54] Responsabilidad del Estado. Proyecto de artículos aprobado provisionalmente por el Comité de Redacción en segunda lectura (A/CN.4/L.600, 21 de agosto de 2000), pp. 1-16, p. 15.

[55] CIT 2001, en el artículo 54. Véase en este sentido C. Gutiérrez Espada, "Las "contramedidas de terceros" (evolución del concepto a la luz de la práctica internacional)", *Anuario Español de Derecho Internacional* (AEDI), núm. 40 (2024), de próxima publicación, pp. 1-20, en p. 4.

las medidas adoptadas por el Consejo de la Unión Europea contra Birmania/Myanmar en vista de las "violaciones graves y sistemáticas de los derechos humanos en Birmania". [56]

**37.** En este marco, en noviembre de 2022 el Servicio de Acción Exterior de la Unión Europea llevó a cabo un análisis exhaustivo y muy interesante de esta cuestión en un documento hecho público por la plataforma *AsktheEU.org* a raíz de una solicitud de acceso a documentos en virtud del Reglamento (CE) nº 1049/2001.[57] En su estudio, el SEAE señala que se han producido avances significativos desde 2001, cuando la CDI adoptó el artículo 57 anteriormente mencionado. En concreto, menciona cuatro casos en los que Estados occidentales, pero también de otros continentes, han adoptado contramedidas colectivas, a saber:

i) en 2005 contra Irán en relación con el desarrollo de su Programa Nuclear,
ii) en 2011 contra Libia por la represión de manifestaciones y protestas en el marco de la llamada "Primavera Árabe",
iii) también en 2011 contra Siria por el uso de la fuerza por parte del régimen en el contexto del conflicto interno del país,
iv) y en 2014 contra Rusia por su anexión de Crimea.[58]

**38.** Estos acontecimientos llevaron al Servicio Europeo de Acción Exterior a abogar por la formación de una norma de Derecho internacional consuetudinario que permita a terceros Estados tomar contramedidas contra un Estado que viole normas imperativas de derecho internacional. Según el SEAE, no sólo la práctica sino también la *opinio iuris* son claras, al menos en el caso de una violación flagrante de una norma *erga omnes como* en el caso de la agresión rusa a Ucrania.

**39.** De esta forma, el SEAE rescata y apoya a nuestro juicio la postura inicial de la CDI en su proyecto del año 2000, rechazando implícita pero necesariamente que la práctica sea aún embrionaria habida cuenta de la evolución sufrida en la práctica estatal y de organizaciones internacionales en los últimos 22 años.

**40.** En este contexto, y en relación con las contramedidas adoptadas en respuesta a la ciberactividad maliciosa, el Manual de Tallin 2.0 reconocía que había voces que defendían la legitimidad de las contramedidas colectivas, especialmente en situaciones en las que ningún Estado es responsable de la ciberoperación maliciosa en cuestión[59] . Esta tesis no es sólo doctrinal, sino que también ha sido defendida públicamente por algunos Estados. Por ejemplo, la Presidenta de la República de Estonia Kersti Kaljulaid expresó abiertamente su apoyo a esta opinión en 2019:

---

[56] Proyecto de artículos sobre la responsabilidad de las organizaciones internacionales 2011, aprobado por la Comisión de Derecho Internacional en su 63º período de sesiones, celebrado en 2011, y presentado a la Asamblea General como parte del informe de la Comisión sobre la labor realizada en ese período de sesiones (A/66/10, párr. 87), pág. 96. Véase también para esta referencia C. Gutiérrez Espada, "Las "contramedidas de terceros" (evolución del concepto a la luz de la práctica internacional)", *cit*., en p. 5.

[57] Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, DO L 145 de 31.5.2001, p. 43-48. La solicitud fue presentada por Davide Giovannelli en julio de 2023. Sobre las implicaciones de este documento sobre la figura de las contramedidas colectivas véase C. Gutiérrez Espada, Las "contramedidas de terceros" (evolución del concepto a la luz de la práctica internacional), Anuario Español de Derecho Internacional, Año 2024, Número 40, pp. 1-20.

[58] Servicio Europeo de Acción Exterior (Consejo de la Unión Europea [Secretaría General]), *Third-party Countermeasures under International Law (Documento revisado),* Bruselas, 17 de noviembre de 2022, WK 15858/2022 INIT, LIMITE, COJUR, pp. 1-33).

[59] M.N. Schmitt (editor general), *Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Operaciones Cibernéticas*, cit. p. 113: "El Grupo Internacional de Expertos reconoció un punto de vista según el cual pueden adoptarse contramedidas contra actores no estatales. Según este punto de vista, las entidades no estatales pueden llevar a cabo operaciones cibernéticas que violen las obligaciones que supuestamente deben a los Estados, como el cumplimiento de la prohibición del uso de la fuerza y la exigencia de respetar su soberanía. Según este punto de vista, en la medida en que los actores no estatales deben obligaciones jurídicas a los Estados, los Estados "perjudicados" tienen derecho a tomar contramedidas contra los actores no estatales en caso de que incumplan dichas obligaciones".

"Estonia promueve la posición de que los Estados que no resulten directamente perjudicados puedan aplicar contramedidas para apoyar al Estado directamente afectado por la operación cibernética maliciosa. Las contramedidas aplicadas deben seguir el principio de proporcionalidad y otros principios establecidos en el derecho consuetudinario internacional"[60].

**41.** Del mismo modo, Nueva Zelanda ha expresado recientemente su apoyo a una opinión similar:

"Dado el interés colectivo en la observancia del derecho internacional en el ciberespacio, y la asimetría potencial entre los estados maliciosos y los estados víctimas, Nueva Zelanda está abierta a la proposición de que los estados víctimas, en circunstancias limitadas, puedan solicitar asistencia a otros estados para aplicar contramedidas proporcionadas para inducir el cumplimiento por parte del estado que actúa en violación del derecho internacional. [...]"[61]

**42.** En cambio, otros Estados, como Francia han reafirmado recientemente la tesis ortodoxa de que las contramedidas colectivas no están autorizadas en Derecho internacional:

"Según el derecho internacional, tales contramedidas deben ser adoptadas por Francia en su calidad de víctima. Las contramedidas colectivas no están autorizadas, lo que excluye la posibilidad de que Francia adopte tales medidas en respuesta a una violación de los derechos de otro Estado."[62]

**43.** Del mismo modo, Canadá ha sostenido oficialmente que no existe suficiente *opinio iuris* para las contramedidas cibernéticas colectivas, aunque este Estado parece abierto a esta posibilidad en el futuro:

"La asistencia puede prestarse a petición de un Estado lesionado, por ejemplo cuando el Estado lesionado no posee todos los conocimientos técnicos o jurídicos necesarios para responder a ciberactos internacionalmente ilícitos. Sin embargo, las decisiones sobre las posibles respuestas son competencia exclusiva del Estado lesionado. Canadá ha considerado el concepto de "contramedidas cibernéticas colectivas" pero, hasta la fecha, no ve suficiente práctica estatal u opinio juris para concluir que estén permitidas por el derecho internacional. Canadá distingue las "contramedidas cibernéticas colectivas" de las acciones adoptadas en "legítima defensa colectiva", incluidas las medidas adoptadas en el ciberespacio".[63]

**44.** Por otro lado, en el contexto de los ataques híbridos, el Parlamento Europeo aboga desde 2021 por una reinterpretación de las cláusulas de defensa mutua y solidaridad consagradas en los artículos 42, apartado 7, del TUE y 222 del TFUE que permita, *entre otras cosas, la adopción de* contramedidas colectivas por parte de los Estados miembros de la UE de forma voluntaria. [64]

**45.** En 2022, el Parlamento Europeo expresó una opinión similar en relación con China. El Parlamento subrayó "la necesidad de fomentar una cooperación más estrecha con los países de la OTAN y el G7 para combatir las amenazas híbridas, como los ciberataques y las campañas de desinformación provenientes de China; permitiendo, por ejemplo, que los Estados miembros impongan contramedidas

[60] Discurso de la Presidenta de la República de Estonia en la inauguración de CyCon 2019. Disponible en el siguiente enlace: https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/

[61] New Zealand Foreing Affairs and Trade, The Application of International Law to State Activity in Cyberspace (1 de diciembre de 2020) 3-4. Véase como referencia el siguiente enlace: https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf (traducción del autor).

