Eunomia. Rivista di studi su pace e diritti umani
Eunomia X n.s. (2021), n. 1-2, 83-110
e-ISSN 2280-8949
DOI 10.1285/i22808949a10n1-2p83
http://siba-ese.unisalento.it, © 2021 Università del Salento

VÍCTOR LUIS GUTIÉRREZ CASTILLO

UNIVERSIDAD DE JAÉN

Los ciberataques estatales en tiempos de paz: análisis de su calificación jurídica a la luz del Derecho internacional *

Abstract: *At present, most of the interactions of countries, at all levels, are carried out in cyberspace. Recently, many state governments are facing the problem of cyber-attacks and the danger of wireless communication technologies. In some other cases, cyber-attacks can have military or political purposes. Despite their potential for disruption to international peace and security, there is no specific international legal structure for analyzing cyber-attacks. The aim of this paper is to study the framework of jus ad bellum to cyber-attacks and to examine the application of articles 2(4) and 51 of the United Nations Charter to this new reality. This paper argues these provisions and the United Nations General Assembly Resolution* 3314 (XXIX) *can be interpreted to include cyber-attacks. It is expected that the comprehensive review study presented will be useful.*

Keywords : Cyber-attaque ; state responsibility ; United Nations Charter, international Peace and Security

1.- *Introducción*

Podemos definir los ciberataques estatales como aquellas ofensivas llevadas a cabo en el ciberespacio atribuibles a un Estado, contra otro Estado y que comprometen la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan[1]. Este tipo de ofensiva plantea dos tipos de desafíos: por una parte, los relativos a los ataques de servicios esenciales al funcionamiento de un país y su defensa, y por otra, los planteados por la protección de informaciones sensibles desde el punto de vista político, militar o económico, ante las

*Este trabajo es el resultado de las investigaciones realizadas en el marco del Grupo de investigación SEJ-399 "Derecho Común Europeo y Estudios Internacioales" del SICA (Junta de Andalucia) y del *Framework of Stars Project year 2020 -2nd part (Supporting Talented Researchers- Action 2- Incoming Visiting Professor- Long Term) CUP* de l'Università degli Studi di Bergamo.

[1] 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», nº. 40, de 26 de febrero de 2013.

tecnologías de intrusión informáticas cada vez más sofisticadas. Y es que, no cabe duda que, en razón de su carácter subrepticio, los ciberataques fuerzan a una revisión de las nociones tradicionales de fronteras, siendo en todo caso inviolables.

La mayoría de actividades informáticas de naturaleza maliciosa tienen lugar en tiempo de paz[2], lo que puede provocar confusión, en cuanto que engloban los ciberataques estatales. Por esta razón, antes de acotar el objeto de nuestra investigación, es necesario realizar algunas matizaciones conceptuales, en relación con las múltiples actividades ilegales que se pueden desarrollar en el ciberespacio. Nuestro trabajo, por tanto, no versará sobre la ciberdelincuencia, la cibercriminalidad o del *phishing*[3], regulados por los derechos penales nacionales. Tampoco sobre el ciberespionaje industrial, que consiste en copiar secretos industriales con el fin de obtener una ventaja competitiva; ni sobre el ciberterrorismo (que es la conducta en el ciberespacio de actividades terroristas por grupos armados transnacionales, actuando en su nombre y por su propia cuenta) en el ámbito del derecho de los conflictos armados. Cuestiones éstas que ya han sido tratadas en el *Manual Tallin*[4], el único texto que hasta el momento ha estudiado la cuestión.

Si los conflictos de baja intensidad eran los métodos privilegiados de grandes potencias durante la guerra fría, en nuestros días los ciberataques estatales están siendo el instrumento perfecto para alcanzar los mismos objetivos sorteando el marco jurídico internacional de prohibición del uso de la fuerza. De hecho, los EEUU ya han 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 todas que plantean nuevos interrogantes sobre la calificación de estas acciones en tiempos de paz[5].

---

[2] K. ZIOLKOWSKI (dir.), *Peacetime Regime for State Activities in Ciberspace. International Law, International Relations and Diplomacy*, Tallinn, 2013, NATO, Publication, p. 15.

[3] Práctica que consiste en engañar a alguien para que teclee su contraseña en una web fraudulenta

[4] M. N. SCHIMTT (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warface*, Cambridge, 2013, Cambridge University Press.

[5] 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 unida*s, Res. AG 2625, Doc. Off AGNU, 25 ses, sup nº. 28, Doc UN A/5217 (1970), preámbulo, párr. 7.

2.- *Los ciberataques estatales y la "Paz y seguridad internacionales"*

La palabra "ciberataque" es un neologismo formado a partir de las palabras "ciberespacio" y "ataque". El ciberespacio representa un espacio universal constituido por una red interdependiente de infraestructuras informáticas que conforman internet, las redes de telecomunicaciones, los sistemas informáticos, así como los procesadores y controladores integrados[6]. Íntegramente creados por el hombre[7], no están limitados por fronteras y es por este motivo que presenta ciertas similitudes con el alto mar y el espacio ultraterrestre. Por tanto, el ciberespacio no depende de la competencia de un solo Estado o de un grupo de Estados, constituyendo un bien común planetario. En lo que se refiere al término "ataque", éste presenta usos diferentes según se trate del plano jurídico-militar o informático. En este último ámbito, se califica como tal toda tentativa de acceso no autorizado a un sistema de servicios a redes o a información, o toda tentativa que trate de comprometer la integridad de un sistema.

