Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

VÍCTOR LUIS GUTIÉRREZ CASTILLO*

AGRESIÓN Y NUEVOS ESCENARIOS DE CONFLICTO: ANÁLISIS A LA LUZ DEL *IUS CONTRA BELLUM* CONTEMPORÁNEO

1.- *Introducción*

El 14 de diciembre de 1973, tras 24 años de negociación, se adoptó la Resolución 3314 (XXIX) de 1974 de la Asamblea General de las Naciones Unidas denominada «Definición de la agresión». Dicha Resolución representó un equilibrio transaccional[1] entre las potencias existentes en aquel momento, sirviendo de guía al Consejo General de Naciones Unidas para calificar los comportamientos y hechos acaecidos en la práctica internacional de los Estados. En su preámbulo ya se advierte el esfuerzo que supuso alcanzar el citado consenso, así como la voluntad de poner en marcha medidas preventivas y asistenciales en relación con los Estados víctimas de agresión. Su redacción al día de hoy, no está exenta de críticas, debido, entre otras razones, al encorsetamiento de su redacción, que, inevitablemente, limita su alcance[2]. Tal como está planteada la definición, se podría afirmar que en el concepto de "agresión" solo encajarían las acciones directas llevadas a cabo por actores exclusivamente estatales que ejercen un uso de la fuerza, como la que ha sufrido Ucrania por parte de Rusia.

* Profesor titular de Derecho Público y Relaciones Internacionales, Universidad de Jaén.
[1] Expresión utilizada de *Twenty-ninth Session of the General Assembly, Sixth Committee*, 15 October 1974, *Report of the Special Committee on the Question of Defining Agression* (A/9619 and Corr. 1), Declaración del Sr. Petrella, en L.M. GIORGI, *Estancados en la guerra fría: el concepto de la agresión*, en *Visión Conjunta*, 2009, p. 40 ss.
[2] *Ibid.* p. 42.

Y es que, el ataque armado llevado a cabo por este país constituye, a todas luces, una violación de la prohibición del uso de la fuerza del artículo 2.4 de la Carta de las Naciones Unidas. Esta agresión infringe, además el derecho de Ucrania al respeto a su integridad territorial y a su independencia. Constituye, por tanto, un ataque a los propósitos de la ONU sobre el mantenimiento de la paz (art. 1) y a otros principios esenciales del ordenamiento jurídico internacional, como la obligación que tienen todos los Estados de resolver las controversias por medios pacíficos (art. 2.3) y la prohibición de la intervención en los asuntos internos de otros Estados (Resolución 2625/XXV de la Asamblea General de las Naciones Unidas)[3]. Este tipo de agresión en pleno 2022 ha sorprendido, entre otras razones, por las formas tradicionales (e incluso atemporal) de ejecución (invasión terrestre militar…), que contrasta con la evolución de la sociedad internacional contemporánea (interdependiente, heterogénea, mutable…) en la que la intervención física parece haber pasado a un segundo plano.

Y es que, qué duda cabe, las relaciones internacionales han cambiado en las últimas décadas, estando condicionadas por un mundo cada vez más digitalizado, donde las nuevas armas y las tecnologías cobran un gran protagonismo. En este contexto, el escenario en el que se plantean los conflictos también evoluciona. Nos encontramos ante escenarios etéreos, intangibles e incluso invisibles (como el ciberespacio) en el que actores no estatales operan en concurrencia (y competencia) con los Estados. Partiendo de esta premisa merece la pena reflexionar sobre la necesaria interpretación evolutiva que precisan las normas que conforman el *ius contra bellum* contemporáneo con el fin de dar una respuesta a los ataques que tienen lugar en estos nuevos escenarios de conflicto.

2.- *El artículo 2 (4) de la Carta de Naciones Unidas: piedra angular del* ius contra bellum *contemporáneo*

Si por la condena inequívoca/tajante del recurso a la guerra, el Pacto Briand-Kellogg[4] supone la transición del *jus ad bellum* al *jus contra bellum*[5], no cabe duda de que el artículo 2(4) de la Carta de las Naciones Unidas constituye el elemento principal del nuevo sistema normativo del recurso al uso de la fuerza[6], en virtud del cual, los Estados deben abstenerse «…de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la

[3] Afirmación extraída de la Declaración de los miembros de la AEPDIRI sobre la agresión rusa en Ucrania, que compartimos plenamente, y que puede consultarse en https://www.aepdiri.org/index.php/declaracion-ucrania [última consulta 3/4/2022].

[4] También es conocido como Pacto de París, se trata de un tratado internacional firmado el 27 de agosto de 1928 en la capital francesa a iniciativa Aristide Briand, Ministro de Asuntos Exteriores de Francia y del Secretario de Estado de los EEUU, Frank B. Kellogg por el cual los Estados signatarios se comprometían a no usar la guerra como mecanismo para la solución de las controversias internacionales. Mediante este acuerdo ambos países se comprometían a garantizar una paz internacional duradera mediante la renuncia de la guerra como instrumento para resolver los conflictos de política exterior, simultáneamente se decidió establecer un tribunal de arbitraje, auspiciado por la Sociedad de Naciones, el cual debía decidir sobre todas las disputas entre los países. Aunque el Pacto fue concebido en inicio como un tratado bilateral entre los Estados Unidos de América y Francia, pronto recibió la adhesión de las principales potencias del momento, siendo suscrito al día siguiente por 15 Estados más y, posteriormente, por sesenta y tres Estados, entre los que se encontraba la URSS. Dicho acuerdo es considerado el precedente inmediato del artículo 2.4 de la Carta de las Naciones Unidas, en el que se consagra con carácter general la prohibición del uso de la fuerza.

[5] Y. DINSTEIN, *War, aggression and self-defence*, Cambridge, 2005, p. 83.

[6] Sentencia de la Corte Internacional de Justicia de 19 de diciembre de 2005, *Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c Ouganda)*, *CIJ Recueil*, 2005, par. 148.

independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas»[7]. De hecho, dicho Pacto al tiempo que estableció la obligación de solución pacífica de las controversias (artículo 2), declaró, en su artículo 1, como hecho antijurídico el recurso a la guerra como modo de solución de las controversias internacionales o instrumento de política nacional: «las Altas Partes Contratantes declaran solemnemente en nombre de sus respectivos pueblos, que condenan recurrir a la Guerra para el arreglo de las diferencias internacionales y renuncian a ella como instrumento de política nacional en sus relaciones mutuas»[8].

La prohibición contra la amenaza o el uso de la fuerza es una norma internacional consuetudinaria y convencional de *jus cogens*[9]. En virtud del artículo 103[10] de la Carta, la prohibición contenida en el artículo 2(4) se impone sobre cualquier otra obligación internacional contraída por parte de un Estado miembro de Naciones Unidas[11]. Esta norma se completa por el principio consuetudinario de la no intervención. Ahora bien, aunque presente una apariencia simple en sus disposiciones, el artículo 2 de la Carta ha dado lugar a numerosas discusiones tanto por su contenido como por su alcance. De hecho, uno de los mayores debates que se plantea en la práctica es el relativo al tipo de fuerza que se prohíbe: ¿se trata exclusivamente de la fuerza militar o también de la prohibición de otros medios que puedan constreñir a un Estado económica, política o ideológicamente?[12].

Sobre la base de los trabajos preparatorios de la Conferencia de San Francisco, una buena parte de la doctrina ha considerado que la prohibición del uso de la fuerza enunciada en la Carta de Naciones Unidas, se refiere a la fuerza militar[13]. Conforme a esta interpretación la prohibición del uso de la fuerza en las relaciones internacionales, implicaría la prohibición tanto de amenazas al recurso de la fuerza militar como al ejercicio de acciones militares[14]. En este sentido, varias Resoluciones de la Asamblea General de Naciones Unidas, como la Resoluciones 2625[15], también han sido utilizadas para interpretar el citado artículo. Estos textos han permitido determinar la existencia de una *opinio juris* en cuanto a su carácter consuetudinario, así como al carácter inderogable de la prohibición del empleo de las fuerzas en las relaciones internacionales, apoyándose en la idea de que, mientras el artículo 2(4) se

---

[7] Puede consultarse el texto de la Carta en línea, en concreto en https://www.un.org/es/about-us/un-charter/full-text [última consulta 3/2/2022].

[8] El texto está disponible en http://www.admin.ch/ch/f/rs/i1/0.193.311.fr.pdf [última consulta 3/2/2022].

[9] Para un estudio de las normas que conforman el *ius cogens*, véase F. QUISQUE REMÓN, *Las normas de ius cogens: ausencia de catálogo*, en *Anuario Español de Derecho Internacional*, 2012, p. 143 ss. Para un estudio del tema véase C. DÍAZ BARRADO, *El uso de la fuerza en las relaciones internacionales*, Ministerio de Defensa, Madrid, 1989.

[10] El texto de dicho artículo afirma literalmente que «En caso de conflicto entre las obligaciones contraídas por los Miembros de las Naciones Unidas en virtud de la presente Carta y sus obligaciones contraídas en virtud de cualquier otro convenio internacional, prevalecerán las obligaciones impuestas por la presente Carta».

[11] O. SCHACHTER, *In Defense of International Rules on the Use of Force*, en *The University of Chicago Law Review*, 1986, p. 113 ss.

[12] O. CORTEN, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law (French Studies in International Law)*, Oxford, 2012, p. 50; Y. DINSTEIN, *War, aggression and self-defence,* Cambridge, 2005, p. 86.

[13] Y. DINSTEIN, cit., p. 86 y A. RANDELZHOFER, *Article 2(4)*, en B. SIMMA et al. (Coords.), *The Charter of the United Nations, A Commentary,* Oxford, 2002, p. 117.

[14] S. FORD, *Legal processes of change: article 2(4) and the Vienna Convention on the Law of Treaties*, en *Journal Confl & Sec*, 1999, pp. 78-79.