[62] International Law Applied to Operations in Cyberspace, Documento compartido por Francia con el grupo de trabajo de composición abierta establecido por la resolución 75/240, en 4. Disponible en https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf. (traducción del autor).

[63] Gobierno de Canadá, Derecho internacional aplicable en el ciberespacio, en el punto 37, disponible en https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9. (traducción del autor).

[64] Resolución del Parlamento Europeo, de 7 de octubre de 2021, sobre el estado de las capacidades de ciberdefensa de la UE (2020/2256(INI)) DO C 132 de 24.3.2022, p. 102-112, apartado 35. Véase, para una propuesta similar, la Resolución del Parlamento Europeo, de 17 de febrero de 2022, sobre la aplicación de la Política Común de Seguridad y Defensa - Informe anual 2021 (2021/2183(INI)), DO C 342 de 6.9.2022, p. 167-190, apartado 54.

colectivas de manera voluntaria, incluso en los casos en los que los ataques no sean tan graves como para activar el artículo 5 del Tratado de la OTAN o el artículo 42, apartado 7, del TUE."[65]

**46.** Ese mismo año, el Parlamento Europeo también consideró "la disuasión, la atribución y las contramedidas colectivas, incluidas las sanciones" como una de las áreas de trabajo de la reciente "comisión especial sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación, y el refuerzo de la integridad, la transparencia y la responsabilidad en el Parlamento Europeo".[66]

**47.** El Parlamento manifestó con rotundidad en una resolución adoptada en paralelo a la decisión mencionada que las contramedidas en este contexto pueden incluir sanciones adoptadas en virtud de los artículos 29 TUE y 215 TFUE,[67] y se refirió a las adoptadas en caso de ciberataques en virtud de la Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a la adopción de medidas restrictivas contra ciberataques que amenacen a la Unión o a sus Estados miembros[68] y del Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a la adopción de medidas restrictivas contra ciberataques que amenacen a la Unión o a sus Estados miembros[69] .

**48.** Resulta relevantes asimismo que el Parlamento Europeo solicitara también "a la Unión que defina con claridad qué constituye un hecho internacionalmente ilícito y que establezca unos umbrales mínimos para la puesta en marcha de contramedidas como consecuencia de esa nueva definición, que deben ir acompañadas de una evaluación de impacto para aportar seguridad jurídica; señala que el Consejo debe poder tomar decisiones por mayoría, en vez de por unanimidad, sobre las sanciones relativas a injerencias extranjeras". [70]

**49.** Lo anterior plantea la cuestión de si las contramedidas colectivas en respuesta a actividades cibernéticas maliciosas pueden adoptarse de manera lícita en casos más allá de la violación de normas *erga omnes*, que podrían aceptarse como Derecho internacional consuetudinario si atendemos a la opinión del SEAE, además de que, en realidad, la violación de una obligación erga omnes afecta a toda la comunidad internacional y por tanto, en este caso se podría argumentar que más que una medida colectiva es bilateral con independencia del Estado que la adopte, o en casos de incumplimiento de obligaciones contraídas con un grupo de Estados.

En favor de esta posición se pueden esgrimir tres argumentos:

(i) la práctica estatal reciente muestra un aumento en la adopción de contramedidas colectivas, así como una *opinio iuris* favorable, y no todos los casos de práctica estatal menciona-

[65] Resolución del Parlamento Europeo, de 16 de septiembre de 2021, sobre una nueva estrategia UE-China (2021/2037(INI)) DO C 117 de 11.3.2022, p. 40-52, apartado 27.

[66] Decisión del Parlamento Europeo, de 10 de marzo de 2022, relativa a la creación de una comisión especial sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (INGE 2), y a la definición de sus responsabilidades, composición numérica y mandato (2022/2585(RSO)), DO C 347 de 9.9.2022, p. 238-240, apartado K(1)(a)(x). Esta decisión ha sido modificada en 2023 sin que ello afecte a la parte citada. Decisión del Parlamento Europeo, de 14 de febrero de 2023, por la que se modifica la Decisión, de 10 de marzo de 2022, relativa a la creación de una comisión especial sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (INGE 2), y por la que se adaptan su denominación y sus competencias (2023/2566(RSO)).

DO C 283 de 11.8.2023, p. 60-63.

[67] Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)), DO C 347 de 9.9.2022, p. 61-96, en 136-142.

[68] Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra ciberataques que amenacen a la Unión o a sus Estados miembros, ST/7299/2019/INIT, DO L 129I de 17.5.2019, p. 13/19.

[69] Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a la adopción de medidas restrictivas contra ciberataques que supongan una amenaza para la Unión o sus Estados miembros, ST/7302/2019/INIT, DO L 129I de 17.5.2019, p. 1/12.

[70] Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación, citada en el párrafo 137.

dos por el SEAE en su estudio se referían a violaciones de normas *erga omnes* (véase, por ejemplo las medidas adoptadas contra Libia por la represión de manifestaciones y protestas en 2011) y podría decirse lo mismo del ejemplo dado por la CDI en 2011 (violaciones de los derechos humanos en Birmania)

(ii) algunos Estados miembros han pedido abiertamente la adopción de contramedidas colectivas en el contexto cibernético, y

(iii) el Parlamento Europeo también ha abogado por la adopción de contramedidas colectivas, en particular sanciones, en el contexto conexo de ataques híbridos/desinformación.

**50.** A la luz de lo anterior, aunque tanto la CDI como la Corte Internacional de Justicia han rechazado por el momento la adopción de contramedidas colectivas, y la práctica de los Estados hasta la fecha no parece ser suficientemente coherente y universal,[71] las posiciones adoptadas recientemente por la Unión Europea pueden contribuir a ampliar los límites existentes en materia de contramedidas colectivas para concebir algunas contramedidas colectivas lícitas en caso de ciberataques graves, y a petición del Estado perjudicado.

**51.** En todo caso, los Estados miembros de la Unión sí que podrían defender con arreglo al Derecho internacional vigente, aunque resultaría difícil de justificar, su actuación conjunta en respuesta a un ciberataque invocando la excepción de "necesidad" prevista en la regla 26 del Manual de Tallinn 2.0[72], que permite la adopción de medidas colectivas y no requiere la comisión previa de un hecho ilícito internacional[73]. Para ello, los Estados miembros deberían poder acreditar que la actuación conjunta se adopta en respuesta a actos que presentan un peligro grave e inminente, ya sea de naturaleza cibernética o no, a un interés esencial, y que esta respuesta constituye el único medio de salvaguardar dicho interés.