Ahora bien, a pesar de las definiciones por las que se pretende acotar el concepto de ciberataque, no podemos negar que se trata de un término genérico que sirve para calificar los ataques informáticos llevados a cabo única y exclusivamente en el ciberespacio[8]. Este tipo de ataques se pueden llevar a cabo por acción u omisión[9] y tienen como objetivo explotar los fallos o deficiencias que puedan surgir del acceso de un usuario al ciberespacio. La doctrina los clasifica en tres tipos: a) los *ciberataques perturbadores* que intentan inutilizar o tomar el control de los sistemas informáticos de

---

[6] R. KISSEL (ed.), *Glossary of key information security terms*, NISTIR 7298 Revision 2, 2013, National Institute of Satandards and Technology, U.S. Department of Commerce, p. 57, en línea https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf [última consulta 3/1/2022]

[7] CH. C. DEMSHAK & P. DOMBROWSKI, *Rise of a Cybered Westphalian Age*, en «*Strategic Studies Quaterly*», Spring 2011, pp. 32-35. Ver también F. SCHREIER, *On Cyberwafare*, Geneva, 2012, *Centre for the Democratic Control of Armed Forces*, DCAF Horizon 2015 Working Paper Series (7), en línea https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf [última consulta 3/1/2022]

[8] SECURITE PUBLIQUE CANADA (ed.), *Stratégie de cybersécurité du Canada : renforcer le Canada et accroître sa prospérité*, 2010, Ottawa - Ontario : Sécurité publique Canada, en línea https://publications.gc.ca/site/eng/9.638020/publication.html [última consulta 3/1/2022].

[9] Piénsese, por ejemplo, en los ataques distribuidos de denegación de servicios (DDOS), que hasta ahora se veían básicamente como una forma de bloqueo *on-line*. Éstos se han convertido en una herramienta de guerra de información.

infraestructuras críticas como el SCADA (*Supervisory Control and Data Acquisition*)[10] y que tienen como fin causar daño físico o funcional; b) los *ciberataques no intrusivos* que usan técnicas para bloquear accesos o la desfiguración de webs con el propósito de cambiar contenidos y c) *los ciberataques intrusivos*, cuyo objetivo se centra en acceso a datos, ya sea para obtenerlos utilizando *malware* info-stealer ("ladrón de información") o alterarlos[11]. Todos ellos pueden ser impulsados/patrocinados, organizados, coordinados y/o realizados por personas físicas, jurídicas o, incluso, por Estados, siendo la autoría de estos últimos los que nos interesa a efectos de nuestra investigación.

El ciberespacio se considera como un nuevo campo de batalla y, por tanto, podría asimilarse a otros espacios en los que se desarrollan conflictos, como la tierra, el mar, el aire, o incluso, el espacio extra-atmosférico. Los ciberataques estatales son a menudo calificados por la prensa como "actos de ciberguerra", calificación poco apropiada, ya que para que pudiera calificarse así, el ciberataque tendría que llevarse a cabo en un contexto de conflicto armado o de actividades militares, gracias a una gran variedad de medios y métodos numéricos en el ciberespacio y que comprende tanto las actividades ofensivas como las defensivas dirigidas contra infraestructuras informáticas.

3.- *La comisión de los ciberataques estatales: los métodos utilizados*

Los autores de los ciberataques estatales pueden ser agentes *de jure* o *de facto* del Estado. Durante la última década, se han constatado ciberataques estatales llevados a cabo por grupos de individuos impulsados por diversas motivaciones que actuaban

[10] SCADA es el sistema usado para monitorizar y controlar procesos en instalaciones industriales y empresas públicas, como plantas químicas, centrales eléctricas, refinerías, oleoductos de gas y petróleo, entre otros, en: D. ROSENFIELD, *Rethinking Cyber War*, en «Critical Review», vol. 21, nº. 1, 2009, pp. 77-78, disponible en http://www.tandfonline.com/doi/pdf/10.1080/08913810902812156, [última consulta 3/1/2022]

[11] Por consiguiente, se estima que el ciberataque engloba las actividades muy diversas, entre los que podrían destacar: la explotación no autorizadas de las redes informáticas (*computer network exploitation*), los cambios de direcciones de dominio, la denegación de un servicio, la saturación de correos, el *BlindRadars* (o bloqueo de tráfico aéreo) o los ataques por pulso electromangnéticos. Para más información véase F. J. UREÑA CENTEO, *Ciberataques, la mayor amenaza actual*, en «*Boletín del Instituto Español de Estudios Estratégicos* (ieee.es)», Documento Análisis, 40/2013, pp. 7-8 en línea https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf [última consulta 3/1/2022]

(presuntamente) en función de los intereses de un determinado Estado. Los individuos y entidades implicados en los ciberataques contra otros Estados responden a menudo a razones esencialmente patrióticas: éstos se llevan a cabo como una forma de reivindicación o protesta contra las decisiones políticas de otro Estado. Ahora bien, el análisis de las herramientas utilizadas para el lanzamiento de ataques informáticos puede permitir la determinación de la responsabilidad individual o estatal de un ataque, permitiendo apreciar mejor los desafíos que plantean las nuevas armas.

Por lo que respecta a los métodos más utilizados desde 2006 para ejecutar los ciberataques estatales[12], podemos señalar dos principalmente, la instalación clandestina de programas maliciosos y los ataques de los *sites* en internet. En relación al primero, cabe señalar que se trata de un programa informático infiltrado en una red, sin previo consentimiento de su propietario o de su usuario, con la intención de comprometer la confidencialidad, la integridad o la disponibilidad de datos, de aplicaciones de la víctima o del sistema de explotación; o únicamente con el fin de importunar a la víctima. Puede presentarse bajo la forma de un virus, de un "gusano" o de un troyano[13]. En este sentido, la integridad de una red informática puede verse comprometida debido al uso de un software espía que es un programa concebido con el fin de recopilar información sobre los usuarios o las organizaciones propietarias de la red infectada. Esta información sobre el medio es transmitida a personas no autorizadas. La bomba lógica es otro tipo de software malicioso, con un sistema de activación diferido (a distancia) y concebido para causar daños en el sistema informático o ejecutar ciertas accesiones, únicamente cuando se reúnen ciertas condiciones predefinidas por el creador del programa.