[15] Resolución 2625 (XXV), de 24 de octubre de 1970, *Declaración sobre los principios de Derecho Internacional referente a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas*. El texto está disponible en línea en https://www.un.org/es/documents/ag/res/25/ares25.htm [última consulta 3/2/2022].

refiere a prohibición bajo la forma de fuerza armada, el principio de no-intervención se aplica a «otras formas de coacción»[16].

Por lo que se refiere al aspecto espacial, el citado artículo 2(4) de la Carta de Naciones Unidas recoge una prohibición amplia del uso de la fuerza. Al no existir ninguna precisión terminológica, cabe entender que dicha prohibición no solo podría ser aplicable al espacio terrestre, aéreo y marino[17], sino también a otros escenarios en los que queda afectada la soberanía y seguridad de los Estados. Piénsese, por ejemplo, en el ciberespacio[18]. En este sentido el citado artículo no solo tiene en cuenta la integridad territorial o la independencia política del Estado, sino que comprende todos los usos de la fuerza incompatibles con los propósitos de Naciones Unidas. De esta última referencia podría concluirse que el artículo 2(4) incluye todo recurso a la fuerza, al margen de su impacto o gravedad[19], pudiendo comprender acciones inéditas en el momento de su redacción como las que causadas por los ciberataques estatales[20].

En otro orden de ideas, como puso de manifiesto la CIJ en el asunto de las actividades militares y paramilitares en Nicaragua y contra Nicaragua, los actos que suponen una violación del principio consuetudinario de no-intervención y que impliquen, bajo una forma directa o indirecta, el empleo de la fuerza en las relaciones internacionales, constituyen una violación de dicho principio, quedando, por tanto, prohibidos. En este sentido, la Corte, determinó de forma expresa que «le principe de non-intervention se réfère à l'obligation internationale qu'a l'État de ne pas intervenir physiquement et matériellement, par ses forces armées ou des agents publics, sur le territoire d'un autre État sans l'accord de ce dernier»[21]. Es por ello que toda intervención ilícita en los asuntos de otro Estado y acompañado del recurso a la fuerza constituye una violación de la prohibición del recurso al uso de la fuerza en las relaciones internacionales[22]. Ahora bien, en este sentido, la Corte ha precisado que «le simple envoi de fonds (aux forces rebelles d'un autre pays), s'il constitue à coup sûr un acte d'intervention dans les affaires intérieures (de celui-ci) (…) ne représente pas en lui-même un emploi de la force»[23]. Podría concluirse pues, que todo empleo de la fuerza supone una intervención, pero no todas las intervenciones implican una violación del artículo 2(4): es necesario que el medio empleado por el Estado contra otro Estado, conlleve el uso de la fuerza para que podamos hablar de recurso ilícito.

---

16 *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c Etats-Unis d'Amérique), fond*, 1986, en *Recueil des Cours de l' Académie du droit international de La Haye*, 14, par. 19; A. RANDELZHOFER, *Article 2(4)*, cit., p. 112, par. 19 y p. 118; G. ARANGIO-RUIZ, *The Normative Role of the General Assembly of the United Nations and the Declaration of Principles of Friendly Relations*, en *Recueil des Cours de l' Académie du droit international de La Haye*, 1972, par. 99-100, pp. 599-601.

17 G. ARANGIO-RUIZ, *The Normative Role of the General Assembly of the United Nations*, cit., par. 57, p. 534.

18 Véase M. N. SCHMITT (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, 2013, pp. 10 y 42; W.G. SHARP, *Cyberspace and the use of force, Falls Church (VA),* Virginia, 1999, pp. 33-34.

19 A. RANDELZHOFER, *Article 2(4)*, cit., par. 16 en la p. 117; T. RUYS, «*Armed Attack* » *and Article 51 of the UN Charter,* New York, , 2010, p. 55.

20 K. ZIOLKOWSKI, *General Principles of International Law as Applicable in Cyberspace*, en K. ZIOLKOWSKI (dir.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn 2013, pp. 143-144 y 172-175.

21 J-P. PANCRACIO & E.-M. PETON, *Un mutant juridique, ¿l'agression internationale?*, *Cahiers de l'IRSEM,* nº. 7, 2011, p. 67.

22 Sentencia de la Corte Internacional de Justicia de 27 de junio de 1986 *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond*, *CIJ Recueil*, 1986, par. 205.

23 *Ibidem*., par. 228.

El empleo ilícito de la fuerza puede revestir «formes (…) plus graves (…) (celles qui constituent une agression armée) et d'autres modalités moins brutales» en las que se requiere de organización, fomento, asistencia, participación o tolerancia de actos subversivos o terroristas sobre el territorio de otro Estado por su parte[24]. Estas diferentes modalidades pueden ejercerse de forma directa o indirecta. Mientras que el artículo 2(4) de la Carta no realiza distinción alguna entre el empleo directo e indirecto del uso de la fuerza[25], la Corte Internacional de Justicia (en adelante, CIJ) sí que lo hace, al afirmar que «Cet élément de contrainte, constitutif de l'intervention prohibée et formant son essence même, est particulièrement évident dans le cas d'une intervention utilisant la force, soit sous la forme directe d'une action militaire, soit sous celle, indirecte, du soutien á des activités armées subversives ou terroristes à l'intérieur d'un autre État»[26]. La Corte llega a esta conclusión basándose en los párrafos 8 y 9 de la Resolución 2625, los cuales expresan, en palabras de la Corte, el derecho internacional consuetudinario en materia de uso de fuerza indirecta.

3.- *Nuevos escenarios de conflicto ergo nuevos desafíos para la paz y seguridad internacionales*

Uno de los nuevos escenarios de conflicto en la sociedad internacional contemporánea es el que llevan a cabo los Estados en el ciberespacio, ámbito de información que se encuentra implementado dentro de los ordenadores y de las redes digitales de todo el mundo. Este espacio, a diferencia de los tradicionales, es virtual, inexistente desde el punto de vista físico y en él operan sujetos, públicos y privados, que generan interactividad con diversos propósitos. El mundo digital existe sobre las redes y se supone sinónimo de universalidad, ubicuidad e inmediatez. Ahora bien, al igual que no podemos desvincularnos del mundo físico, tampoco podemos hacerlo del mundo digital. Las fronteras que las comunidades políticas y Estados han levantado a lo largo de la historia se resisten igualmente a caer en el espacio digital, condicionante de la soberanía de los Estados. En la última década han sido numerosas las ocasiones en las que algunos gobiernos han denunciado ser víctimas de ciberataques sin haber podido exigir responsabilidades internacionales por ello. Atendiendo a los criterios definidos por la CIJ y empleados en derecho internacional público[27] para atribuir la responsabilidad de un hecho internacionalmente ilícito a un Estado, puede ser muy difícil, por no decir imposible, imputar un ciberataque a un Estado al día de hoy. De hecho, el artículo 8 del Proyecto de artículos de Responsabilidad de Estados por

[24] *Ibidem*., par. 191.
[25] M. SCHWEBEL, *Agression, intervention and self-defence in modern international law*, en *Recueil des Cours de l' Académie du droit international de La Haye*, 1972, p. 458.
[26] *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, cit., par. 205. Véase también *Déclaration sur le renforcement de l'efficacité du principe de l'abstention du recours à la menace ou à l'emploi de la force dans les relations internationales,* Resolución AG 42/22, Doc off AG NU, 42 sess, Doc NU A/42/766 (1987), par. 2.
[27] La Comisión de Derecho Internacional también ha confirmado la validez de la teoría del control efectivo (véase Proyecto de Artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos, adoptado por la CDI en su 53 período de sesiones (A/56/10) y anexado por la Asamblea General en su Resolución 56/83, de 12 de diciembre de 2001. Puede verse en el *Anuario de la Comisión de Derecho Internacional* 2001, vol. II, parte 2, Nueva York, UN, 2001, p. 31 (Doc. UN A/CN.4/SER.A/2001/Add.1 (Part. 2), art. 8, pp. 110-112.

hechos internacionalmente ilícitos[28] no es de gran ayuda a este respecto. Piénsese que no es sencillo para un Estado víctima de un ciberataque, probar que ha sido objeto de intrusiones concretas y directas por otro Estado en el ciberespacio. Tampoco es fácil demostrar que detrás de la intervención de piratas informáticos se encuentra otro Estado ejerciendo un control directo y efectivo. El acceso a los elementos de prueba es un gran obstáculo para la determinación de la responsabilidad de un ciberataque, ya que recae sobre la víctima el peso de probar la existencia de una consecución lógica de hechos atribuibles a otro Estado. En el caso del *Estrecho de Corfú*, la CIJ reconoció la admisibilidad de presunciones de hecho y de pruebas circunstanciales presentadas por el Estado víctima, considerando éstas «comme particulièrement probants quand ils s´appuient sur une série de faits qui s´enchaînent et qui conduisent logiquement à une même conclusion»[29]. En el caso de acciones realizadas en el ciberespacio, la complejidad de la prueba aumenta, debido al medio en el que nos encontramos. Qué duda cabe, los autores de un ciberataque (ya sean agentes estatales o particulares) buscan la clandestinidad para alcanzar sus objetivos. La existencia de estos ataques no trasciende a un gran público más allá de referencias en la prensa, mientras que su veracidad nunca es confirmada por parte de los Estados implicados. La práctica reciente nos puede servir de referencia al respecto.

El ciberataque sufrido por Georgia en el año 2008, es un ejemplo de lo expuesto[30]. La coincidencia temporal entre el bloqueo de sus servicios informáticos y el inicio de una ofensiva militar terrestre rusa, hace pensar que los piratas informáticos debieron ser conscientes previamente de los planes de la armada rusa[31] y que su actuación se llevó a cabo

---

[28] Asamblea General A/RES/56/83, 28 de enero de 2002, *Responsabilidad del Estado por hechos internacionalmente ilícitos*.

[29] Sentencia de la Corte Internacional de Justicia de 9 abril de 1949, *Affaire du détroit de Corfou. (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord c. Albanie), CIJ Recueil*, 1949, p. 18.