**52.** Esta regla se corresponde con el Estado de necesidad al que hace referencia el artículo 25 del proyecto de artículos de la CDI, que ha sido aceptado por el Tribunal Internacional de Justicia y, que el Manual de Tallinn 2.0 considera que constituye Derecho internacional consuetudinario[74]. De hecho, como se ha afirmado, el Manual de Tallinn parece ir incluso más allá de lo previsto por la costumbre internacional, encarnada en el mencionado artículo 25. Lo anterior se desprende de dos razones principales:

(i) el Manual de Tallin 2.0 considera, respecto de la inminencia del peligro, que el peligro es siempre inminente cuando la "ventana de oportunidad" de tomar medidas para prevenirlo está a punto de cerrar, y

(ii) no descarta que se pueda emplear el uso de la fuerza por razones de necesidad[75], lo que sin embargo no es aceptable habida cuenta de que la prohibición del uso de la fuerza es una norma de *ius cogens* y no se prevé en Derecho internacional el estado de necesidad como una excepción a la misma. No obstante, como acertadamente ha subrayado el profesor GUTIÉRREZ ESPADA, la prohibición del uso de la fuerza sólo tiene como *ius cogens* su núcleo duro (la agresión), y el uso de la fuerza en estado de necesidad para evitar un peligro grave inminente contra intereses esenciales del Estado no constituye una agresión.[76]

---

[71] C. Gutierrez Espada, *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio,* Aranzadi, Cizur Menor, 2020, en particular Capítulo 3, apartado 4, párrafo 69.

[72] M.N. Schmitt (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, cit., p. 135: "Rule 26 – Necessity A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it".

[73] Id. (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, cit., comentario 9 a la regla 26.

[74] *Ibid*.: "in light of its acceptance by the International Court of Justice and other bodies, the International Group of Experts agreed that as a general matter, and as described below, the plea is customary in nature and can be applied in the cyber context".

[75] Id. (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, cit., comentario 18 a la regla 26: "It should be cautioned that whether measures based on the plea of necessity may involve forcible action is unsettled in international law. The International Group of Experts was split on this issue [...]".

[76] C. Gutiérrez Espada, *El estado de necesidad y el uso de la fuerza en Derecho internacional reflexiones sobre la inter-*

**53.** De hecho, para los expertos que redactaron el Manual de Tallinn 2.0, que no ven claro que el derecho de legítima defensa lo sea de las Organizaciones internacionales *per se*, el estado de necesidad puede constituir una válvula de escape. A nuestro juicio, la invocación de esta figura deberá, no obstante, respetar las obligaciones impuestas por el Derecho internacional general, recordando además que el uso de las contramedidas por organizaciones internacionales tiene límites mayores respecto del uso de esta figura por los Estados[77].

**54.** A este respecto, si las medidas restrictivas aprobadas por la Unión frente a un ciberataque son tales que pudieran ser interpretadas como dirigidas a un Estado (i.e. por el uso de infraestructuras estatales, la involucración de funcionarios, la violación de la debida diligencia, o una condena o imputación pública que acompañara la adopción de las medidas restrictivas…) la Unión podría invocar la necesidad de su actuación, si se cumplen los requisitos mencionados, para evitar cualquier responsabilidad internacional derivada de su respuesta al ciberataque en cuestión. A este respecto, algunos Estados como Francia,[78] Alemania[79] y Japón[80] han aceptado recientemente la posibilidad de invocar el estado de necesidad en el ámbito cibernético, aunque estas posturas son minoritarias.

## IV. La legítima defensa en respuesta a ciberamenazas

**55.** De conformidad con el artículo 51 de la Carta de las Naciones Unidas, ninguna disposición de la Carta "menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales […]." En esta sección se analiza si los Estados pueden ejercer su derecho inmanente de legítima defensa individual o colectiva, en caso de ser víctimas de un ciberataque.

**56.** El artículo 51 de la Carta presupone la existencia de un "ataque armado", por tanto, el ciberataque que motive la invocación de este artículo debe poder definirse como tal. Para determinar la noción de ciberataque grave como ataque armado a los efectos del artículo 51 de la Carta resulta necesario subrayar que, de conformidad con el Derecho internacional, y en particular con la jurisprudencia del Tribunal Internacional de Justicia, sólo el uso de la fuerza armada grave, no un "uso menor" de la misma, permite alegar el derecho de legítima defensa[81]. A este respecto, para evaluar la gravedad de un ataque armado, el criterio aplicable según el Tribunal Internacional de Justicia es el de la envergadura o

*pretación y consecuencias que pueden derivarse, en tal materia, de la aceptación por la CDI del estado de necesidad*, Tecnos, Madrid, 1987; C. Schaller, 'Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity' (Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) *Texas Law Review*, n.º 95, 2016, p. 1619 y DELERUE, F., *Cyber operations and international law*, Cambridge University Press, 2020, p. 349. Véase también sobre el estado de necesidad y el uso de la fuerza M.J. Cervell Hortal, *La legítima defensa en el derecho internacional contemporáneo: (nuevos tiempos, nuevos actores, nuevos retos)*, cit, pp. 57-62.

[77] Véase a este respecto el artículo 22 del proyecto de artículos sobre la responsabilidad de las organizaciones internacionales (2011), aprobado por la Comisión de Derecho Internacional de las Naciones Unidas, en segunda lectura, en su 63° período de sesiones (2011). Véase también respecto de la evolución del debate sobre este artículo C. Gutierrez Espada, *La responsabilidad internacional de Estados y Organizaciones (balance provisional de coincidencias y matices)*, Diego Marín, Murcia, 2010; y, sobre todo, C. Gutierrez Espada, *La responsabilidad internacional de las organizaciones internacionales a la luz del proyecto definitivo de artículos de la Comisión de Derecho Internacional (2011)*, Comares, Granada, 2011, pp. 177-206.

[78] Ministerio de Defensa de Francia, International Law Applied to Operations in Cyberspace, *cit*., p. 8.

[79] Gobierno Federal de Alemania, 'On the Application of International Law in Cyberspace', cit., pp. 14-15

[80] Ministerio de Asuntos Exteriores de Japón, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', 28 de mayo de 2021, p. 5: "The Government of Japan is of the view that a State may invoke necessity under international law when the requirements shown in Article 25 of the ILC's Articles on State Responsibility are satisfied."

[81] Sentencia 27 junio 1986, ICJ Reports/CIJ Recueil 1986, pp. 14 ss., párrafos 191-195 y 210-211; sentencia 6 noviembre 2003, caso de las plataformas petrolíferas, ICJ Reports/CIJ Recueil 2003, párrafos 51, 64 in fine y 72; y sentencia 19 diciembre 2005, actividades armadas en la República Democrática del Congo, ICJ Reports/CIJ Recueil 2005, párrafos 127, 146, 161-164.

alcance y efectos (scale and effects),[82]criterio citado por algunos Estados como Estonia,[83] Dinamarca,[84] o Finlandia,[85] para sostener que ciertos ciberataques graves equivalen a un ataque armado a en el sentido de esta jurisprudencia.

**57.** En efecto, como ha señalado GUTIÉRREZ ESPADA, el criterio a seguir es el de los efectos o consecuencias y no tanto el de los medios empleados o el de los objetivos perseguidos[86]. Por otro lado, como ha señalado SEGURA SERRANO recientemente con referencia a la jurisprudencia del Tribunal Internacional de Justicia en el asunto *Armas Nucleares*, "como punto de partida se puede afirmar que no hay nada que impida considerar una operación cibernética como constitutiva de un ataque armado."[87]

**58.** En el caso de ciberataques, el Manual de Tallinn 2.0 concluye que los que resulten en la muerte o lesión de personas, causen daños físicos, o supongan la destrucción de bienes de manera significativa constituyen usos de la fuerza que generan el derecho de legítima defensa, por tanto ataques armados[88]. Alemania ha expresado públicamente su apoyo a esta conclusión del Manual.[89] Por otro lado, como ha señalado Finlandia, más allá de la muerte o lesión de personas, y los daños físicos significativos "it is impossible to set a precise quantitative threshold for the effects, and other circumstantial factors must be taken into account in the analysis, as well."[90]

**59.** En todo caso, la mayor parte de ciberataques no alcanza, afortunadamente, este (impreciso) umbral. Sin embargo, una potencia tan relevante en el ciberespacio como Estados Unidos mantiene, afortunadamente a nuestro juicio de forma aislada en la esfera internacional, que cualquier uso de la fuerza permite la invocación del derecho inmanente de legítima defensa, rechazando explícitamente la distinción efectuada por el Tribunal Internacional de Justicia entre usos menores de la fuerza y ataque armado.[91]

**60.** De hecho, como se ha afirmado, ningún ciberataque ha reunido hasta la fecha las características exigidas para ser considerado como un ataque armado[92], ni Estado alguno ha alegado formalmente

[82] Sentencia 27 junio 1986, ICJ Reports/CIJ Recueil 1986, cit., párrafo 195: "The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces."(énfasis añadido)

[83] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, cit., p. 30: "Estonia believes that cyber operations that cause injury or death to persons, damage or destruction could amount to an armed attack under the UN Charter"

[84] Gobierno de Dinamarca, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 Julio de 2023), pp. 6-7.