[12] Ver J.A. LEWIS, *A list of significant cyber events since 2006*, 19 December 2013, Center for Strategic & International Studies y del mismo autor *Cyberwarfare and its impact on international security*, UNODA Occasional Papers nº. 19, June 2010, en línea http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP_19.pdf [última consulta 3/1/2022]

[13] Para más información R. LONGEON & J.L. ARCHIMBAUD, *Guide de la securité des systèmes d'information à l'usage des directeurs* (de laboratoires de recherche), 2ème trimestre 1999, Paris Centre National de la Recherche Scientifique, en línea https://hal.archives-ouvertes.fr/hal-00561702/document [última consulta 3/1/2022]

El segundo método más utilizado, es el de los ataques cibernéticos contra sites de internet. La denegación del servicio, también llamado "ataque por saturación", tiene por objetivo el bloque del acceso autorizado a las redes, a los sistemas o aplicaciones, enviando simultáneamente un gran número de solicitudes de conexión, provocando una pérdida de recursos informáticos. Este tipo de ataque trata de perturbar el buen funcionamiento del servicio o del *site* de internet. La denegación del servicio como consecuencia del ciberataque tiene efectos inmediatos aparentes. Aunque los *sites* de internet afectados se encuentran bloqueados, su contenido no está afectado, a no ser que el ataque vaya acompañado de actos de desconfiguración contra la página o programa.[14] Es fácil llevar a cabo este tipo de ataques y son difíciles de interrumpir. En conclusión, los ciberataques presentan nuevos desafíos en materia de relaciones internacionales. Sus consecuencias pueden variar desde la interferencia de señales numéricas de comunicación hasta la neutralización de infraestructuras de un Estado, con la finalidad de causar el pánico en la población y daños tanto humanos como materiales.

4.- *La praxis de los ciberataques estatales*

En las últimas décadas han sido varios los casos en el contexto internacional en el que se ha constatado la existencia de ciberataques estatales. Haremos mención, a continuación, a algunos de lo más referenciados. El más conocido fue el que sufrió 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 en 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

[14] Rapport d'information du Sénat – Session extraordinaire de 2011-2012. *Rapport d'information fait au nom de la commission des affaires étrangères, de la defense et des forces armées sur la cyberdéfense*, par M. J-M BOCKEL, Sénateur, nº. 681, registrado en la Presidencia del Senado el 18 de julio de 2012, p. 11.

móvil y servicios de urgencia[15]. 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[16]. A pesar de que lo s ataques se realizaron desde ordenadores ubicados en 178 países distintos, [17] el gobierno estonio sostuvo desde un primer momento que Moscú había estado detrás de los ataques de los que había sido víctima[18]. Estos acontecimientos llevaron a la OTAN a repensar su política de ciberdefensa e impulsar nuevas medidas de lucha. De esta moto, elaboró por primera vez una "Política de Ciberdefensa", basada en tres pilares fundamentales: a) la subsidiariedad, en virtud de la cual, se determina que la asistencia sólo se activará a petición del Estado afectado; b) la no duplicidad, es decir, se evita la duplicación innecesaria de las estructuras o capacidades en los planos internacional, regional y nacional y c) la seguridad, es decir, la cooperación basada en la confianza de los aliados[19].

Un segundo ejemplo de ciberataque fue el que padeció Georgia. Debido a diferencias político-militares entre este país y Rusia, a causa de la situación de Abjasia y

[15] Véase TRAYNOR, *The Guardian* 17 May 2007.
[16] Esta afirmación se hizo en un debate en el Senado francés sobre el tema. *Rapport d'information du Sénat*… cit.
[17] K.K. LIIS VIHUL ENEKEN TIKK, *International cyber incidents: legal considerations*, Tallin, 2010, CCD COE Publications, p. 23.
[18] En marzo de 2009, con ocasión de un panel de discusión sobre las guerras de información del siglo XXI, un diputado de la *Douma* (cámara baja del Parlamento de Rusia) declaró que los ataques contra Estonia se habían lanzado por su asistente, por iniciativa propia de este último. Algunos días más tarde, un grupo de jóvenes patriotas rusos, Nashi se atribuyó la responsabilidad de dichos ataques. *Nashi* es un movimiento de jóvenes rusos próximos al Kremlin y subvencionado por éste, que convocó protestas ante la embajada de Estonia en Moscú, al comienzo de la crisis ruso-estonio en 2007, describiendo sus acciones como un "bloqueo" de la representación diplomática.
[19] M. J., CARO BEJARANO, *La nueva dimensión de la amenaza global: la amenaza cibernética*, «Boletín del Instituto Español de Estudios Estratégicos (ieee.es)», Documento Análisis, 40/2013, p. 5, en línea https://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA40-2013_AmenazaCibernetica_MJC.pdf [última consulta 3/1/2022]

Osetia del Sur, aquel país fue víctima de ataques informáticos[20]. 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"[21]; 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 el 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 bloque 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.

Por último, otro ejemplo, de ciberataque es el que denunció la República Islámica de Irán. *Stuxnet* es un "gusano" (o código dañino) que forma parte de un programa secreto

[20] N. SHACHTMAN, *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It*, «Wired Danger Room Magazine», 11 March 2009, en línea http://www.wired.com/dangerroom/2009/03/georgia-blames/ [última consulta 3/1/2022]

[21] CE, CONSEIL, *Report of the independent international Fact-Finding Mission on the Conflict in Georgia*, Volume II, September 2009, en línea https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf [última consulta 3/1/2022]

de los EEUU titulado *Olympic Games*[22] 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 iranís 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[23].

5.- *Los ciberataques y su encaje en el art. 2(4) de la Carta de Naciones Unidas: un asunto pendiente en la agenda jurídico-política de las relaciones internacionales*

Si por la condena inequívoca del recurso a la guerra, el Pacto Briand-Kellogg supone, según ciertos autores, la transición del *jus ad bellum* al *jus contra bellum*[24], el artículo 2(4) de la Carta de Naciones Unidas es el elemento principal del nuevo sistema normativo de recurso al uso de la fuerza[25]. Este hecho permite reafirmar los propósitos de la ONU descritos en el artículo 1.1 de la citada Carta. En este contexto, la prohibición de la amenaza o uso de la fuerza se codifica de forma explícita en un tratado internacional que la convierte en una obligación *erga omnes*[26]. En su art. 2, de conformidad con lo dispuesto en su capitulo VII, se consagra con carácter general el principio de la

[22] D. E. SANGER, *Obama order sped up wave of cyberattacks agains Iran*, «The New York Times», June 2012.
[23] E.PEREZ & A. ENTOUS, *FBI Probes Leaks on Iran Cyberattack*, «The Wall Street Journal», 5 June 2012.
[24] Y. DINSTEIN, *War, aggression and self-defence*, Cambridge, Cambridge University Press, 2005, p. 83.
[25] Sentencia de 19 de diciembre de 2005, *asunto de las actividades armadas en el territorio del Congo (República Democrática del Congo c. Uganda)*, CIJ *Rec.* 168, 2005, par. 148.
[26] Ver *Consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado*, Opinión consultiva, 9 de julio de 2004, para 188. Esta opinión, así como las opiniones y declaraciones separadas de los magistrados de la Corte, en línea: http://www.icj-cij.org/cijwww/cdocket/cmwp/cmwpframe.htm [última consulta 3/1/2022]

prohibición del uso de la fuerza. La norma contenida en la Carta tiene una formulación más completa que la prohibición contenida en el Pacto Briand-Kellog porque, en primer lugar, no se refiere exclusivamente a la guerra sino al "uso de la fuerza"; en segundo lugar, la prohibición comprende no sólo el uso de la fuerza, sino también la "amenaza" de uso de la fuerza[27].