[30] Debido a diferencias político-militares entre este país y Rusia, a causa de la situación de Abjasia y Osetia del Sur, aquel país fue víctima de ataques informáticos. Del 19 al 20 de julio de 2008, el site de internet del presidente de Georgia sufrió un ataque masivo, que contenía el siguiente mensaje propagandístico: «Win+love+in+Russia»; el incidente no tuvo mayor alcance hasta el 7 de agosto, fecha oficial del comienzo del conflicto armado internacional con la Federación rusa. Apenas unas horas antes del inicio de la invasión del territorio georgiano por la armada rusa, el tráfico de internet del país quedó bloqueado. Georgia se encontró totalmente aislada del resto del mundo: ni las personas que vivían en Georgia, ni las que se encontraban en el exterior podían recibir información alguna del desarrollo del conflicto militar. El 8 de agosto, *Tiblisi* acusó a Moscú de haber utilizado piratas informáticos para ejecutar ciberataques contra los sites de internet georgianos, gubernamentales y de información, Rusia negó las acusaciones. A partir del 9 de agosto de 2008, varios grupos rusos con motivaciones aparentemente patrióticas crearon sites y foros de discusión para organizar y coordinar los ataques por saturación contra los sites georgianos. Se reclutaron piratas informáticos, gracias a la elaboración y distribución on-line de instrucciones sobre el *modus operandi* con la finalidad de provocar el bloqueo del servicio de dichos sites. Entre las organizaciones rusas que participaron en los ciberataques, se constató que varias direcciones IP habían sido utilizadas por la *Russian Business Network* (RBN), una organización rusa, disuelta en el momento de los ataques que ya había estado implicada en casos de cibercriminalidad. Las autoridades georgianas procedieron a realojar sus sites en los servidores de otros países como EEUU, Estonia y Polonia. A pesar de estas medidas, durante el conflicto armado entre Rusia y Georgia, los sites de internet georgianos permanecieron fuera de servicio, sufriendo ataques de desconfiguración, acompañados de mensajes que contenían propaganda política pro-rusa. Para más información. N. SHACHTMAN, *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It*, in *Wired Danger Room Magazine*, 11 March 2009, en línea http://www.wired.com/dangerroom/2009/03/georgia-blames/ [última consulta 3/2/2022]

[31] US. CYBER CONSEQUENCES UNIT, *Special report*, *Overview of the Cyber Campaign Against Georgia*, 2009, en línea https://indianstrategicknowledgeonline.com/web/US-CCU-Georgia-Cyber-Campaign-Overview.pdf [última consulta 3/2/2022].

para proporcionar una ventaja militar a ésta última[32]. Sin embargo, fue imposible demostrar tal extremo al no existir prueba irrefutable que vincularse a este país.

Esta ausencia de flexibilidad de las normas internacionales a la hora de determinar la responsabilidad internacional de hechos ilícitos a Estados permite a los países, autores o cómplices de ciberataques, escudarse tras una "negación plausible". Es por ello que, con el fin de impedir que los Estados continúen lanzando o patrocinando ciberataques con total impunidad, ciertos autores han propuesto la noción de *responsabilidad imputada*[33]. En virtud de esta propuesta, se podrá imputar a un Estado los ciberataques cometidos por servidores situados en su territorio. Este nuevo marco de análisis abandona un modelo de responsabilidad internacional centrado en la atribución de un Estado de un acto determinado[34], hacia un modelo de responsabilidad indirecta basado en el deber de respetar las obligaciones internacionales en materia de prevención de un hecho ilícito internacional[35].

Para los defensores de esta noción, el derecho internacional público impone a los Estados, un deber de vigilancia estatal por el que se exige que se provea de medios necesarios para prevenir que su territorio sea utilizado con el fin de perjudicar los derechos de otro Estado soberano[36]. La CIJ ha confirmado el carácter *erga omnes* de este tipo obligaciones, como resultado del deber estatal de precaución, indicando que la responsabilidad de un Estado puede verse comprometida cuando cometa graves omisiones en sus labores de prevención de un hecho internacionalmente ilícito[37]. Por tanto, siguiendo este planteamiento si un Estado tuviera conocimiento de que su territorio es utilizado para cometer actividades cibernéticas maliciosas contra otro Estado[38] y no hiciera nada al respecto, podría ser considerado responsable internacionalmente debido a la falta de prevención ante la violación de los derechos del Estado víctima.

Ahora bien, sin negar la virtualidad de este planteamiento, no podemos dejar de reconocer la dificultad de hacerla efectiva en la práctica, ya que la existencia del deber de vigilancia no implica, necesariamente, que un Estado sea responsable de todo acto de violencia transfronterizo cometido desde su territorio. Y es que, en materia de ciberataques, sería muy forzado determinar la responsabilidad de un Estado por la simple razón de que los ataques sean lanzados desde equipos informáticos o servidores situados en su territorio o desde sus infraestructuras gubernamentales. Situación distinta, según la doctrina, podría darse si un Estado permitiera, con total conocimiento de causa, que una ciberinfraestructura estatal fuese utilizada en tiempos de paz por actores privados para llevar a cabo acciones

---

[32] *Remarks H.E. Mr Mikheil Saakashvili, President of Georgia*, 63e sesión de la Asamblea General de las Naciones Unidas, alocución presentada en Nueva York, 23 de septiembre 2008, en línea https://www.un.org/en/ga/63/generaldebate/georgia.shtml [última consulta 3/2/2022]

[33] Entre otros autores, destaca J. KULESZA, *State responsability for cyber-attacks on international peace and security*, en *Polish Yearbook of International Law*, 2009, p. 139 ss.

[34] Para un estudio con mayor profundidad sobre este tema véase M. AZNAR GÓMEZ, *Responsabilidad internacional del Estado y acción del Consejo de Seguridad de las Naciones Unidas*, Ministerio de Asuntos Exteriores, Madrid, 2000.

[35] K. ZIOLKOWSKI, Ius ad bellum *in Cyberespace- Some Thoughts on the «Schmitt-Criteria» for Use of Force,* in C. CZOSSECK, R. OTTIS & K. ZIOLKOWSKI, (dir.), *2012 4th International Conference on Cyber Conflict (CyCon 2012)*, Tallinn, 2012, p. 306.

[36] *Affaire de la Fonderie de Trail (États-Unis c. Canada), Sentence arbitrale du 11 mars 1941 (Décision finale),* RSA, p. 1905 ss.

[37] *Affaire du détroit de Corfou. Arreêt du 9 avril 1949 (fond), CIJ Recueil*, 1949, cit., p. 22.

[38] W.G. SHARP, W.G. *Cyberspace*, cit., p. 112.

hostiles contra otro Estado[39]. Un Estado podría entonces ver su responsabilidad comprometida no por el uso de la fuerza en sí mismo (al no poder imputársele ésta) sino por su apoyo[40] a la misma, lo que podría suponer una violación de los principios de la prohibición del recurso a la fuerza y de la prohibición de no intervención[41].

Tanto la jurisprudencia internacional como la práctica de los Estados, sostienen que la simple pasividad por parte de un Estado ante la presencia de grupos armados en su territorio, no puede considerarse como un hecho que le implique en las actividades ilícitas del grupo. Dada esta circunstancia, podría proponerse que la responsabilidad imputada a un Estado fuera analizada desde la óptica de la aplicación efectiva de la obligación del control de los medios. En este contexto, a la hora de determinar la responsabilidad de un ciberataque se podrían tener en cuenta, a efectos de evaluación, los siguientes elementos: la multiplicación de ataques informáticos similares provenientes del Estado sospechoso, las medidas tomadas con el fin de evitar y sancionar este tipo de infracciones y la asistencia que proporciona el Estado a otros Estados víctimas de ciberataques cometidos por personas que se encuentran en su territorio. De este modo, sólo se desplazará la carga de la prueba del Estado víctima al Estado que no haya respetado sus obligaciones. Esta circunstancia permitirá a la víctima no sólo beneficiarse de una práctica de la prueba más flexible conforme a las pruebas circunstanciales, sino que también permitirá evitar los fraudes de control territorial llevados a cabo por otros Estados[42].

Los ciberataques estatales plantean otras cuestiones relativas al recurso a la fuerza no cinética por parte de un Estado y sobre todo, los actos de violencia contra un Estado cuyas consecuencias no son materiales. En la línea del artículo 2(4) de la Carta que prohíbe el recurso a la fuerza armada, el modelo elemental de análisis de empleo de la fuerza se fundamenta sobre el tipo de instrumento coercitivo utilizado. Aparentemente, los delegados de la Conferencia de San Francisco sólo tuvieron en cuenta la fuerza militar llevada a cabo mediante las armas de guerra conocidas hasta el momento: un ciberataque no podría haber constituido entonces una violación del artículo 2(4) según este marco de análisis, debido a que se trata de un recurso a la fuerza no cinegético. Esta aproximación es criticable, a nuestro juicio, ya que no tiene en cuenta la aparición de nuevas armas no cinegéticas tales como las radiológicas o biológicas.

El hecho de que un ordenador haya sido utilizado como medio principal de ejecución de un ataque contra un Estado, no debería ser pertinente a la hora de calificar el acto en sí a la luz del citado artículo. Y es que la CIJ ha declarado que: «la Charte n'interdit ni permet

---

39 N. MELZER, *Cyberwafare and International Law*, in *UNIDIR Resources*, 2011, en línea https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [última consulta 3/2/2022].

40 N. MELZER, *Cyberwafare,* cit., p. 11.

41 El apoyo de un Estado a las acciones internacionalmente ilícitas de agentes no estatales viola los principios de no recurso a la fuerza y de no intervención. Así lo afirma la CIJ en *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c Etats-Unis d'Amérique), fond*, cit., pars. 110 y 242. En este orden de ideas, el hecho de que un Estado se provea de piratas informáticos, de herramientas informáticas especialmente concebidas para cometer una acción ofensiva contra otro Estado, supone un uso de la fuerza que puede ser calificado como agresión indirecta, si dicho acto ofensivo cometido por el grupo de piratas es una actividad "suficientemente grave" y siempre que pueda probarse implicación sustancial del Estado.