[85] International law and cyberspace, Finland's national positions, p. 6.

[86] C. Gutierrez Espada, *De la legítima defensa y el ciberespacio*, Comares, Granada, 2020, párrafo 24.

[87] A. Segura Serrano, *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023, p. 112. En aquel asunto, el TIJ señaló que las previsiones de la Carta de Naciones Unidas sobre el recurso a la fuerza "apply to any use of force, regardless of the weapons employed" (Legality of the Threat or Use of Nuclear Weapons, I.C.J. Reports 1996, p. 226, párrafo 39),

[88] M.N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 69, comentario 8, p. 333: "Acts that injure or kill persons or physically damage or destroy objects are uses of force", y (*a contrario*), Regla 71, comentario 12, p. 342: "The case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled".

[89] Gobierno Federal de Alemania, 'On the Application of International Law in Cyberspace', Position Paper (Marzo de 2021), p. 15: "The right to self-defence according to art. 51 UN Charter is triggered if an armed attack occurs. Malicious cyber operations can constitute an armed attack whenever they are comparable to traditional kinetic armed attack in scale and effect. Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0."

[90] International law and cyberspace, Finland's national positions, p. 6.

[91] US Department of Defense, Office of the General Counsel, Law of War Manual (Junio de 2015, actualizado en julio de 2023), apartado 1.11.5.2: "The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force. Others [refiriéndose a la sentencia en el asunto Nicaragua], however, would be inclined to draw more of a distinction between "armed attacks" and uses of force that do not give rise to the right to use force in self-defense."

[92] F. Delerue, *Cyber operations and international law*, cit., p. 461. Más recientemente véase también A. Segura Serrano, *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023, p. 113.

el derecho de legítima defensa en respuesta a un ciberataque[93], aunque es evidente que los efectos de un ciberataque pueden ser tan catastróficos como los de un ataque llevado a cabo con armas cinéticas.

**61.** A este respecto, el Ministerio de Defensa francés ha señalado que un ciberataque que afectara a infraestructuras críticas con consecuencias importantes, o que pudiera paralizar secciones enteras de la actividad del país, desencadenara desastres tecnológicos o ecológicos y causara numerosas víctimas, sería similar al uso de armas convencionales, y podría por tanto ser considerado como un ataque armado[94]. Más recientemente lo han hecho también Italia[95] o Noruega.[96]

**62.** Cuestión distinta es la planteada por algunos expertos del grupo internacional encargado de redactar el Manual de Tallinn, a saber, si cabría invocar la legítima defensa en respuesta a un ciberataque que no cause daños físicos, pero sí una grave perturbación. Cabe recordar que un ataque de este tipo tuvo lugar en Estonia en 2007, pocos días después del traslado en Tallin del monumento a los soldados soviéticos caídos durante la II Guerra Mundial[97]. De hecho, el ciberataque del que fue objeto Estonia se compuso de numerosos ciberataques, lanzados desde Rusia con apoyo oficial según el Gobierno Estonio, que crearon un nivel de tráfico en Internet sin precedentes durante semanas. Este tráfico colapsó las páginas web de bancos, medios de prensa y organismos gubernamentales, impidiendo a los empleados estatales comunicarse por correo electrónico. Estonia valoró entonces la posibilidad de alegar su derecho a la legítima defensa, así como de invocar el artículo 5 del Tratado de la OTAN en respuesta al ciberataque del que fue víctima[98], comparado por el entonces ministro de defensa estonio con un bloqueo naval, un acto de guerra[99], y por un miembro del parlamento de ese país con una explosión nuclear[100]. Cabe recordar a este respecto que la OTAN aceptó en 2014 que un ciberataque puede permitir la invocación del Artículo 5[101].

---

[93] *Ibid*. Véase también Ministère des Armées. Republique Française, *Droit International appliqué aux opérations dans le cyberespace*, 9 septembre 2019, disponible en www.defense.gouv.fr, pp. 1-18, p. 9 " À l'heure actuelle, aucun État n'a qualifié une cyberattaque menée à son encontre d'agression armée. "

[94] Ministerio de Defensa de la República Francesa, *Droit International appliqué aux opérations dans le cyberespace*, 9 septembre 2019, cit., p. 9 " Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables. Cela serait le cas d'une opération dans le cyberespace provoquant une déficience des infrastructures critique avec des conséquences significatives, ou susceptibles de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques et de faire de nombreuses victimes. Dans une telle hypothèse, les effets de cette opération seraient similaires à ceux qui résulteraient de l'utilisation d'armes classiques".

[95] Ministerio de Asuntos Exteriores y Cooperación Internacional, Italian position paper on "International law and cyberspace", p. 9: "Italy deems that wrongful cyber operations conducted by State or non-State actors may constitute an armed attack when their scale and effects are comparable to those resulting from conventional armed attacks, resulting in significant physical damage of property, human injury and loss of life, or disruption in the functioning of critical infrastructure."

[96] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, cit., p. 70: "A cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law. Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash"

[97] Sobre este ciberataque y las primeras reacciones al mismo puede consultarse la siguiente noticia publicada en mayo de 2007 en el diario El País: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

[98] P. Pawlak/ T. Biersteker, (eds.), *Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace*, Chaillot Paper 155, European Union Institute for Security Studies, 2019, en particular el capítulo "Mission controls Sanctions under international law", p. 46.

[99] La referencia a la entrevista al Ministro de defensa estonio puede consultarse en el diario New York Times: ""It turned out to be a national security situation," Estonia's defense minister, Jaak Aaviksoo, said in an interview. "It can effectively be compared to when your ports are shut to the sea". Este artículo está disponible en el siguiente enlace: https://www.nytimes.com/2007/05/29/technology/29estonia.html

[100] En los términos utilizados por el portavoz del Parlamento, Ene Ergma: "When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing." Véase la referencia en Buchan., R, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law Vol. 17, No. 2 (2012), pp. 211-227, p. 215.

[101] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014: "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis".

**63.** A este respecto, tanto el Manual de Tallin 2.0 como, más recientemente, el Ministerio de Defensa francés, determinan que la acumulación de los efectos de varios ciberataques que individualmente considerados no serían suficientes para ser considerados como ataque armado puede traspasar el umbral requerido para alegar el derecho de legítima defensa[102]. Francia encuentra apoyo para esta afirmación en la sentencia del Tribunal Internacional de Justicia en el asunto de las plataformas petrolíferas, en el que el Tribunal no descartó el criterio de evaluar si una serie de ataques contra los Estados Unidos constituye un ataque armado[103]. En un sentido similar, una comunicación de la Comisión de 2016 señalaba que varias amenazas híbridas, como podrían ser varios ciberataques, pueden constituir una "agresión armada" en el sentido del artículo 42, apartado 7, TUE[104].