Como es sabido, la prohibición contra la amenaza o el empleo de la fuerza es una norma internacional consuetudinaria y convencional de *jus cogens*. En virtud del artículo 103 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[28]. Esta norma se completa por el principio consuetudinario de la no intervención. Aunque presente una apariencia simple en estas disposiciones, el art. 2(4) ha ocasionado numerosas discusiones tanto por su contenido como por su alcance. En este sentido, uno de los mayores debates relativos a su interpretación es el relativo al tipo de fuerza prohibida: ¿se trata exclusivamente de la fuerza militar o también de la prohibición de aquellos medios que constriñan económica, política o ideológicamente?[29] Basándonos en los trabajos preparatorios de la Conferencia de San Francisco, la mayor parte de las obras doctrinales sobre el empleo de la fuerza en las relaciones internacionales, enuncian que la fuerza militar prohibida por el artículo 2(4) es la militar[30]. De modo que, si se interpreta el artículo 2(4) en este sentido, significa que la fuerza no debe utilizarse contra ningún Estado, al margen de que éste sea o no de Naciones unidas[31]. La prohibición se aplica a las relaciones internacionales de los Estados, tanto a las amenazas al recurso de la fuerza militar como a las acciones militares. Las Resoluciones 2625 y 42/22 de la Asamblea General de Naciones Unidas se han utilizado también con el fin de interpretar esta

[27] M. DÍEZ DE VELASCO, *Instituciones de Derecho Internacional Público*, Editorial Tecnos, Madrid, 1999, p. 823.
[28] O. SCHACHTER, *In Defense of International Rules on the Use of Force*, in « Chicago L. Rev. », 53, 1986, pp 113-129.
[29] O. CORTEN, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law (French Studies in International Law)*, Osford, Hard Publishing, 2012, p. 50.
[30] T. RUYS, *Armed Attack and article 51 of the UN Charter*, New York, 2010, Cambridge University Pressp. 54.
[31] Véase párrafo 4 del articulo 2 en UN, *Répertoire de la pratique suivie par les organes des Nations Unies*, supp. 2 (1955-1959), vol. 1, article 2(4), par. 2

disposición. Estos textos permiten determinar la existencia de una *opinio juris* en cuanto al carácter consuetudinario[32] y no derogatorio[33] de la prohibición del empleo del uso de la fuerza en las relaciones internacionales, apoyándose en la idea de que el artículo 2(4) no se refiere a la coacción por parte de las fuerzas armadas, mientras que el principio de no-intervención sí se aplica a otras formas de coacción[34]. De una interpretación amplia del citado artículo, podría afirmarse pues, que la prohibición del uso de la fuerza es una prohibición expansiva que afecta a cualquier espacio posible de conflicto: la tierra, el aire, el mar, el espacio e incluso el ciberespacio.

El artículo 2(4) no tienen en cuenta solamente la integridad territorial o la independencia política del Estado, sino que comprende también todos los usos de la fuerza que sean de cualquier otra forma incompatibles con los propósitos de Naciones Unidas. A nuestro juicio esta disposición se refiere a todos los usos de la fuerza, al margen de su impacto o gravedad e incluye los casos de ciberataque estatal[35].

Por lo que se refiere al empleo ilícito de la fuerza, según la Corte Internacional de Justicia (en adelante CIJ), los actos que supongan una violación del principio consuetudinario de no-intervención que impliquen, bajo una forma directa o indirecta, el empleo de la fuerza en las relaciones internacionales constituye una violación del principio prohibiéndolos[36]. En este sentido, coincidimos con los profesores J-P PANCRACIO y E-M PETON, cuando afirman 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 »[37]. Toda intervención ilícita en los asuntos de otro Estado

[32] *Actividades militares y paramilitares en Nicaragua y contra Nicaragua contra los Estados Unidos de América*, sentencia de fondo de 27 de junio de 1986, *CIJ. Rec*. 1986, pars. 189-90, 292.
[33] *Declaración sobre el mejoramiento de la eficacia del principio de abstención de la amenaza o de la utilización de la fuerza en las relaciones internacionales*, Resolución 42/22 de la AGNU, Doc off. AG UN, 42e sess, Doc UN A/42/766 (1987), par. 2.
[34] *Actividades militares y paramilitares en Nicaragua…*cit., par. 191.
[35] K. ZIOLKOWSKI, *General principles of international law as applicable in cyberespace*, dans K. ZIOLKOWSKI (dir.), *Peacetime Regime for State Activities in Cyberespace. International Law, International Relations and Diplomacy*, Tallinn 2013, NATO CCD COE Publication, pp. 143-144.
[36] *Actividades militares y paramilitares en Nicaragua,* cit., par. 209.
[37] J.P. PANCRACIO et E-M. PETON, *Un mutant juridique, ¿l'agression internationale?*, «Cahiers de l'IRSEM», 7, 2011, p. 24, nota 18.

y acompañado del uso de la fuerza constituye una violación de la prohibición del recurso al uso de la fuerza en las relaciones internacionales. Sin embargo, como recuerda la CIJ, el simple envío de fondos a las fuerzas rebeldes de un país, si bien constituye un acto de intervención en los asuntos internos de otro Estado, no constituye *per se* el empleo de la fuerza[38]. De este modo podría afirmarse que todo empleo de la fuerza es una intervención, pero no todas las intervenciones violan el artículo 24: es necesario que el medio empleado por un Estado contra otro, conlleve el uso de la fuerza para que podamos hablar de recurso ilícito al uso de la fuerza.