42 De esta forma se evitará que los ciberataques estatales se cometan gracias a la pasividad de un Estado. Véase CH. C. DEMSHAK & P. DOMBROWSKI, *Rise of a Cybered Westphalian Age*, en *Strategic Studies Quarterly*, 2011, pp. 32-35.

expressément l'emploi d´aucune arme particulière»[43]. Por tanto, sea directo o indirecto, la comunidad internacional está más interesada en las consecuencias del empleo del uso de la fuerza que en los medios utilizados para ejercer dicha fuerza. La fuerza armada, por ejemplo, no se define por el empleo o la liberación de energía cinética, sino por la naturaleza de las consecuencias directas y previsibles, especialmente en el caso de pérdidas humanas y de destrucción física.

En 1998, Schmitt enunció una serie de factores basados en la distinción entre la fuerza armada y otras formas de coacción, como las presiones diplomáticas, económicas y políticas, con el objetivo de calificar los ataques informáticos, en relación con el artículo 2(4) de la Carta[44]. Diez años más tarde, habiendo perfeccionado sus criterios, Schmitt propone un nuevo marco de análisis para ayudar a los Estados a calificar las actividades informáticas de las que son víctimas, con independencia de su origen. Según este planteamiento, que ha sido utilizado por los autores del *Manual Tallinn*, un ciberataque constituye un empleo de la fuerza si las dimensiones y sus efectos son paralelos a aquellos que se habrían obtenido tras el empleo de armas cinéticas[45].

Si comparamos las consecuencias de los ciberataques con las de los ataques no cibernéticos, este ejercicio nos permite hacer uso restrictivo de la palabra "fuerza" del artículo 2(4) para responder a los últimos avances tecnológicos sin poner en tela de juicio el marco actual del *jus contra bellum*[46]. De todos modos, es importante subrayar que los defensores de esta interpretación no parten de una distinción en relación con la naturaleza informática o cinética de los medios de ataque utilizados, sino que se centran en los efectos ocasionados. Conforme a la misma, sólo aquellos ciberataques que pueden producir efectos cinéticos se considerarían como "uso de la fuerza". Ahora bien, dado que la mayoría de los ciberataques son más perturbadores que destructores y éstos no causan (hasta el momento) resultados materiales, sería erróneo tener en cuenta solamente los efectos que resulten de destrucciones físicas. No somos partidarios de la aplicación de este criterio de calificación para estos casos, ya que adolece de un carácter excesivamente restrictivo. Si siguiéramos este criterio, quedarían excluidos del "uso de la fuerza" los ciberataques que paralizaran las infraestructuras básicas de un país, así como los ataques informáticos destinados a bloquear los servicios de *sites* que proporcionan servicios esenciales a la población[47]. Por este motivo, ciertos autores, a los que nos sumamos, proponen un método de análisis de los ciberataques

---

[43] Opinión consultiva de la Corte Internacional de Justicia de 8 de julio de 1996, *Avis consultatif concernant la licéité de la menace ou de l'emploi d'armes nucléaires (Requête pour avis consultatif présentée par l'Assemblée générale)*, CIJ *Recueil* 1996, par. 35 y 36.

[44] M. N. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, en *Columbia Journal of Transnational Law*, 1998-1999, pp. 914-915.

[45] El título completo es *Tallinn Manual on the International Law Applicable to Cyber Warfare*. No se trata de un documento oficial por tanto no refleja la doctrina de la OTAN, ni la postura de las organizaciones o Estados representados, ni la del propio centro CCD COE. En este manual se identifica por un lado el derecho internacional que puede aplicarse a la ciberguerra y, por otro, se establecen 95 normas que deberían regir este tipo de conflictos. Aborda temas como la soberanía, la responsabilidad de los estados, el *jus ad bellum*, el *jus in bello, el derecho* humanitario internacional y la ley de neutralidad, entre otros. El manual está disponible en formato electrónico en la página web. Para más información véase M. N. SCHMITT (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013, p. 45. Para un interesante estudio del mismo véase A.P. VELÁZQUEZ ORTIZ, "El Manual de Tallin: estudio y crítica de los principales conceptos y normas", en S. ALDA MEJÍAS & S. ANGEL SANTANO (aut.) *La seguridad, un concepto amplio y dinámico: V Jornadas de estudios de seguridad*, 2013, pp. 607-633

[46] M.N. SCHMITT, *Computer Network*, cit., p. 915.

[47] En este sentido véase N. MELZER, *Cyberwafare,* cit.

estatales basado en la naturaleza del objetivo perseguido y que defiende la imputación de una responsabilidad estricta a los autores de los ciberataques[48]. Según esta corriente, cuanto más esencial sea el objetivo del ciberataque para el funcionamiento del Estado, mayor será la probabilidad de considerarlo una violación del artículo 2(4). Partiendo de esta premisa, podría afirmarse que todo ciberataque contra las infraestructuras críticas de un país es un empleo ilícito de la fuerza, sin importar el nivel de gravedad del ataque[49]. El enfoque de la responsabilidad estricta se encuentra sujeto a una cierta subjetividad, debido a que los Estados disponen de una discreción total a la hora de definir qué servicios considera como esenciales o una infraestructura crítica.

En este sentido, no podemos olvidar que a los efectos que en las normas internacionales relativas al uso de la fuerza puede tener el denominado "umbral de gravedad" que se encuentra en la definición del crimen de agresión en el artículo 8 bis del Estatuto de Roma. Haciendo hincapié en la gravedad como característica definitoria de la agresión, algunos autores, como L. Pezzano, se preguntan si el umbral del artículo 8 bis introduce una nueva categoría dentro de los usos ilícitos de la fuerza[50].

4.- *¿Nuevas excepciones al principio de abstención del recurso al uso de la fuerza?*

Como reconoce la doctrina, la prohibición contenida en el artículo 2(4) «ne s´occupe ni des raisons matérielles de ce recours à la forcé, ni de l'existence d'une cause juste»[51]. Si la apariencia consuetudinaria de la prohibición del uso de la fuerza se encuentra «non conditionné par les dispositions relatives à la sécurité collective»[52], su componente condicional sufre algunas excepciones, como son los artículos 39 y 51 de la Carta. La primera excepción es la posibilidad para el Consejo de Seguridad de Naciones Unidas de recurrir a la fuerza aplicando el artículo 39, así como la de «(…) ejercer, por medio de fuerzas aéreas, navales o terrestres, la acción que sea necesaria para mantener o restablecer la paz y la seguridad internacionales» (art. 42), en el marco de su capítulo VII. La segunda excepción al uso ilícito de la fuerza en relaciones internacionales es el derecho a la legítima defensa previsto en el artículo 51 de la Carta. A su estudio y análisis nos ocuparemos en los siguientes epígrafes[53].

Conforme a los artículos 12 y 24 de la Carta, el Consejo de Seguridad de Naciones Unidas tiene la responsabilidad de mantener la paz y la seguridad internacional. El artículo 39 le capacita para adoptar recomendaciones o medidas de conformidad con los artículos 41 y 42 al efecto de mantener o restablecer la paz y la seguridad internacionales, si constata la

---

48 C. DEMSHAK & P. DOMBROWSKI, *Rise of a Cybered Westphalian Age*, in *Strategic Studies Quarterly*, 2011, pp. 32-35.

49 L. PEZZANO, *El umbral de gravedad en el crimen de agresión: ¿una nueva categoría en los usos ilícitos de la fuerza?*, en *Anuario Iberoamericano De Derecho Internacional Penal*, 2021, p. 86 ss.

50 *Ibídem*.

51 H. WEHBERG, *L'interdiction du recours à la force. Le principe et les problèmes qui se posent*, en *Recueil des Cours de l'Académie du droit international de la Haye*, 1951, p. 64.

52 *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, cit., par. 188.

53 Para un estudio en mayor profundidad véase C. DÍAZ BARRADO, *La prohibición del uso de la fuerza y sus excepciones: Balance a los cincuenta años de Naciones Unidas*, en F. M. MARIÑO MENÉNDEZ (coord.), *Balance y perspectivas de Naciones Unidas en el cincuentenario de su creación*, Universidad Carlos III de Madrid-Boletín Oficial del Estado, Madrid, 1996, p. 141 ss.

existencia de una amenaza para la paz, el quebrantamiento de la paz o un acto de agresión. La determinación de un acto de agresión es un prerrequisito del ejercicio de las prerrogativas que reconoce el artículo 39 al Consejo de Seguridad. Al igual que en el caso del artículo 2(4) donde se omite cualquier definición de "fuerza", tampoco se incluye en el texto convencional lo que se entiende por "agresión", siendo sólo el Consejo de seguridad, conforme al artículo 39, el competente para decidir si el artículo 2(4) ha sido objeto de una violación. La calificación de situación es una evaluación política y no jurídica. El Consejo de Seguridad dispone de una discreción total y aparentemente ilimitada en cuanto a la constatación de una situación de agresión. La discrecionalidad de la que dispone en virtud de dicho artículo 39 de la Carta se ilustra por su práctica. En efecto, el Consejo de Seguridad ha sido reticente a la hora de calificar como "agresiones" el empleo unilateral del uso de la fuerza en algunas ocasiones, obviando con ello la aplicación del citado artículo 39 en sus resoluciones. Una vez calificada la situación *de facto*, el Consejo de Seguridad podrá autorizar a los Estados a recurrir a la fuerza armada para poner fin a «amenaza a la paz, quebrantamiento de la paz o acto de agresión» (Artículo 39 de la Carta de Naciones Unidas)[54] en aquellos casos en los que las medidas no coercitivas del artículo 41 no hayan sido efectivas. Por tanto, podríamos afirmar que mientras que el artículo 39 de la Carta concede plenos poderes en materia de coerción al Consejo de Seguridad en casos de "actos de agresión", el artículo 51 subordina el recurso al uso de la fuerza al concepto más restrictivo de "agresión armada"[55].