**64.** A nuestro juicio, tal y como sostienen algunos miembros del grupo de expertos del Manual de Tallin 2.0[105], y más recientemente Gutierrez Espada[106], un ciberataque que cause una grave perturbación en sistemas esenciales para la vida de los ciudadanos de un Estado, aunque no suponga daños físicos significativos, sí que permitiría la invocación del derecho de legítima defensa por parte del Estado afectado. A este respecto, gobiernos relevantes en el ciberespacio como Francia[107] y el Reino Unido[108], han señalado que ciberataques de este tipo pueden ser definidos como usos de la fuerza, generadores por tanto en el Estado afectado del derecho a adoptar contramedidas o de invocar la legítima defensa en función de sus efectos. Asimismo, recientemente Singapur ha expresado también públicamente esta conclusión en términos inequívocos: "In Singapore's view, it is also possible that, in certain limited circumstances, malicious cyber activity may amount to an armed attack even if it does not necessarily cause death, injury, physical damage or destruction, taking into account the scale and effects of the cyber activity. An example might be a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure."[109]

**65.** Por último, cabe preguntarse si un ciberataque que no haya sido aún perpetrado puede generar el derecho a la legítima defensa. Este supuesto es distinto de lo que algunos autores denominan

---

[102] M. N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 71, comentario 11, p. 342: "An important issue is whether a State may exercise the right of self-defence in response to a series of cyber incidents that individually fall below the threshold of an armed attack. In other words, can they constitute an armed attack when aggregated? The International Group of Experts agreed that the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incidents as a composite armed attack".; Ministère des Armées. Republique Française, *Droit International appliqué aux opérations dans le cyberespace*, 9 septembre 2019, cit., p. 9.

[103] Asunto de las plataformas petrolíferas, ICJ Reports/CIJ Recueil 2003, párrafo 64. En efecto, en aquel caso el Tribunal afirmó "the question is whether that attack, either in itself or in combination with the rest of the "series of. . . attacks" cited by the United States can be categorized as an "armed attack" on the United States justifying self-defence [y concluyó el párrafo señalando que] Even taken cumulatively, and reserving, as already noted, the question of Iranian responsibility, these incidents do not seem to the Court to constitute an armed attack on the United States, of the kind that the Court, in the case concerning Military and Paramilitary Activities in and against Nicaragua, qualified as a "most grave" form of the use of force".

[104] Comunicación conjunta al Parlamento Europeo y al Consejo, Comunicación conjunta sobre la lucha contra las amenazas híbridas Una respuesta de la Unión Europea, Bruselas, JOIN/2016/018 final, p. 18: "A diferencia del artículo 222 del TFUE, si varias amenazas híbridas graves constituyen una agresión armada contra un Estado miembro de la UE, podría invocarse el artículo 42, apartado 7, del TUE para aportar una respuesta adecuada en el momento oportuno".

[105] M. N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 71, comentario 12, p. 342.

[106] C. Gutierrez Espada, *De la legítima defensa y el ciberespacio,* cit., , pp. 44-45, párrafo 27.

[107] Ministère des Armées. Republique Française, *Droit International appliqué aux opérations dans le cyberespace*, 9 septembre 2019, cit., p. 7.

[108] Ministry of Defence (Development, Concepts And Doctrine Centre). Cyber Primer. Second edition, July 2016, pp. 1-100 (disponible en www.gov.uk/mod/dcdc), p. 13 (apartado 1A.5 del Anexo 1A de su capítulo 1): "A cyber operation may constitute a use of force if it causes the same or similar effects as a kinetic attack (...) Such as a sustained attack against the UK banking system, which could cause severe financial damage to the state leading to a worsening economic security situation for the population".

[109] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, cit., p. 84, apartado 8.

*interceptive self-defence*, esto es, la invocación de la legítima defensa ante un ataque lanzado, en curso, pero que aún no ha desencadenado sus efectos, respecto del que, en nuestra opinión, sería aplicable la legítima defensa si, por sus potenciales efectos, el ciberataque es muy grave[110].

**66.** En este contexto, el Manual de Tallin 2.0 considera que cabe invocar la legítima defensa contra ciberataques inminentes[111], esto es, no perpetrados o lanzados aún, lo que resultaría conforme con el Derecho internacional general[112], aunque algunos autores discrepan[113]. Por el contrario, el Manual de Tallinn 2.0 rechaza, y aquí el apoyo doctrinal es mayor[114], la legítima defensa contra ciberataques latentes o futuros, esto es, el lanzamiento de un ataque preventivo contra un potencial agresor (o legítima defensa preventiva),[115]que también ha sido categóricamente rechazada por Estados como Francia,[116] y Brasil.[117]

**67.** En relación con lo anterior, no resulta sencillo precisar en qué momento se está ante un ataque "inminente", y por tanto se puede lanzar una operación avalada por el derecho de legítima defensa. A este respecto, la mayoría de miembros del grupo de expertos encargados de la redacción del Manual de Tallin 2.0 consideró que ese momento llega cuando el atacante está claramente comprometido a lanzar un ataque armado y el Estado víctima perderá su oportunidad de defenderse eficazmente a menos que actúe. En otros términos, sólo cabe actuar anticipadamente durante *el último lapso de oportunidad* para defenderse de un ataque armado que se avecina (the 'last feasible window of opportunity' standard)[118]. Algunos Estados, como Australia, han defendido esta figura poniendo como ejemplo ciberataques graves:

> "[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts. This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy. Consider, for example, a threatened armed

[110] Véase a este respecto, por ejemplo, T. Gazzini, "The Changing Rules on the Use of Force in International Law", Juris, 2005, pp. 151-153. En el caso de los ciberataques, por su propia naturaleza se despliegan a gran rapidez por lo que la utilidad de esta figura sería, en todo caso, limitada.

[111] M.N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 73, p. 350: "The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy".

[112] Véase a este respecto, por ejemplo, la resolución del Instituto de Derecho Internacional en su sesion de Santiago de Chile (10 A Resolution, 27 de octubre de 2007: "Problèmes actuels du recours à la force en droit international. A. Légitime défense") párr. 3. : "El derecho de legítima defensa del Estado víctima nace ante un ataque armado ("agresión armada") en curso de realización o manifiestamente inminente (...)".

[113] F. Delerue, *Cyber operations and international law*, Cambridge University Press, 2020, p. 476: "pre-emptive self-defence is highly controversial and not accepted by most States or the literature. This book adheres to the view that pre-emptive self-defence is invalid under positive international law. Moreover, pre-emptive self-defence, even if it was accepted as a de *lege lata* right of the targeted State, would be of very little help in the context of cyber operations".

[114] Véase a este respecto, por ejemplo, A. Randelzhofer y G. Nolte, "Article 51" en Simma, B. et al (eds), *The Charter of the United Nations: A Commentary*, Oxford University Press, 2012, p. 1423.

[115] M.N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 73, comentario 10, p. 353: "The International Group of Experts agreed that a preventive strike, that is, one against a prospective attacker who has not initiated any preparations or expressed either impliedly or explicitly an intention to carry out an armed attack, does not qualify as a lawful exercise of anticipatory self-defence".

[116] Ministerio de Defensa de Francia, International Law Applied to Operations in Cyberspace, 9 Septiembre de 2019, cit., p. 9.

[117] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, cit., p. 20: "For Brazil, the right to self-defense exists once there is an actual or imminent armed attack. Under international law, there is no right to "preventive self-defense" - a notion that does not find legal grounds neither in art. 51 of the Charter nor in customary international law. Finally, as with responses to armed activities using conventional weapons, self-defense against armed attacks caused by digital means must be necessary and proportionate."