El empleo ilícito de la fuerza puede revestir formas más graves, como aquéllas que constituyen una agresión armada y otras modalidades menos brutales[39] 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. Estas diferentes modalidades pueden ejercerse de forma directa o indirecta. En efecto, mientras que el artículo 2(4) de la Carta no hace distinción alguna entre el empleo directo e indirecto del uso de la fuerza[40], la CIJ sí la establece, afirmando expresamente 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 forcé, 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»[41].

6.- *Los ciberataques estatales, ¿una nueva forma de empleo ilícito de la fuerza?*

Según la interpretación realizada por la CIJ del artículo 2(4), el apoyo de un Estado a las actividades armadas subversivas o terroristas en otro Estado constituye una violación de la prohibición del uso de la fuerza. El propósito de la subversión es la desestabilización de un gobierno la cual que puede ser interpretado como un acto contra la integridad

[38] *Actividades militares y paramilitares en Nicaragua,* cit., par. 228.
[39] *Actividades militares y paramilitares en Nicaragua,* cit., parr. 191.
[40] S.M. SCHWEBEL, *Agression, intervention and self-defence in modern international law*, in *Recueil Académie du droit international de La Haye*, 136, 1972, p. 458.
[41] *Actividades militares y paramilitares en Nicaragua,* cit., parr. 205. Véase también la Resolución 42/22, cit., par. 6.

territorial o la independencia política del Estado en cuestión. En el caso de los gobiernos de Estonia y Georgia, como los gobiernos de cualquier Estado, tienen el derecho a ejercer su autoridad el ciberespacio que pertenece a su jurisdicción. Por lo tanto, los ataques por saturación que sufrieron en 2007 y 2008 podrían ser considerados como actos de subversión[42]. Cabe preguntarse en este contexto si tales actividades suponen o no un empleo directo de la fuerza armada, tal como prevé el párrafo 4 del artículo 2.

Los ciberataques estatales plantean otras cuestiones tales como el recurso a la fuerza no cinética por parte de un Estado y sobretodo, 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[43]. 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 de la redacción de la Carta, 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 puede considerarse superada debido a que no tiene en cuenta la aparición, tras la redacción de la Carta, de nuevas armas no cinegéticas tales como las armas nucleares, radiológicas, biológicas y químicas. El hecho de que un ordenador haya sido utilizado, como medio principal de ejecución de un ataque contra un Estado, no parece pertinente a la hora de calificar el acto como que uso ilícito de la fuerza. En efecto, la CIJ ha declarado que la Carta no prohíbe ni permite expresamente el empleo de un arma en particular[44]. En efecto, 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; este es el propósito último de la prohibición contenida en el artículo 2(4). La fuerza armada no se define por el empleo o la liberación o no de

[42] J. BARKHAM, *Information Warfare and International Law on the Use of Force*, *International Law and politics*, 34, Seq: 57, 2001, p. 89.
[43] M.N. SCHMITT, Computer Network Attack and the Use of Force in International Law : Thoughts on a Normative Framework, « *Columbia Journal of Transnational Law* », 37, 1998-1999, p. 909.
[44] *Opinión consultiva sobre la licitud del empleo o amenaza de armas nucleares* de 1996, *CIJ Rec*., par. 39.

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, entre los que destacan las presiones diplomáticas, económicas y políticas y cuyo objetivo es la calificación de los ataques informáticos, en relación con el artículo 2(4) de la Carta[45]. 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, sea cual sea su origen. Según este planteamiento, que ha sido utilizado por los autores del *Manual Tallin*, 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[46]. En este contexto, los factores no constituyen criterios jurídicos, pero tienen en cuenta una serie de consideraciones que son susceptibles de influenciar la evaluación de la naturaleza del empleo de la fuerza; los criterios deben ser evaluados de forma holística. Si comparamos las consecuencias de los ciberataques con las de los ataques no cibernéticos, este ejercicio nos permite hacer uso de la definición restrictiva 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*[47]. De todos modos, es importante subrayar que los defensores de este planteamiento no realizan una distinción entorno a la naturaleza informática o cinética de los medios de ataque utilizados, centrándose en los efectos ocasionados. Sólo aquellos ciberataques que pueden producir efectos cinéticos se consideran como uso de la fuerza. Dado que la mayoría de los ciberataques son más perturbadores que destructores y éstos no causan (hasta el momento) resultados no materiales (con la excepción de *Stuxnet*)[48], sería erróneo tener en cuenta solamente los efectos que resulten en destrucciones físicas. En efecto, nos arriesgamos a encontrarnos ante un enfoque demasiado restrictivo que excluya los ciberataques paralizando las infraestructuras

[45] M.N. SCHMITT, *Computer Network*, cit., pp. 914-915.
[46] M.N. SCHIMTT (dir.), *Tallinn Manual on the International Law*, cit., p. 45.
[47] M.N. SCHMITT, *Computer Network*, cit., p. 915.
[48] M.N. SCHMITT, *International Law in Cyberespace : The Koh speech and Tallinn Manual Juxtaposed*, « Harvard International Law Journal », 54, 2012, p. 20.

críticas de un país, así como los ataques informáticos destinados a bloquear los servicios de sites que proporcionan servicios esenciales a la población[49]. Por este motivo, ciertos autores proponen un método de análisis de los ciberataques estatales basado en la naturaleza del objetivo y que defiende la imputación de una responsabilidad estricta a los autores de los ciberataques[50]. Según esta corriente, cuanto más esencial sea el objetivo del ciberataque para el funcionamiento del Estado, mayor será la probabilidad de que éste sea considerado como una violación del artículo 2(4). Por tanto, podría concluirse 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. El enfoque de la responsabilidad estricta se encuentra sujeto a una cierta subjetividad, debido a que los Estados disponen de discrecionalidad a la hora de definir qué servicios considera como una infraestructura crítica. A día de hoy, parece que el modelo de análisis propuesto por Schmitt parece el más apropiado para el examen de un ciberataque estatal, llevado a cabo en tiempos de paz, en relación con las disposiciones del artículo 2(4) de la Carta. Sujeto a la existencia de pruebas concluyentes en cuanto a la responsabilidad de Rusia tras los ataques el bloque de servicios del que fue víctima Estonia en 2007 nos permite concluir que se trató de un uso ilícito de la fuerza[51]. Y es que, como afirma 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 »[52]. Si, como señaló la CIJ, el aspecto consuetudinario de la prohibición del uso de la fuerza está « non conditionné par les dispositions relatives à la sécurité collective»[53], su componente condicional sufre algunas excepciones[54], como son los artículos 39 y 51 de la Carta.