El recurso al uso de la fuerza como respuesta a una "agresión armada" está permitido en la medida que se informe inmediatamente al Consejo de Seguridad y se cumplan una serie de condiciones: a) la existencia una agresión armada llevada a cabo por un Estado; b) la posibilidad del Estado víctima de recurrir a las acciones reconocidas por el derecho consagrado en el artículo 51 de la Carta; c) el recurso a la fuerza como respuesta a una agresión armada efectivamente sobrevenida y d) el respeto a los principios de necesidad y de proporcionalidad. Ahora bien, en palabras de la CIJ, aunque no se defina en la Carta, «l'accord paraît aujourd'hui général sur la nature des actes pouvant être considérés comme constitutifs d'une agression armée»[56]. Cabe recordar, en este sentido, que existen dos elementos importantes en una agresión armada: la violación de la integridad territorial o soberana de otro Estado y el empleo de medios militares o paramilitares. La noción de "agresión armada" del artículo 51 es mucho más restrictiva que la del artículo 39[57]. Todo acto de agresión armado es una agresión, pero toda agresión no tiene por qué suponer necesariamente una agresión armada. Asimismo, al igual que, todo empleo unilateral e ilícito de la fuerza no constituye una agresión armada, toda agresión armada sí constituye una violación del artículo 2(4). Las diferencias entre la versión francesa e inglesa del artículo 51, que tratan respectivamente de "*agression armée*" y de "*armed attack"* (en lugar de *armed aggression*)

---

54 En este sentido, cabe señalar que el Consejo de Seguridad, de las tres calificaciones desencadenantes del sistema de seguridad colectiva (amenaza para la paz, quebrantamiento de la paz y acto de agresión), normalmente utiliza la de "amenaza para la paz". Para un estudio sobre este tema véase P. ANDRÉS SÁENZ DE SANTA MARÍA, *Las normas relativas al uso de la fuerza: la seguridad colectiva y la legítima defensa en el contexto de la reforma de las Naciones Unidas*, en C. GARCÍA/A. RODRIGO (ed.), *La seguridad comprometida. Nuevos desafíos, amenazas y conflictos armados*, Tecnos, 2008, p. 113 ss.; R. BERMEJO GARCÍA, *Cuestiones actuales referentes al uso de la fuerza en el Derecho Internacional*, en *Anuario de Derecho Internacional*, 1999, p. 3 ss.

55 H. WEHBERG, *L'interdiction*, cit., p. 64.

56 *Actividades militares y paramilitares en Nicaragua,* cit., par. 176.

57 A. RANDELZHOFER, *Article 51*, en B. SIMMA et al. (dir.), *The Charter of the United Nations, A Commentary*, Oxford, 2002, pp. 794-5.

ponen de relieve esta circunstancia, así como la falta de consenso en la Conferencia de San Francisco por a la hora de conformar los límites de este concepto.

5.- *Algunas reflexiones en torno a la interpretación del concepto de agresión: reglas tradicionales en constante mutación*

Conforme la Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas, la agresión es definida como «el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado o en cualquier otra forma incompatible con la Carta de las Naciones Unidas»[58] y que no está justificado por la legítima defensa o por ningún otro medio de defensa reconocido por el derecho internacional. La condena de la agresión es un elemento importante en las relaciones internacionales desde inicios del siglo XX, como demuestra el Pacto de la Sociedad de Naciones[59] y el Estatuto del Tribunal Militar de Núremberg. En 1974, siguiendo la corriente francesa de interpretación del artículo 51 de la Carta que trata sobre la *agression armée* y no de *attaque armée*, la Asamblea General elaboró una definición sobre la agresión, como anexo a la Resolución 3314 (XXIV).

Durante los trabajos del Comité especial sobre la elaboración de dicha Resolución, la mayor parte de los delegados alcanzaron un acuerdo a la hora de reconocer una relación de gravedad entre los términos "fuerza", "agresión" y "agresión armada" utilizados respectivamente en los artículos 2(4), 39 y 51 de la Carta. Con la finalidad de llegar a un consenso, se convino que el término "agresión" contenido en la Resolución tuviera el mismo sentido que el dispuesto en el artículo 39 de la Carta. Según la Resolución, para que un acto hostil sea considerado como un acto de agresión, debe haberse cometido por un Estado, constituir un empleo de la fuerza armada y ser "de una gravedad suficiente", evaluada *a posteriori* por el Consejo de Seguridad[60].

A pesar de esta circunstancia, no podemos olvidar que la citada Resolución 3324 (XXIX) de 1974 carece de fuerza obligatoria, constituyendo en la práctica una herramienta interpretativa (no vinculante) utilizada ante el Consejo de Seguridad de Naciones Unidas para el ejercicio de sus "atribuciones políticas". De hecho, como ya pusimos de manifiesto, el Consejo de Seguridad en raras ocasiones ha calificado actos de agresión y, cuando lo ha hecho, ha evitado cualquier referencia expresa a la citada Resolución. Circunstancia que

---

[58] *Definición de agresión*, Doc. off AG UN, cit., art. 1.

[59] El Pacto de Sociedad de Naciones ciertas guerras fueron consideradas lícitas, entre las que cabe citar la guerra de agresión, regulada en el artículo 10, el cual reza así: «Los Miembros de la Sociedad se comprometen a respetar y a mantener contra toda agresión exterior la integridad territorial y la independencia política presente de todos los Miembros de la Sociedad. En caso de agresión, de amenaza o de peligro de agresión, el Consejo determinará los medios para asegurar el cumplimiento de esta obligación». Esta disposición dio lugar a una controversia doctrinal: para unos, era obvio que esta disposición imponía a los Miembros una auténtica obligación jurídica, dejando claro que la guerra de agresión estaba expresamente prohibida por el Pacto (cfr. W. FOMARNICKI, *La définition de l'agresseur dans le droit internacional moderne*, en *RCADI*, 1949, p. 22 ss.). Informacón obtenida de la publicación R. BERMEJO, *El uso de la fuerza, la sociedad de Naciones y el Pacto Briand-Kellogg*, en Y. GAMARRA CHOPO / C. R. FERNÁNDEZ LIESA (coord.) *Los orígenes del Derecho internacional contemporáneo: estudios comemorativos del Centenario de la Primera Guerra Mundia*l, 2015, p. 217 ss.

[60] Sobre esta cuestión véase L. PEZZANO, *El umbral de gravedad en el crimen de agresión ¿una nueva categoría en los usos ilícitos de la fuerza?*, en *Anuario Iberoamericano de Derecho Internacional Penal*, 2016, p. 86 ss.

puede explicarse más por el carácter político del Consejo de Seguridad que por las eventuales insuficiencias normativas de esta disposición.

5.1.- *Sobre la responsabilidad internacional por el acto de agresión*

Partiendo de lo dispuesto en la Resolución 3314 y en el Proyecto de artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos de 2001[61], todo acto de agresión y, por tanto, todo acto constitutivo de una violación del artículo 2(4) de la Carta, debe ser susceptible de atribución a un Estado, determinándose su responsabilidad en virtud de las reglas jurídicas de la responsabilidad estatal internacional. En este sentido, en derecho internacional los comportamientos y acciones de órganos estatales constituyen hechos atribuibles al Estado al que éstos pertenecen, ya ejerzan funciones legislativas, ejecutivas, judiciales o de otra índole y cualquiera que sea su posición en la organización interna, tanto si pertenece al gobierno central como a una división territorial[62].

Existen, de todos modos, excepciones a este principio de base que permiten atribuir a un Estado actos cometidos por órganos no estatales, en función del control que éste pueda ejercer sobre los autores de los hechos, de las instrucciones o de las directivas otorgadas por los órganos de Estado a actores no estatales o del reconocimiento y de la adopción de los actos concernientes a los Estados. En este sentido, la CIJ ha contribuido a determinar con su jurisprudencia (sirva como ejemplo, el asunto de acciones militares en Nicaragua y contra Nicaragua), el grado de control que debe ejercer un Estado sobre personas o entidades privadas para que el comportamiento de estas últimas pueda ser imputado. La Corte distingue entre grupos de personas que, sin tener el estatuto oficial de órganos de Estado, pueden ser considerados actores que operan en su nombre. En este sentido, el comportamiento de grupos de individuos que dependen desde un punto de vista logístico y financiero de un Estado extranjero y actúan bajo sus instrucciones, será responsabilidad de dicho Estado. Sin embargo, en el caso de que la dependencia sea únicamente económica o financiera, no se puede atribuir una imputación automática de sus hechos. En estos casos se entiende que dichos grupos siguen siendo independientes, razón por la que la CIJ propone la aplicación de un test de control efectivo. Este test exige una dependencia completa y absoluta de los autores del comportamiento internacional ilícito frente al Estado al que se quiere imputar el hecho alegado. La relación de dependencia puede quedar demostrada de dos formas distintas: si los actos alegados se efectúan por orden directa o instrucciones precisas del Estado; o en ausencia de elementos que permitan establecer la determinación de la responsabilidad directamente, se denote una implicación estatal substancial en la comisión del acto de agresión descrito. Aunque el derecho internacional no define una regla concreta en relación con la prueba del uso ilícito de la fuerza, la CIJ estime que las «allégations formulées contre un Etat qui comprennent des accusations d'une exceptionnelle gravité doivent être prouvées

---

[61] Para un interesante estudio del proyecto de artículos véase C. GUTIÉRREZ ESPADA, *¿Actio popularis en derecho internacional? (El proyecto definitivo de artículos sobre la responsabilidad internacional del estado de agosto de 2001*, en ZLATA DRNAS DE CLÉMENT (coord..), *Estudios de derecho internacional en homenaje al profesor Ernesto J. Rey Caro*, Córdoba, 2002, p. 549 ss.

[62] Comisión de Derecho Internacional, *Informe de la Comisión a la Asamblea General sobre la labor realizada en su 53º periodo de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto 2001)*, A/56/10*, Nueva York, 2001 (*Proyecto de artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos con sus comentarios*, 10-405).

par des éléments ayant pleine forcé probante»[63]. Existe un tercer mecanismo de atribución de responsabilidad por las acciones de agentes privados, definido en el artículo 11 del Proyecto de artículos y que permite imputar a un acto que no le fuese atribuido en el momento de su comisión, pero que haya reconocido y adoptado como suyo por el mismo.