[118] Id., Regla 73, comentario 4, p. 351. Los expertos añaden que lo relevante es determinar en qué momento el Estado víctima debe actuar pues, de lo contrario, se quedaría sin posibilidades de hacerlo: "This window may present itself immediately before the attack in question, or, in some cases, long before it occurs. For these Experts, the critical question is not the temporal proximity of the anticipatory defensive action to the prospective armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts".

> attack in the form of an offensive cyber operation, ...which could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?"[119]

**68.** Conviene, no obstante, alertar sobre el uso de esta figura pues, si finalmente el ciberataque no se produjera, o aun produciéndose no reuniera los efectos exigidos, la reacción armada del Estado víctima del ciberataque se convertiría en una violación del artículo 2.4 de la Carta de Naciones Unidas, y daría lugar, aquí sin duda, al derecho de legítima defensa, individual o colectiva, del Estado agredido. Además, cabe recordar a este respecto que, de conformidad con la jurisprudencia del Tribunal Internacional de Justicia, la legítima defensa está sometida a los requisitos de necesidad y proporcionalidad, que deberán ser acreditados por el Estado que la invoca[120], y que no resultan fáciles de probar en el caso de una respuesta armada a un ciberataque, pues podría parecer más ajustado a estos requisitos tratar de repeler sus efectos.

**69.** En suma, a tenor de lo anterior, el artículo 51 de la Carta puede ser legítimamente invocado en caso de ciberataque que resulte en la muerte o lesión de personas, cause daños físicos, o suponga la destrucción de bienes de manera significativa, especialmente infraestructuras críticas. Además, consideramos que se puede invocar también en caso de ciberataques que, sin causar daños físicos, supongan una perturbación grave en servicios esenciales para la vida de los ciudadanos de un Estado miembro. Por último, con arreglo al Derecho internacional general, y a la interpretación que del mismo se hace en el Manual de Tallin 2.0, se puede alegar también la legítima defensa en caso de un ciberataque inminente cuya perpetración fuera susceptible de provocar los graves efectos mencionados en este párrafo.

**70.** Por otro lado, conviene también interrogarse sobre sobre si los ciberataques deben ser imputados necesariamente a Estados para poder invocar el derecho de legítima defensa. A este respecto, de conformidad con la jurisprudencia del Tribunal Internacional de Justicia, el artículo 51 de la Carta de Naciones Unidas reconoce "la existencia de un derecho inmanente de legítima defensa en caso de ataque armado de un Estado *contra otro"*[121]. Por tanto, para su invocación es necesario que el ataque, o en este caso ciberataque, haya sido perpetrado por las fuerzas armadas de un Estado o, de conformidad con el artículo 3(g) de la definición de agresión por "El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos"[122].

**71.** Como ha precisado Gutiérrez Espada[123], esta interpretación del derecho de legítima defensa ha sido cuestionada por instituciones relevantes, como el Instituto de Derecho Internacional, que en 2007 abría la puerta –de manera cautelosa– a su invocación frente a actores no estatales[124], o el Comité

[119] Gobierno de Australia 'Australia's position on how international law applies to State conduct in cyberspace', disponible en el siguiente enlace: https://www.internationalcybertech.gov.au/our-work/annexes/annex-b

[120] Véase a este respecto, entre otras, la sentencia en el asunto de las plataformas petrolíferas *ICJ Reports/CIJ Recueil 2003*, párrafo 43: "[...]the criteria of necessity and proportionality must be observed if a measure is to be qualified as self-defence".

[121] Dictamen consultivo de 9 de julio de 2004, ICJ Reports-CIJ Recueil, párrafo 139; Véase también la sentencia de 19 de diciembre de 2005, ICJ Reports-CIJ Recueil, párrafos 146-147, en la que el Tribunal insiste en la necesidad de atribuir los ataques a un Estado, en este caso la República Democrática del Congo. De hecho, como ha subrayado GUTIERREZ ESPADA, del primer asunto no cabe desprender categóricamente la conclusión de que se excluye el derecho de legítima defensa en aquellos casos en que el ataque en cuestión tenga origen extranjero. C. Gutierrez Espada, *De la legítima defensa y el ciberespacio*, cit., pp. 13-14, párrafo 14.

[122] Resolución 3314 de las Naciones Unidas sobre definición de la agresión, Asamblea general A/RES/29/3314, Vigésimo noveno período de sesiones, 14 diciembre 1974, Anexo, artículo 3(g).

[123] Véase la evolución de esta figura en C. Gutierrez Espada, *De la legítima defensa y el ciberespacio*, cit, pp. 13-22, párrafos 14-17.

[124] "Problèmes actuels du récours à la force en droit international. A. Légitime défense", 10.ª resolución de 27 de octubre de 2007, párrafo 10, i y ii.

sobre el Uso de la Fuerza de la ILA en 2016[125]. Asimismo, en los últimos años, Dinamarca[126], Rusia[127], y especialmente Estados Unidos, este último con mayor claridad y decisión que los demás[128], han respaldado la aplicación de la legítima defensa frente a actores no estatales[129], a la que no se habría opuesto la resolución 2249 (2015) del Consejo de Seguridad, de 20 de noviembre.

**72.** En efecto, mediante esta resolución, y por unanimidad, los miembros del Consejo de Seguridad de Naciones exhortaban a los Estados Miembros de esta organización "que tengan capacidad para hacerlo a que adopten todas las medidas necesarias, de conformidad con el derecho internacional, en particular la Carta de las Naciones Unidas y el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario, sobre el territorio que se encuentra bajo el control del EIIL, también conocido como Daesh, en Siria y el Iraq, redoblen y coordinen sus esfuerzos para prevenir y reprimir los actos terroristas cometidos específicamente por el EIIL […]"[130]. Esta resolución, que no fue adoptada en el marco del Capítulo VII de la Carta de Naciones Unidas, el que permite al Consejo de Seguridad autorizar el uso de la fuerza, y que no menciona la institución de la legítima defensa, es sin embargo considerada como otro refrendo, sino jurídico al menos político, a la lucha internacional contra el Daesh en Siria, y en concreto a las medidas adoptadas por Francia, promotora de la resolución[131].

**73.** A este respecto, como afirman Gutiérrez espada y Cervell Hortal con base en los textos mencionados, así como en otros como el Manifiesto presentado por el Centro de Derecho Internacional de la Universidad Libre de Bruselas en 2016 "no parece razonable (…) que un Estado al que actores no estatales que operan desde el territorio de otro (*incapaz de evitarlo o controlarlo y sin que el Consejo de Seguridad adopte las medidas apropiadas*) atacan con las armas de manera continuada no pueda, bajo la cobertura del Derecho, reaccionar con las armas contra las bases e instalaciones de esos grupos armados"[132]. Esta afirmación es extrapolable al caso de ciberataques cometidos no por grupos armados sino por agentes cibernéticos.

**74.** No obstante, algunos Estados como Brasil han expresado recientemente su oposición a la posibilidad de invocar la legítima defensa frente a actos cometidos por actores no estatales en el ámbito cibernético, habida cuenta precisamente de sus características especiales: "[…]self-defense is only triggered by an armed attack undertaken by or attributable to a State. It is not possible to invoke self-defense as a response to acts by non-State actors, unless they are acting on behalf or under the effective control of a state. This norm becomes even more relevant with cyber operations, where technical, legal and operational challenges to determine attribution might make it impossible to verify potential abuses of the right of self defense, which in turns creates the risk of low impact persistent unilateral military action undermining the collective system established under the Charter."[133]

---

[125] Draft Report on Aggression and the Use of Force (may 2016), Johannerbug Conference [2016], Use of Force, pp. 1-20, p. 10.