---

[49] N. MELZER, *Cyberwafare and International Law*, UNIDIR Resources, 2011, en linea https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [última consulta 3/1/2022]

[50] Sir IAN BROWNIW, *International Law and the Use of Force by States*, 1963, p. 362.

[51] M.N. SCHMITT, *Cyber operations and the Jus and Bellum revisited*, *Cyber operations and the jus ad bellum revisited,* « Villanova Law Review », 56 (3), 2011, pp. 588.

[52] H. WEHBERG, *L'interdiction du recours à la forcé. Le principe et les problèmes qui se posent*, *Rec. Des Cours de l'Académie du droit international de la Haye*, 1951 p. 64.

[53] *Actividades militares y paramilitares en Nicaragua,* cit., par. 188.

[54] *Ibid*, par. 193.

7.- *Algunas reflexiones en torno a la seguridad colectiva y el derecho a la legítima defensa a la luz de los ciberataques*

La primera excepción es la posibilidad para el Consejo de Seguridad de Naciones Unidas de recurrir a la fuerza aplicando el artículo 39 de la Carta de Naciones Unidas y 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.

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 autoriza al Consejo de Seguridad a realizar « recomendaciones o decidirá que medidas serán tomadas de conformidad con los Artículos 41 y 42 para mantener o restablecer la paz y la seguridad internacionales» si éste constata «…la existencia de amenaza a la paz, quebrantamiento de la paz o acto de agresión». En este sentido, la determinación de un acto de agresión es un pre-requisito del ejercicio por parte del Consejo de Seguridad de las prerrogativas del artículo 39. 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". Según el artículo 39, sólo el Consejo de Seguridad puede decidir si el artículo 2(4) ha sido violado. La calificación de una situación por parte del Consejo de Seguridad es una evaluación política y no jurídica. Éste dispone de una discreción total y aparentemente ilimitada en cuanto a la constatación de una situación de agresión. La discreción de la que dispone el Consejo de Seguridad en virtud del artículo 39 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, obviando en la mayoría de casos la aplicación del artículo 39 de la Carta en sus resoluciones. Una vez calificada la situación *de facto*, el Consejo de Seguridad podrá autorizar el uso a recurrir a la fuerza armada para poner fin a «amenaza a la paz, quebrantamiento de la paz o acto de agresión» (art. 39) en aquellos casos en los que las medidas no coercitivas del artículo 41 no hayan sido efectivas. 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 se permite como respuesta a una "agresión armada", siempre que el Consejo de Seguridad haya sido inmediatamente informado de la acción armada defensiva llevada a cabo. El ejercicio del derecho a la legítima defensa debe responder a las siguientes condiciones: la agresión armada debe haberla llevado a cabo un Estado; sólo el Estado víctima de una agresión armada puede servirse del derecho consagrado en el artículo 51; el recurso a la fuerza debe ser una respuesta a una agresión armada sobrevenida y únicamente en respuesta a ella, el recurso a la fuerza debe respetar los principios consuetudinarios de necesidad y de proporcionalidad. La acción en legítima defensa deberá tener en cuenta que el Consejo de Seguridad podrá tomar las acciones que el considere necesarias para mantener o reestablecer la paz y seguridad internacionales. Aunque no se defina en la Carta, la CIJ ha afirma expresamente que «l´accord paraît aujourd´hui général sur la nature des actes pouvant être considérés comme constitutifs d´une agression armée»[56]. Existen dos elementos importantes en una agresión armada[57]: una violación de la integridad territorial o soberana de otro Estado y el empleo de medios militares o paramilitares (de ahí el empleo del adjetivo "armado"). La noción de "agresión armada" del artículo 51 es mucho más restrictiva que la de "agresión" del artículo 39[58]. Un acto de agresión armado es una agresión, pero toda agresión no constituye necesariamente una agresión armada. Al igual que, todo empleo unilateral e ilícito de la fuerza no constituye una agresión armada, aunque 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*, ponen de relieve el compromiso decidido por los redactores de la Carta en la Conferencia de San Francisco.

[55] H. WEHBERG, *L'interdiction du recours à la forcé,* cit., p. 64.
[56] *Actividades militares y paramilitares en Nicaragua,* cit., parr. 188, par. 176.
[57] J. KAMMERHOFER, *Uncerainties of the law on self-defence in the United Nations Charter*, « Netherlands Yearbook of International Law», 143, 2004, p. 160.
[58] A. RANDELZHOFER, *Article 51* en B. SIMMA et al, dir, *The Charter of the United Nations*, A Comentary, vol 1, 2 ed., Oxford, Oxford University Press, 2002, par. 17, pp. 794-5.

Todo apunta a que el término *armed attack* ha sido utilizado en la versión inglesa debido a la falta de consenso, en el momento de redacción de la Carta, sobre la definición de *aggresión*.

8.- *La posible responsabilidad de Estado por ciberataques*

Con el fin de determinar si un ciberataque estatal constituye un acto de agresión, de acuerdo con los parámetros del derecho internacional[59], el Estado víctima debería convencer al Consejo de Seguridad, no sólo de la implicación de un Estado en la ejecución u organización del ataque informático, sino también el hecho de que el ciberataque o sus consecuencias constituyen un empleo ilícito de la fuerza de una gravedad suficiente[60]. Conforme a la práctica del Consejo de Seguridad, deberá demostrar también que el ciberataque perseguía un fin agresivo. Ahora bien, en este contexto cabe preguntarse si un ciberataque puede ser estatal en derecho internacional público. Según los autores del *Manual Tallinn*, un Estado es responsable de cualquier ciberataque que le sea imputable y que constituya una violación de una obligación internacional. La imputación jurídica de un ciberataque a un Estado es un ejercicio difícil[61], por una razón: el carácter clandestino de los ataques cometidos por los agentes de un Estado, debido a la opacidad que reviste la naturaleza exacta de la relación existente entre un Estado y las personas privadas, autores últimos del ataque informático contra otro Estado.