Ahora bien, la determinación de responsabilidad por una agresión debe ser probada. El mero hecho de constatar una agresión no implica automáticamente la existencia de una responsabilidad, para ello es preciso determinar su atribución. Y es que, mientras que en general la calificación de una situación por parte del Consejo de Seguridad en virtud del artículo 39 no comporta la responsabilidad internacional del Estado al que se presume agresor, el artículo 5(2) de la Resolución 3314 (XXIX) prevé que «la agresión origina responsabilidad internacional».

5.2.- *Aspectos controvertidos en relación con el elemento material y subjetivo: la violación prima facie del artículo 2(4) y la existencia de la intencionalidad*

El *actus reus (*elemento objetivo de un hecho ilícito*)* del acto de agresión se describe en el artículo 1 de la Resolución 3314 (XXIX), en la misma línea que el artículo 2(4) de la Carta, aunque con algunas diferencias. Y es que, mientras que el empleo ilícito de la fuerza armada está expresamente condenado en dicha Resolución, ésta omite cualquier condena a la amenaza de la fuerza. Circunstancia ésta que abre numerosos interrogantes. La fuerza no debe emplearse contra la integridad territorial y la independencia política de "otro Estado", pero ¿y en el caso de la soberanía del mismo? ¿afecta también la prohibición de la fuera a cuestiones relacionadas exclusivamente con la soberanía de los Estados? Las respuestas a estos interrogantes pueden generar dudas, ya que el recurso a la fuerza armada está prohibido en casos de incompatibilidad con "la Carta de Naciones Unidas", pero no con "los propósitos de Naciones Unidas". Una lista no exhaustiva de actos constitutivos de agresión se enuncia en el art. 3 de la Resolución 3314 (XXIX). Se trata de una relación (no cerrada) de actos concretos y concisos, redactados en un contexto bien diferente al actual. En este sentido, se citan, entre otros, la invasión, la ocupación, el bombardeo, el bloqueo naval, el ataque de las fuerzas armadas, así como cualquier ataque de la marina o de la aviación civil por parte de las tropas militares de otro Estado. Relación ésta que no es exhaustiva y que puede ampliarse atendiendo a las prerrogativas del Consejo de Seguridad reconocidas en el artículo 39 de la Carta y que reconoce la propia Resolución en su artículo 4.

El artículo 2 de la Resolución 3314 (XXIX) contiene una presunción refutable que especifica que el primer acto de violencia cometido por un Estado, que viole el artículo 2(4) de la Carta, deberá ser considerado como una prueba *prima facie* de un acto de agresión, susceptible de evaluación posterior de otras circunstancias relativas a la situación por parte del Consejo de Seguridad. La disposición incluye una cláusula de mínimos, que exige alcanzar un nivel de gravedad suficiente para que los actos de hostilidad puedan ser calificados como agresión. Esta reserva permite evitar no solamente las conclusiones precipitadas de agresión, sino también limitar el ejercicio del derecho a la legítima defensa prevista en el artículo 51 de la Carta.

[63] Sentencia de la Corte Internacional de Justicia de 26 de febrero de 2007, *Affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (Croatie c. Serbie)*, CIJ *Recueil* 2007.

Aunque no se especifique nada al respecto en la citada Resolución, la jurisprudencia de la CIJ y la práctica de los Estados demuestran que la presencia de una *mens rea* (intención criminal) es uno de los elementos del acto de agresión. Circunstancia ésta particularmente importante para la evaluación de los actos hostiles de menor envergadura, debido a que permite probar, sin ninguna duda, la intención maliciosa del agresor. Para los casos de ataques a gran escala, la intención se deduce a menudo del acto material del atacante a menos que no existan hechos probados que demuestren lo contrario. Sea cual sea el tipo de acto estudiado, la *mens rea* (intención criminal) debe ser evaluada en función del contexto global de ésta.

6.- *Los nuevos escenarios de conflicto: análisis a la luz del ius contra bellum contemporáneo*

Atendiendo al contexto histórico de la Resolución 3314 (XXIX), así como sus fundamentos jurídicos, no cabe duda de que los elementos constitutivos de "agresión" sólo podían conformarse por referencia a la Carta, la cual menciona en sus artículos 1 y 39 las amenazas a la Paz, el quebrantamiento de la Paz y los actos de agresión, y, en el artículo 51, el ataque armado. De esta idea puede desprenderse que el concepto de agresión abarca varios tipos de situaciones, entre las que el ataque armado es la más peligrosa. El hecho de que la Carta no mencione la "agresión indirecta" no debería haber supuesto obstáculo para una distinción en la propia Resolución entre la agresión directa y la agresión indirecta. Y es que, tanto la una como la otra constituyen una amenaza para la paz internacional y la diferencia entre ambas guardan similitud con la que existe entre el "ataque armado" y el "quebrantamiento de la paz". Cabe señalar, asimismo, que el párrafo 4 del artículo 2 de la Carta no define la agresión, solo hace referencia a los comportamientos prohibidos de los que la agresión no es más que un ejemplo. El artículo 39 establece una progresión en la gravedad de estos comportamientos en la que el grado más alto corresponde a la agresión. La omisión en la citada Resolución de cualquier referencia a la agresión indirecta, refleja, como ya hemos apuntado, el contexto histórico en el que se consensuó la esperada definición. No obstante, la referencia a la "agresión indirecta" la hemos tenido en cuenta en diferentes foros internacionales. Así, por ejemplo, la encontramos en la jurisprudencia de la CIJ y en normas convencionales de carácter regional. En este sentido la CIJ ha declarado que el artículo 3(g) de la Resolución representa la norma consuetudinaria internacional de la prohibición de la agresión indirecta. Partiendo de su interpretación podría decirse que estaríamos ante este tipo de agresión en casos de «actes d'ingérence extérieure n'impliquant pas l'emploi directe du manifeste de la forcé armée»[64], que revistan una gravedad similar a la de la agresión directa.

Ahora bien, las referencias que encontramos tanto en la jurisprudencia internacional como en la Resolución de la agresión indirecta parecen restrictivas en su alcance, ya que parecen circunscribirla al uso de la fuerza y a acción de actores estatales. En este orden de ideas, parecen contemplarse dos tipos de agresión indirecta en el artículo 3(g) de la Resolución 3314 (XXIX): los actos de agresión directamente atribuibles al Estado agresor y aquéllos donde la implicación sustancial del agresor debe ser probada. La característica principal de la agresión indirecta es que el Estado agresor, sin haber cometido actos hostiles

[64] E. AKOTO, *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public? (part 2)*, en *Ottawa Law Review*, fall 2015, pp. 199.

de forma directa, cuenta con un intermediario, que puede estar situado incluso en un tercer país y que no es un agente *de jure o de facto* de este Estado, sino que cuenta con su propio jefe, de ahí la problemática de la prueba de implicación sustancial de dicho Estado. En este sentido, el enfoque de la CIJ sigue la misma línea de actuación que la praxis internacional, que revela que la agresión se realiza de forma progresiva y consiste, casi siempre, en la organización, asistencia, incitación, financiación, estímulo o tolerancia «d'activités subversives ou terroristes dirigées contre un autre État».

A pesar de las omisiones referidas, la agresión indirecta sí parece haber sido tenida en cuenta en otros foros internacionales a hora de configurar lo que podría llamarse un *ius contra bellum* regional. Piénsese, por ejemplo, en el artículo 28 de la Carta de la Organización de Estados Americanos (OEA), la cual menciona la agresión en términos genéricos (emplea e el término amplio de «toda agresión»), posibilitando con ello un mayor alcance a este concepto, incluyendo así tanto la agresión directa como la indirecta. En este sentido, el citado artículo afirma que «toda agresión de un Estado contra la integridad o la inviolabilidad del territorio o contra la soberanía o la independencia política de un Estado americano, será considerada como un acto de agresión contra los demás Estados americanos»[65]. Asimismo, el artículo 6 del Tratado interamericano de Asistencia recíproca (TIAR)[66] brinda otro ejemplo al referirse a la "agresión que no sea ataque armado".

Teniendo en cuenta el marco normativo (convencional y consuetudinario) que conforman el *ius contra bellum* contemporáneo, encontramos serias dificultades para calificar los ataques que pueden producirse en nuevos escenarios, como en el ciberespacio y que no solo suponen una amenaza para la paz, sino que también afectan a la seguridad y soberanía de los Estados[67]. Piénsese, por ejemplo, en los ciberataques estatales, ofensivas llevadas a cabo en el ciberespacio, que comprometen la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, modificación, degradación o destrucción

[65] Puede consultarse el texto completo de la Carta de la OEA en https://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-41_carta_OEA.asp [última consulta 3/2/2022].

[66] El TIAR es un tratado firmado en el seno de la OEA que busca la cooperación en materia de seguridad y defensa. Dicho tratado establece dos principios fundamentales: primero, condena el uso de la fuerza para la resolución de conflictos entre los países firmantes y, segundo, asegura la defensa mutua en caso de que alguno de los Estados partícipes sea agredido. El TIAR fue firmado en 1947 como resultado de la doctrina Monroe y en plena Guerra Fría —la Organización para el Tratado del Atlántico Norte sería constituida sólo dos años después, en 1949—. Mediante este tratado, los Estados miembros se comprometen a consensuar sus acciones para hacer frente a otros Estados que agredan a alguno de los integrantes del pacto. Para ello, el propio documento reconoce diversas medidas que se pueden llevar a cabo como respuesta a los ataques, desde las sanciones económicas hasta la ruptura de relaciones diplomáticas. Incluso se podría llegar a autorizar el uso de la fuerza siempre y cuando se cumpliera con lo permitido por el derecho internacional: que se trate de actos de defensa colectiva. Por otro lado, el tratado interamericano no solo permite consensuar sanciones ante agresiones, sino también ante «cualquier otro hecho o situación que pueda poner en peligro la paz de América» lo que puede incluir multitud de escenarios. En esos casos, se convoca el Órgano de Consulta para que decida las medidas a tomar ante la amenaza existente. En la actualidad, forman parte del Pacto Argentina, Bahamas, Brasil, Chile, Colombia, Costa Rica, El Salvador, Guatemala, Haití, Honduras, Panamá, Paraguay, Perú, República Dominicana, Trinidad y Tobago, Estados Unidos y Uruguay. Por otra parte, Venezuela, Bolivia, Ecuador y Nicaragua abandonaron el tratado en 2012. Para más información véase R. MANSILLA BLANCO, *Do TIAR á OTAS: dinámicas da arquitectura de seguridade en América do Sur*, en *Tempo Exterior,* 2009, p. 103 ss.