[126] Gobierno de Dinamarca, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 Julio de 2023), página 7 (452).

[127] Sesión sobre la investigación del accidente de una aeronave rusa en el Sinaí (17 de noviembre de 2015), http://en.Kremlin.ru/events/president/news/50707. Reproducido en Sentinelle, bulletin 453, 22.

[128] Report on the legal and policy framework guiding the United States' use of military force and related national security operations, The White House, december 2016, pp. 1-61, pp. 9-10.

[129] Sobre la evolución de la práctica estatal y del debate relativo a la invocación de la legítima defensa frente a actores no estatales véase M.J. Cervell Hortal, *La legítima defensa en el derecho internacional contemporáneo: (nuevos tiempos, nuevos actores, nuevos retos)*, cit., pp. 208-244. Véase también, M. J. Cervell Hortal, Sobre la doctrina "unwilling or unable State" (¿podría el fin justificar los medios?), *Revista española de derecho internacional*, Vol. 70, N.º 1, 2018, pp. 77-100, Revista española de derecho internacional, Vol. 70, N.º 1, 2018, pp. 77-100, en pp. 84-87.

[130] Resolución 2249 (2015) de 20 de noviembre de 2015, S/RES/2249 (2015), apartado 5.

[131] Véase en relación con esta resolución, *inter alia*, L. N. González Alonso "¿Daños jurídicos colaterales?: La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional", cit., p. 17.

[132] C. Gutiérrez Espada / M. J. Cervell Hortal, *El Derecho internacional (Corazón y Funciones)* cit*.,* p. 550, párrafo 18 del capítulo 12.

[133] Official compendium of voluntary national contributions on the subject of how international law applies to the use of

**75.** A nuestro juicio, a la vista de la evolución mencionada, y especialmente de las características del ciberespacio –en el que resulta extremadamente difícil, aun deseando hacerlo, controlar las actividades de ciberdelincuentes– se debe permitir responder a ciberataques perpetrados por actores no estatales. Esta opinión viene respaldada además por dos argumentos particularmente relevantes:

(v) la mayoría de expertos del Manual de Tallin 2.0 considera la legítima defensa aplicable a ciberataques de actores no estatales, a pesar de reconocer que la jurisprudencia del Tribunal Internacional de Justicia no avala aún esta tesis[134]; y
(vi) el artículo 42.7 TUE, la denominada cláusula de asistencia mutua de la Unión Europea, que se refiere al artículo 51 de la Carta de Naciones Unidas, ya ha sido aplicado en respuesta a actos llevados a cabo por actores no estatales, en particular cuando Francia lo invocó en noviembre de 2015 en respuesta a los atentados del Daesh en territorio francés.

**76.** En relación con el primer argumento, conviene no obstante ser cauto respecto del valor de la opinión del Manual de Tallinn que, como el propio texto indica, no es un documento oficial sino la opinión de expertos independientes que actúan únicamente a título personal[135]. A este respecto, el Manual de Tallinn no codifica la costumbre internacional ni puede representar la *opinio iuris* de los Estados de nacionalidad de los expertos participantes sino que constituye una expresión de la doctrina de los publicistas de mayor competencia de las distintas naciones, como medio auxiliar para la determinación de las reglas de derecho, con arreglo al artículo 38(d) del Estatuto de la Corte Internacional de Justicia[136].

**77.** Por otro lado, el hecho de que los expertos participantes en el Manual de Tallinn provengan mayoritariamente de Estados con una visión similar del Derecho internacional, como Reino Unido, Estados Unidos, o Australia ha facilitado los avances en la redacción del Manual, y que éste sea muy detallado. Lo anterior contrasta con las dificultades del Grupo de Expertos de Naciones Unidas, mucho más diverso, para precisar principios generales aplicables al ciberespacio. El Manual de Tallin 2.0 puede, en este contexto, resultar útil para marcar el camino hacia el que podría dirigirse la comunidad internacional en el futuro[137].

**78.** En relación con el segundo argumento, el Presidente francés François Hollande invocó el artículo 42.7 TUE tras los atentados de París de 13 de noviembre de 2015 perpetrados por un agente no estatal, el Daesh. Pocos días después, los entonces 27 Estados miembros de la UE restantes respaldaron de manera unánime esta decisión, y se pusieron a disposición de Francia para prestar a este Estado miembro su ayuda y asistencia[138].

---

information and communications technologies by States, UNODA, A/76/136, Agosto de 2021, posición de Brasil, apartado 3 relativo al uso de la fuerza, p. 20.

[134] M. N. Schmitt (editor general*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 71, comentario 19: "A majority of the International Group of Experts concluded that State practice has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, such as terrorist or rebel groups". Para el rechazo a la tesis del TIJ véase el comentario 18: "For its part, the International Court of Justice does not seem to have been prepared to adopt this approach, although it appears that there is a lack of unanimity on the Court in this regard".

[135] Id., p. 2: "It is essential to understand that Tallinn Manual 2.0 is not an official document, but rather the product of two separate endeavours undertaken by groups of independent experts acting solely in their personal capacity".

[136] WH Boothby, "Cyber Capabilities", en WH BOOTHBY, WH (ed.), *New Technologies and the Law in War and Peace*, Cambridge University Press, 2018, p. 89.

[137] Id., p. 133: "The UN GGE process can demonstrate that it is only by including experts from a representative selection of States that an inevitably less detailed, more generalised set of provisions can be achieved. It will then be those that consider that extant law goes further than the GGE experts have acknowledged that will be dissatisfied. Curiously, therefore, neither process generates unanimity of view in the short term. Arguably, it is the kind of process associated with the Tallinn Manuals that will set a more prescriptive legal agenda for the global community to, perhaps gradually, move towards.

[138] Outcome of the Council Meeting: 2426th Council meeting–Foreign Affairs, 6, 14120/15 (Nov. 17), p. 6: "Defence ministers discussed the reaction to the Paris attacks of 13 November 2015. French President François Hollande had invoked article 42(7) of the Treaty on European Union, requesting bilateral aid and assistance from the other EU member states. Ministers

**79.** En efecto, la invocación de la cláusula de defensa mutua permitió a Francia reforzar su interpretación sobre la licitud de la legítima defensa en caso de ataque terrorista por parte de actores no estatales mediante acciones militares fuera de su territorio, en concreto en Siria, un Estado que no ha dado su consentimiento para que se bombardee su territorio –o al menos no a Francia–[139] y que no se puede afirmar que dirija o sea responsable de las actuaciones del Daesh.

**80.** A este respecto, el apoyo, por unanimidad, de los Estados miembros de la Unión Europea a Francia cuando invocó la cláusula de defensa mutua constituye sin duda un aval a la tesis francesa de que había sido víctima de una *agresión armada* por parte del Daesh, y de que tenía derecho a la legítima defensa "de conformidad con el artículo 51 de la Carta de las Naciones Unidas", tal y como estipula el artículo 42(7) TUE. El Parlamento Europeo habría avalado también el empleo del artículo 42(7) TUE en el marco de la legítima defensa de la Carta de Naciones Unidas al afirmar que "una vez que Francia ha invocado la cláusula de defensa mutua, los demás Estados miembros están obligados a prestarle ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas […]"[140]. Sin embargo, Francia ha afirmado rotundamente en fechas más recientes que no considera aceptable la invocación del derecho de legítima defensa frente a actos llevados a cabo por actores no estatales, y que su invocación en el caso del Daesh fue excepcional y condicionada por el carácter de *quasi-Estado* de dicha organización terrorista[141], algo que ya defendió también en 2015[142].