Si tenemos en cuenta los criterios definidos por la CIJ y empleados en derecho internacional público[62] para atribuir la responsabilidad de un hecho internacionalmente ilícito a un Estado, puede ser muy difícil, por no decir imposible, imputar un ciberataque

[59] Definición de agresión, Doc. off AG UN, 29e ses., anexo, Doc. UN A/RES/29/3314 (1974), art. 3.a.
[60] *Ibid*., art. 2.
[61] K. ZIOLKOWSKI, *Ius ad bellum in Cyberespace – Some thoughts on the Schmitt-Criteria for Use of Force*, en C. CZOSSEK, R, OTTIS AND K. ZIOLKOWSKI (dir.), 2*012 4th International Conference on Cyer Conflict*, Tallin, NATO CCD COE Publications, 2012, nota 148, p. 306.
[62] La Comisión de Derecho Internacional también ha confirmado la validad 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 AG en su Resolución 56/83, de 12 de diciembre de 2001. Puede verse en *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.

a un Estado. En efecto, el artículo 8 del Proyecto de artículos de Responsabilidad de Estados por hechos internacionalmente ilícitos[63] no es de gran ayuda debido a que no es sencillo para un Estado B, víctima de un ciberataque, probar que ha sido resultado de intrusiones precisas de un Estado A; o demostrar que dicho Estado A ha ejercido un control directo o efectivo, durante el curso del incidente informático, a través de terceros. Se constata que el acceso a los elementos de prueba es un gran obstáculo para la atribución de un ciberataque a un Estado. En el caso del *Estrecho de Corfú*, la CIJ ha reconocido 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»[64]. Por estas circunstancias es muy difícil demostrar la implicación de un Estado en el caso de un ciberataque. El ejemplo georgiano es la perfecta ilustración de lo que parece ser un nodo. La coincidencia temporal entre el bloque de los servicios y el inicio de la ofensiva militar terrestre rusa, hace pensar que los piratas informáticos debían ser conscientes previamente de los planes de la armada rusa[65] y que ésta se llevo a cabo para proporcionar una ventaja militar a Rusia[66]. Sin embargo, ninguna prueba irrefutable demuestra los vínculos existentes entre Rusia y los responsables de los foros de discusión que propusieron la lista de objetivos georgianos. Por otra parte, el simple hecho de que un Estado o uno de sus agentes hiciera referencia a las acciones cibernéticas hostiles no es suficiente para atribuirle dichos actos, el derecho internacional exige un reconocimiento y una adopción de actividades internacionales litigiosas. En cuanto a los ciberataques que se ejecutan por los agentes de un Estado, los obstáculos a la imputabilidad jurídica de éstos se deben a su carácter secreto. Por tanto, la existencia de

[63] Naciones Unidas A/RES/56/83. Asamblea General. Resolución aprobada por la Asamblea General 56/83. Responsabilidad del Estado por hechos internacionalmente ilícitos.
[64] *Asunto Estrecho de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte contra Albania*), 1949, Sentencia del 15 de diciembre de 1949, *CIJ Rec*., 1949, p. 18.
[65] 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 enero 2022].
[66] M. SAAKASHVILI, *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 3/1/2022]

estos ataques no transciende a un gran público más allá de referencias en la prensa, mientras que su veracidad jamás se confirma o se niega por parte de los Estados implicados. Sin embargo, si observamos las reservas de la CIJ en cuanto al carácter probatorio de las informaciones de notoriedad pública, no podemos concluir a ciencia cierta que Israel o Estados Unidos fueran los responsables de la creación de *Stuxnet*[67] o de la infección que éste llevó a cabo en el programa nuclear iraní, a pesar de las investigaciones abiertas por el gobierno americano[68]. Esta ausencia de flexibilidad de las normas internacionales de imputabilidad de hechos ilícitos a Estados permite a los países, autores o cómplices de ciberataques, escudarse en la negación plausible de los hechos.

Con el fin de impedir que los Estados continúen lanzando o patrocinando ciberataques contra otros Estados con total impunidad, ciertos autores han propuesto que se recurra a la noción de "responsabilidad imputada"[69], para superar el obstáculo que supone la prueba del vínculo y demostrar más fácilmente que un Estado se encuentra tras un ataque informático. Este nuevo marco de análisis, que tiene en cuenta el hecho de que se cometan cada vez con mayor frecuencia actos contra un Estado por parte de actores privados, afirma que el derecho internacional ha evolucionado lentamente desde un modelo de responsabilidad internacional centrado en la atribución de un acto a un Estado, hacia un modelo de responsabilidad indirecta basado en el deber de un Estado de respetar las obligaciones internacionales en materia de prevención de un hecho ilícito internacional[70].

El derecho internacional público impone a los Estados, un deber de vigilancia estatal que exige al Estado que se prevea de medios necesarios para prevenir que su territorio no sea utilizado para perjudicar los derechos de otro Estado soberano[71]. La CIJ ha

[67] El periodista D. E. SANGER fue quien reveló que Stuxnet habría sido creado por los Estados Unidos e Israel. Véase France, *Rapport d'information fait au nom de la commission des affaires étrangères de la défense et des forces armées sur la cyberdéfense*, cit., p. 8.
[68] E. PEREZ & A. ENTOUS, *FBI Probes leaks on Iran Cyberattack*, «The Wall Street Journal», 5 June 2012 en línea https://www.wsj.com/articles/SB10001424052702303506404577448563517340188 [última consulta 3/1/2022]
[69] Entre otros autores, destaca J. KULESZA, *State responsability for cyber-atttacks on international peace and security*, en «Polish Yearbook of International Law», 139, 2009, pp. 139-152.
[70] K. ZIOLKOWSKI, *Ius ad bellum in Cyberespace*, cit., p. 306
[71] *Asunto Fundición de Trail (Trail Smelter Arbitratin, Canada c. Estados Unidos)*, Sentencia arbitral de 11 de marzo de 1941 (Decisión final), RSA, vol. III, pp. 1905-1982.