[67] J. DOMÍNGUEZ BASCOY, *Ciberguerra y derecho. El "*ius ad bellum*" y "el* ius in bello*" en el ciberespacio*, en *Revista Española de Derecho Militar*, 2013, p. 151 ss.

de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan[68]. La mayoría de actividades informáticas de naturaleza maliciosa tienen lugar en tiempo de Paz[69]. Si los conflictos de baja intensidad eran los métodos privilegiados de grandes potencias durante la guerra fría, en nuestros días, los ciberataques estatales pueden constituir un instrumento perfecto para alcanzar los mismos objetivos sorteando el marco jurídico internacional de prohibición del uso de la fuerza. De hecho, el gobierno de los EEUU ya ha declarado que podrían llevar a cabo acciones militares a título de legítima defensa o de represalias en respuesta a los ciberataques supuestamente encargados por otros Estados. Circunstancias éstas que plantean nuevas dudas sobre la calificación de estas acciones en tiempos de paz[70].

Los ciberataques estatales podrían ser calificados, a tenor de lo expuesto hasta el momento, como agresiones indirectas, ya que manifiestan diversas formas de injerencia y/o menoscabo en la soberanía del Estado que los padece. Piénsese, por ejemplo, en la intervención maliciosa realizada en el ciberespacio para provocar la saturación del sistema informático de un país, afectando gravemente su funcionamiento (el caso de Estonia[71] y Georgia) para acceder a información confidencial o provocar su mal funcionamiento (caso *stuxnet*[72]). Con el fin de garantizar el respeto del marco normativo actual del *jus contra bellum*,

---

[68] Definición contenida en la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas de España, en *Boletín Oficial del Ministerio de Defensa*, de 26 de febrero de 2013.

[69] K. ZIOLKOWSKI (dir.), *Peacetime Regime for State Activities in Ciberspace. International Law, International Relations and Diplomacy*, Tallinn, 2013, p. 15. Puede accederse al documento en línea https://www.ilsa.org/Jessup/Jessup16/Batch%202/Peacetime-Regime.pdf [última consulta 3/2/2022].

[70] En este sentido hay que tener en cuenta lo dispuesto en la *Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas*, Res. AG 2625, Doc. Off AGNU, 25 ses, sup nº. 28, Doc UN A/5217 (1970), preámbulo, párr. 7.

[71] Uno de los casos de ciberataques más conocidos, es el sufrido por Estonia el 26 de abril de 2007. El gobierno de este país trasladó un monumento de la Segunda Guerra Mundial dedicado a la memoria de la armada roja, del centro de la ciudad de Tallin hacia un cementerio militar en el extrarradio. La comunidad rusa, que representa en torno al 30% del total del país, llevó a cabo varias protestas contra esta decisión a través de manifestaciones populares y declaraciones públicas. Tras las manifestaciones y durante más de tres semanas, se bloquearon los servicios de varios *sites* de internet gubernamentales, así como medios de comunicación, bancos, operadores de telefonía móvil y servicios de urgencia. Las interferencias informáticas llegaron a su punto álgido el 9 de mayo, fecha en la que se conmemora el fin de la Segunda Guerra Mundial en Rusia. Los ataques se acompañaron de actividades de desconfiguración de *sites* de internet y envío masivo de emails. Si bien estos servicios no resultaron en destrucción material alguna, sin duda, perturbaron de manera grave la vida cotidiana de los ciudadanos (usuarios) del país, privándoles del acceso a servicios esenciales en línea. A pesar de que los ataques se realizaron desde ordenadores ubicados en 178 países distintos, el gobierno estonio sostuvo desde un primer momento que Moscú había estado detrás de los ataques de los que había sido víctima. Para más información K.K. LIIS VIHUL ENEKEN TIKK, *International cyber incidents: legal considerations*, Tallinn, 2010, p. 23.

[72] *Stuxnet* es un "gusano" (o código dañino) que forma parte de un programa secreto de los EEUU titulado *Olympic Games* y que, presuntamente, tenía como objetivo el sabotaje al programa nuclear iraní. Al parecer, dicho programa fue autorizado en 2006 por el presidente G. BUSH y mantenido por el presidente B. OBAMA tras su elección en 2009. Concebido específicamente para dañar las máquinas centrifugadoras del programa nuclear iraní modificando su velocidad de rotación. Debido a un error de manipulación, *Stuxnet* fue lanzado a internet, siendo así como se reveló su existencia a la comunidad internacional. En noviembre de 2010, las autoridades iraníes anunciaron que las máquinas centrifugadoras de su programa nuclear habían sido infectadas por un virus informático y acusaron a EEUU de ser el origen del ataque. Tras una serie de entrevistas realizadas a lo largo de 18 meses un periodista americano reveló que *Stuxnet* habría sido creado por los servicios de inteligencia americanos e israelíes. Hasta el momento ningún país ha reivindicado su autoría. Para más información véase E. PÉREZ & A. ENTOUS, FBI *Probes Leaks on Iran Cyberattack,* en *The Wall Street Journal*, 5 June 2012 en línea: http://online.wsj.com/article/SB10001424052702303506404577448563517340188.html [última consulta

los ciberataques deberían ser analizados a partir de un modelo disuasivo, que permitiera identificar cualquier violación sutil de una violación del principio de no agresión (aunque no del empleo de la fuerza) y debería minimizar los riesgos de calificación abusiva de los actos de agresión.

Con el fin de determinar si un ciberataque estatal constituye un acto de agresión según la Resolución, el Estado víctima deberá convencer al Consejo de Seguridad, no sólo de la implicación de otro Estado en la ejecución u organización del ataque informático, sino también del hecho de que el ciberataque, o sus consecuencias constituyan, un empleo ilícito de la fuerza de intensidad suficiente como para recibir tal calificación. Conforme a la práctica del Consejo de Seguridad, el Estado víctima también tendrá que demostrar que el ciberataque perseguía un fin agresivo.

7.- *Nuevas formas de agresión indirecta en la sociedad internacional contemporánea*

La mayoría de los ciberataques son llevados a cabo por personas o entidades privadas, representando una forma de agresión indirecta, cuyos efectos son similares a los de una agresión directa. Habiendo sido elaborada la Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas[73] con el fin de servir de guía interpretativa al Consejo de Seguridad de Naciones Unidas, entendemos que el examen de los ciberataques estatales a la luz de la misma, debería realizarse comparando los diferentes tipos de ataques informáticos y sus consecuencias, según las disposiciones del artículo 3 de dicha Resolución.

En este orden de ideas, podría afirmarse que, por analogía, la infección de las infraestructuras esenciales de un Estado por *softwares* maliciosos puede considerarse, en función de sus efectos, supuestos encuadrables en los artículos 3(a), 3(b), y 3 (d) de la Resolución 3314 (XXIX). De forma similar, en el caso de lo dispuesto en el artículo 3(f), el hecho de que un Estado permita que sus infraestructuras informáticas sean utilizadas para cometer ciberataques informáticos contra otro Estado podrá considerarse como un acto de agresión, siempre que pueda probarse que dicho Estado era conocedor de este hecho[74]. El artículo 3(c) de la Definición presenta el bloqueo naval como un acto de agresión. Ciertos autores ya han resaltado las similares existencias entre un bloqueo de servicios y un bloqueo naval[75]. Del mismo modo que, el bloqueo naval viola el derecho de acceso de un Estado a la alta mar, los ataques por saturación[76] violan el derecho de acceso de un Estado al

3/2/2022]; D.E. SANGER, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, en *The New York Time*s, 01 June 2012 en línea: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-ofcyberattacks-against-iran.html?pagewanted=1&_r=2&hp&&pagewanted=al [última consulta 3/2/2022].

[73] Doc. off AG UN, cit., art. 1.

[74] *Affaire du détroit de Corfou*, cit., par. 18 y 22.

[75] S. HERZOG, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, in *Journal of Strategic Security*, 2011, p. 54.

[76] Este tipo de ataques tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Existen diversas formas de ataque: por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo. Durante un ataque de este tipo se envían simultáneamente múltiples solicitudes desde distintos puntos de la red. La intensidad de este «fuego cruzado» compromete la estabilidad, y, en ocasiones, la disponibilidad del servicio.

ciberespacio[77]. Una distinción importante entre los ciberataques y el bloqueo naval, reside en el hecho de que el bloqueo obstaculiza los intercambios de bienes físicos entre Estados mientras que el bloqueo de servicios afecta al flujo de información. Si en el pasado, el bloqueo de información no afectaba a la población, la situación ha cambiado en el siglo XXI. Y es que, debido a la creciente dependencia de internet de las sociedades modernas, un bloqueo de servicios de una cierta amplitud puede constituir una agresión atendiendo a los factores (tamaño, dependencia de internet…) en el que se encuentre el país víctima de un ataque por saturación. Buena prueba de ello es el caso de Estonia. Este pequeño país europeo era (y es) muy dependiente de Internet. Debido a su baja densidad de población y a la remota ubicación de algunas de sus comunidades, Estonia prestaba la mayor parte de los servicios administrativos a través de internet. De hecho, era apodado como "E-stonia". En 2007, en el momento de los ataques cibernéticos, la práctica totalidad del territorio estonio tenía acceso a internet, realizándose, la práctica totalidad de las operaciones bancarias vía on-line. La tasa de penetración de la telefonía móvil de los habitantes que realizaba sus declaraciones de impuestos usando el ciberespacio se acercaba al 90%. Circunstancias todas ellas que explica su alta vulnerabilidad y que las autoridades se sintieran víctimas de un acto de agresión[78].