**81.** En suma, a nuestro juicio la legítima defensa resulta también invocable en caso de un ciberataque perpetrado por actores no estatales cuyos graves efectos sean similares a los de un ataque armado.

## III. Conclusiones

**82.** A la luz de las consideraciones anteriores, se pueden formular las siguientes conclusiones:

**83.** *En primer lugar*, en los últimos años, numerosos estudios y posicionamientos oficiales de Estados y organizaciones oficiales como la Unión Europea han avalado la adopción de medidas de autotutela en respuesta a ciberataques con arreglo a Derecho internacional, y precisado las particularidades de su aplicación al ámbito cibernético.

**84.** *En segundo lugar*, en relación con las medidas de retorsión, cabe destacar su posible aplicación en respuesta a operaciones cibernéticas no sólo ilícitas sino también hostiles, así como su posible adopción de manera colectiva por parte de organizaciones internacionales, habiéndose incluido a este respecto como ejemplo el régimen de sanciones frente a actividades cibernéticas malintencionadas vigente en la Unión Europea.

---

expressed their unanimous and full support for France and their readiness to provide all the necessary aid and assistance. In the coming days France will have bilateral discussions with other member states".

[139] Siria podría haber dado su consentimiento a Rusia y a Irán con este fin. Véase a este respecto D. Akande y M. Milanovic, "The Constructive Ambiguity of the Security Council's ISIS Resolution", EJIL: Talk!, Blog of the European Journal of International Law, publicado el 21 de noviembre de 2015.

[140] Resolución del Parlamento Europeo, de 21 de enero de 2016, sobre la cláusula de defensa mutua (artículo 42, apartado 7, del TUE) (2015/3034(RSP)), apartado D.

[141] Ministère des Armées. Republique Française, *Droit International appliqué aux opérations dans le cyberespace*, 9 septembre 2019, cit., p. 9 : "Conformément à la jurisprudence de la CIJ, la France ne reconnaît pas l'extension du droit de légitime défense à des actes perpétrés par des acteurs non-étatiques dont l'action ne serait pas attribuable, directement ou indirectement, à l'État[...]La France a pu invoquer exceptionnellement la légitime défense à l'encontre d'une agression armée perpétrée par un acteur présentant les caractéristiques d'un "quasi-État "comme elle l'a fait pour son intervention en Syrie face au groupe terroriste Daech. Toutefois, ce cas exceptionnel ne saurait constituer l'expression définitive d'une reconnaissance de l'étirement du concept de légitime défense à des actes perpétrés par des acteurs non-étatiques intervenant sans le soutien direct ou indirect d'un État".

[142] Véase a este respecto C. Gutiérrez Espada y M.J. Cervell HortaL, *El Derecho internacional (Corazón y Funciones)* cit., pp. 550-551, párrafo 19 del capítulo 12. Véase también F. ALABRUNE, "Fondaments juridiques de l'intervention militaire française contre Daech en Irak et en Syrie", Révue Générale de Droit International Public, cit. pp. 45-46.

**85.** Además, las medidas de retorsión presentan ciertas ventajas respecto del resto de medidas de autotutela. En particular, al tratarse de medidas lícitas, no están sujetas a los requisitos procesales y sustantivos de las contramedidas, especialmente en lo tocante a la observancia del principio de proporcionalidad y a la ausencia de obligación de notificar al Estado que ha llevado a cabo el acto hostil o ilícito con carácter previo a su adopción, y menos aún de las exigencias de la legítima defensa. Se ajustan, además, mejor a nuestro juicio al espíritu de los principios fundamentales de la Carta de Naciones Unidas como el de soberanía y no intervención, y en particular a la resolución pacífica de controversias.

**86.** *En tercer lugar*, en relación con las contramedidas, resulta especialmente reseñable la reciente discusión sobre la licitud de las contramedidas colectivas en respuesta a ciberataques, motivada especialmente por las posiciones recientemente adoptadas por la Unión Europea, que pueden allanar el camino para el desarrollo progresivo del Derecho internacional en este ámbito,[143] en particular aceptando en algunos casos limitados las contramedidas colectivas adoptadas en respuesta a ciberataques graves y a petición del Estado perjudicado, de conformidad también con lo previsto en el apartado 5 del artículo 3 y el artículo 21 del TUE.

**87.** No obstante, esta posición no parece contar, hasta la fecha, con suficiente práctica estatal y *opinio iuris*, y de hecho se enfrenta a notables limitaciones y riesgos para el Estado, o Estados que decidan adoptarlas. En particular, junto a las dudas relativas a la licitud de las contramedidas colectivas, cabe recordar que incluso en casos de contramedidas bilaterales emprendidas por el Estado lesionado contra el infractor es difícil atribuir con la necesaria precisión la responsabilidad internacional por el hecho internacionalmente ilícito a un Estado. Además, con frecuencia las contramedidas se adoptarían una vez que la actividad cibernética maliciosa ha finalizado, lo que pone en serio entredicho la función instrumental y no punitiva de las mismas. A este respecto, como se ha expuesto, de conformidad con la jurisprudencia internacional, las contramedidas se deben llevar a cabo para obligar o convencer al Estado infractor para que cese la ciberactividad maliciosa, y no posteriormente con carácter punitivo.

**88.** A este respecto, como ha señalado el Gobierno de China públicamente, el recurso a las contramedidas, así como al uso de la fuerza y otras medidas disuasorias debería evitarse en aras de preservar la paz: "Countries should discuss application of international law in the manner conducive to maintain peace, avoid introducing force, deterrence and countermeasures into cyberspace, so as to prevent arms race in cyberspace and reduce risks of confrontation and conflicts."[144] Cabe recordar también, como hizo el grupo de expertos de Naciones Unidas en su informe de 2015, que "En su utilización de las TIC, los Estados deben observar, entre otros principios del derecho internacional, la soberanía de cada Estado, la igualdad soberana, la solución de controversias por medios pacíficos y la no intervención en los asuntos internos de otros Estados"[145]A nuestro juicio, el recurso a las contramedidas en general, y especialmente en el ámbito cibernético, es susceptible de dificultar el cumplimiento del principio de solución de controversias por medios pacíficos previsto en el artículo 2.3 de la Carta de Naciones Unidas, según el cual "Los Miembros de la Organización arreglarán sus controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia."

[143] Sobre la evolución de esta figura y la existencia de argumentos a favor del desarrollo del Derecho internacional en el sentido de su posible aceptación véase P. Roguski, "Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?", Conference paper, Conference: 2020 12th International Conference on Cyber Conflict (CyCon), pp. 1-18, at p. 17.

[144] Declaración del Consejero SUN Lei de la Delegación China en el Debate Temático sobre Seguridad de la Información y Ciberseguridad en la Primera Comisión del 72º Período de Sesiones de la AGNU, (23 Octubre de 2017, disponible en el siguiente enlace: http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/201710/t20171030_8412335.htm

[145] A/70/174, Septuagésimo período de sesiones Tema 93 del programa provisional* Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacionalapartado 28(b), p. 16.

**89.** Finalmente, en relación con la posibilidad de invocar el derecho a la legítima defensa frente a ciberataques que puedan ser considerados como un ataque armado, llevado a cabo o inminente, la opinión de los Estados, así como de la doctrina especializad, avala la licitud de su invocación ante ciberataques graves que causen la muerte o lesión de personas, o incluso la destrucción o malfuncionamiento continuado de infraestructuras críticas, si bien alertan de las dificultades y riesgos que su aplicación conllevaría para la paz y seguridad internacionales. Asimismo, aunque con menos apoyo estatal y doctrinal, nos resulta aceptable su invocación ante ciberataques muy graves llevados a cabo por agentes no estatales siempre que revistan los requisitos de gravedad y efectos exigidos por la jurisprudencia internacional.