Se puede establecer otra comparación entre los incidentes fronterizos descritos por la CIJ[79] y las intrusiones informáticas. Las intrusiones informáticas son operaciones de ciber-exploración a través de las cuales los atacantes analizan las redes informáticas de la víctima con el fin de poner a prueba sus parámetros de defensa[80] y soberanía. Finalidad que también podría ser atribuible a un Estado cuando traspasa las fronteras de otro. Sin embargo, la determinación de la intencionalidad en uno y otro caso es bien diferente: mientras que las intenciones de los atacantes pueden discernirse fácilmente en el caso de un incidente fronterizo, no ocurre lo mismo con las intrusiones informáticas.

Por otra parte, en el caso de que, con motivo de una intrusión informática, se instalara de forma subrepticia un software malicioso de acceso diferido en el sistema de otro Estado, podríamos encontrarnos ante una operación asimilable a la de instalación de minas. Obviamente, los efectos serían distintos, pero la intencionalidad de dañar o perjudicar a otro Estado sería la misma. En este sentido, la CIJ ha declarado que «(l)e minage d'un seul navire de guerre (peut, éventuellement) suffire à justifier qu'il soit fait usage du "droit naturel" de légitime défense»[81]. Como resultado de las complejidades inherentes a los ciberataques, sería prudente considerar también, como una violación *a prima facie* del artículo 2(4) de la Carta, toda intrusión electrónica contra las infraestructuras críticas de un Estado. La presunción de hecho sería refutable y estaría condicionada a la satisfacción del criterio de "gravedad suficiente" de la citada Resolución.

---

77 France, Sénat - Session extraordinaire de 2011-2012*, Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense, par M. Jean-Marie BOCKEL, Sénateur,* nº. 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 30.

78 I. TRAYNOR, *Russia accused of unleashing cyberwar to disable Estonia,* in *The Guardian* 17 May 2007 en ligne: Guardian.co.uk http*://w*ww.guardian.co.uk/world/2007/may/*17*/topstories3.russia?mobile-redirect=false [última consulta 3/2/2022].

79 *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci,* cit., par. 195.

80 J. BARKHAM, *Information warfare and international law on the use of force*, in *New York University Journal of International Law* and *Politics*, 2001-2002, p. 93.

81 Sentencia de la Corte Internacional de Justicia de 6 de noviembre de 2003, *Affaires plates-formes pétrolières (République islamique d'Iran c. États-Unis d'Amériq*ue), *CIJ Recueil*, par. 72.

Debido a la clandestinidad de los ataques, es muy difícil apreciar la intencionalidad tras un ciberataque estatal hasta que no se ha llevado a cabo y no se ha investigado qué Estado (o Estados) se han beneficiado del mismo. En el caso del conflicto ruso-georgiano de 2008, hay que admitir que la ofensiva terrestre militar rusa unida a los ciberataques que provocaron el bloqueo de servicios, proporcionó una ventaja militar a Rusia. A pesar de ello, los ciberataques perpetrados no han podido ser considerados "operaciones de carácter militar", aunque, sobre la base de lo expuesto hasta el momento, podría valorarse seriamente su calificación como agresión conforme el artículo 2 de la citada Resolución.

En 2003, en el caso de las *plataformas petrolíferas*, la CIJ examinó la cuestión de "savoir si (une) attaque, prise isolément ou dans le cadre de la «série d'attaques invoquée par (un État), peut être qualifié d'«agression armée» contre (celui-ci)»[82]. Se trata de una aplicación de la teoría de la acumulación de los hechos (*Nadelstichtaktik*[83]) que plantea que varios incidentes menores pueden acumularse con el fin de evaluar si procede el derecho a la legítima defensa[84]. Esta teoría sobre situaciones o ataques consecutivos, puede establecer como parte de un plan global y continuo, varios ataques anteriores de menor amplitud. Aunque no se trate de una norma de derecho internacional y esta teoría haya sido criticada por la doctrina, la acumulación de hechos es una herramienta que sirve para evaluar los ataques llevados a cabo por bandas armadas o grupos no militares. Numerosos autores recomiendan que se considere el análisis de los ciberataques estatales desde esta óptica, con el fin de determinar el carácter hostil de la intención de los autores. En este caso, si se aplica la teoría de la acumulación al caso de los ciberataques, éstos podrían calificarse como recurso ilícito al uso de la fuerza[85].

8.- *Conclusiones*

De acuerdo con lo dispuesto en la Carta de Naciones Unidas una de las funciones que tiene atribuida la Asamblea General de Naciones Unidas es la de realizar recomendaciones. Circunstancia ésta que determina el alcance de la Resolución 3314 (XXIX), carente de fuerza vinculante. En este sentido, si bien el artículo 2.4 de la Carta de Naciones Unidas tiene el mérito de introducir obstáculos a los Estados a la hora de usar la fuerza en el plano internacional, será el Consejo de Seguridad de Naciones Unidas el único órgano legitimado para declarar si una situación internacional es considerada o no una amenaza para la paz, quebrantamiento de la paz o acto de agresión. Todo esto implica que los actos enumerados en el artículo 3 del Anexo I de la Resolución 3314 (XXIX) serán tenidos en cuenta por el Consejo a la hora de valorar qué otros actos o comportamientos constituyen una agresión, de conformidad con las disposiciones de la Carta.

No cabe duda que, *a priori*, la definición de agresión contenida en la citada Resolución refleja la circunstancia histórica que permitió un consenso político en plena guerra fría. De ahí que la referencia expresa al uso de la fuerza armada, deja de lado otras formas de alterar

---

[82] *Affaires plates-formes pétrolières,* cit., par. 64.
[83] Para más información sobre esta doctrina véase YAROSLAV SHIRYAEV, *The Right of Armed Self-Defense in International Law and Self-Defense Arguments Used in the Second Lebanon War*, en *Acta Societatis Martensis*, 2007-2008, p. 80 ss.
[84] V. M. KATTAN, *The use and abuse of self-defense in international law : The Israel-Hezbollah conflict as a case study*, 2007, en línea https://www.papers.ssrn.com/sol3/papers.cfm?abstract-id=994282 [última consulta 3/2/2022].
[85] K. ZIOLKOWSKI, *General principles,* cit., p. 160.

la paz mencionadas en el artículo 39 de la Carta. La definición así presentada parece restrictiva en su alcance, no sólo por dicha referencia, sino por descripción que de los actos constitutivos de agresión hace: actos directos y con la participación de actores exclusivamente estatales. Precisamente a causa de ello, y para sortear los límites de la norma, algunos Estados han desarrollado métodos indirectos y sutiles de enfrentamiento, que han encontrado en el ciberespacio un escenario ideal de aparente impunidad. La dificultad de calificar los actos hostiles en este nuevo espacio reside en el hecho de que muy pocos revisten la forma de uso ilícito de la fuerza, debido al carácter no físico de sus consecuencias.

La realidad de nuestra sociedad internacional contemporánea, condicionada por la digitalización y las nuevas tecnologías, exige una nueva interpretación de los parámetros que conforman los perfiles normativos del *ius contra bellum*. Y es que exigir que los ciberataques produzcan daños o perjuicios físicos a los efectos de considerarlos violación *prima facie*, de conformidad con el artículo 2(4), supone ignorar la necesidad creciente de afrontar este tipo de actividades en la esfera internacional. Analizarlos únicamente desde la óptica de la legítima defensa nos llevaría a calificarlos erróneamente de "incidentes menores", lo que haría alejarnos de la realidad. Piénsese, en este sentido, que la multiplicación de este tipo de ataques implica *de facto* adoptar el inicio de una guerra de desgaste: actos de hostilidad que constituyen una amenaza para la paz y la seguridad internacionales. El amplio margen de apreciación del que dispone el Consejo de Seguridad en esta materia, especialmente en el caso de la determinación de la existencia de un acto de agresión, debería permitirle desarrollar en un futuro criterios propios para determinar nuevas modalidades de agresión indirecta, en concreto la agresión informática. Se debería, a nuestro juicio, utilizar una escala de intensidad adaptada a las nuevas circunstancias partiendo de una interpretación amplia del contenido del *ius contra bellum* contemporáneo, comprensivo del uso ilícito indirecto de la fuerza. Se precisa pues una interpretación evolutiva y viva de las normas que lo conforman.

La Resolución 3314 (XXIX) ha vuelto a despertar interés en nuestros días gracias a la labor de la Asamblea de Estados Parte en el Estatuto de la Corte Penal Internacional, que decidió utilizarla como base para redefinir el crimen de agresión[86]. Si tenemos en cuenta la proliferación de nuevos medios y métodos de guerra no cinéticos, la multiplicación de ataques estatales cometidos por grupos de individuos en estos nuevos escenarios de conflicto y, sobre todo, el contenido del nuevo artículo 8 bis del estatuto de Roma que entró en vigor en enero de 2017, se podría llegar a un cierto consenso internacional en lo concerniente a la calificación jurídica internacional de los ataques cometidos en tiempos de paz en estos nuevos "escenarios de conflicto". Y es que, el texto final de dicho artículo reproduce la definición de agresión de la citada resolución, lo que parece indicar que el contenido de ésta última sigue siendo de actualidad.

[86] Para más información sobre este tema véase C. ESCOBAR HERNÁNDEZ, *Corte Penal Internacional, consejo de seguridad y crimen de agresión*, en F. MARIÑO MENÉNDEZ (ed.), *El derecho internacional en los albores del siglo XXI*, Madrid, 2002, p. 248 ss.; J.L. VALLARTA MARRÓN, *La incorporación del crimen de agresión en el estatuto de la Corte Penal Internacional*, en *Anuario Mexicano de Derecho Internacional*, 2011, p. 435 ss.