confirmado el carácter *erga omnes* de las obligaciones de medios, como resultado del deber estatal de precaución, indicando que la responsabilidad de un Estado puede verse comprometida cuando cometa graves omisiones en labores de prevención de un hecho internacionalmente ilícito[72]. Por tanto, si un Estado tiene conocimiento de que su territorio se utiliza para cometer actividades cibernéticas maliciosas contra otro Estado[73], su responsabilidad internacional podrá exigirse debido a la falta de prevención de dicha violación de los derechos del Estado víctima. Según SHARP, se trata de un empleo indirecto de la fuerza al permitir o aceptar con total conocimiento de causa que la ciber-infraestructura sea utilizada, por actores privados, en tiempos de paz para llevar a cabo acciones hostiles contra otro Estado[74]. Un Estado puede entonces ver su responsabilidad comprometida no por el uso de la fuerza en sí mismo (porque éste no le puede ser imputado) sino por su apoyo[75] que puede ser, por ejemplo, la puesta a disposición por parte de un Estado de su infraestructura informática para la formación de autores de ataques[76]. El apoyo de un Estado a las acciones internacionalmente ilícitas de agentes no estatales[77] viola los principios de no recurso a la fuerza y de no intervención. En este mismo orden de ideas, el hecho de que un Estado A se provea de piratas informáticos, de herramientas informáticas especialmente concebidas para cometer una acción ofensiva contra un Estado B, supone un uso de la fuerza[78] que puede ser cualificado como una agresión indirecta, si dicho acto ofensivo cometido por el grupo de piratas es una actividad "suficientemente grave"[79] y siempre que pueda probársela implicación sustancia del Estado A[80]. Subsisten obstáculos a la imputación de la responsabilidad de ciberataques informáticos, como resultado de las técnicas de camuflaje de identidad

[72] *Asunto Estrecho de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte contra Albania*), cit., p. 22.
[73] W.G. SHARP, *Cyberspace and the Use of Force*, Virginia, 1999, Aegis Research Corporation, p. 112.
[74] *Ibid.* p. 67 y N. MELZER, *Cyberwafare and International Law*, cit., p. 11.
[75] N. MELZER, *Cyberwafare and International Law*, cit., p. 11.
[76] W.G. SHARP, *Cyberspace and the Use of Force*, cit., p. 112.
[77] *Actividades militares y paramilitares en Nicaragua y contra Nicaragua contra los Estados Unidos de América*, cit., párrafos 110 y 242.
[78] *Ibid*., párr. 228.
[79] Definición de agresión, Doc. off AG UN, cit., art. 2.
[80] J.N. MOORE, *Jus ad bellum before the international Court of Justice*, in «Va. J. Int'l L.», 54, 903, 2011-2012, p. 907.

utilizadas por los piratas informáticos; que provocan que se cuestione la veracidad de las informaciones obtenidas. En efecto, el hecho de que los primeros resultados de una investigación del origen de un ciberataque que provoca un bloque de servicios situé el origen de éste en direcciones numéricas situadas en un Estado A, no quiere decir que los ataques hayan sido lanzados desde una ciber-infraestructura situada en dicho Estado. Por otra parte, la existencia del deber de vigilancia estatal no supone que un Estado sea responsable de todo acto de violencia transfronterizo cometido desde su territorio. En materia de ciberataques, la responsabilidad de un Estado no puede ser atribuida por la simple razón de que los ciberataques sean lanzados (o así lo parezca) desde equipos informáticos que se encuentren en el territorio de dicho Estado, o desde sus infraestructuras gubernamentales.

De todos modos, el hecho de que se trate de ordenadores gubernamentales podría ser un indicio de que el gobierno esté implicado en la operación informática, aunque dicha presunción debería ser refutable. Además, teniendo en cuenta que tanto la jurisprudencia[81] como la práctica de los Estados, defienden 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 implique a dicho Estado en las actividades ilícitas del grupo, hay autores que proponen que la responsabilidad imputada a un Estado sea analizada desde la óptica de la aplicación efectiva de la obligación de medios. En este contexto, cuando se evalúe, se tendrán en cuenta los siguientes elementos: la multiplicación de ataques informáticos similares provenientes del Estado sospechoso, las medidas tomadas por dicho Estado con el fin de penalizar este tipo de infracciones, la asistencia que proporciona el Estado a otros Estados, víctimas de ciberataques cometidos por personas que se encuentran en su territorio. De este modo, solo se producirá un desplazamiento de la carga de la prueba de la víctima al Estado que no haya respetado sus obligaciones, que permitirá a la víctima no sólo beneficiarse de una práctica de la

[81] Sirvan como ejemplo, los pronunciamientos de la CIJ en los asuntos *Actividades militares y paramilitares en Nicaragua y contra Nicaragua contra los Estados Unidos de América*, cit., par. 195 y *Actividades armadas sobre el territorio del Congo (la República Democrática del Congo contra Uganda)*, cit., par. 301.

prueba más flexible conforme a las pruebas circunstanciales, sino que también permitirá evitar los fraudes de control territorial llevados a cabo por otros Estados. De esta forma se evitará que los ciberataques estatales se cometan gracias a la pasividad de un Estado[82].

9.- *Los ciberataques estatales: análisis a la luz de la definición de agresión*

Conforme a lo dispuesto en la Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas, la agresión es «el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia de otro Estado»[83] 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 de las relaciones internacionales desde inicios del siglo veinte, como demuestra el pacto de la Sociedad de Naciones y el Estatuto del Tribunal Militar de Núremberg. Al día de hoy, 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[84]. La definición de agresión, ha sido elaborada con el fin de servir como guía interpretativa al Consejo de Seguridad de Naciones Unidas; por ello, estimamos que el examen de los ciberataques estatales a la luz de la misma, deberían realizarse comparando los diferentes tipos de ataques informáticos y sus consecuencias, según las disposiciones del artículo 3 de la Resolución 334 (XXIX).

Teniendo en cuenta lo expuesto, actuando por analogía, la infección de las infraestructuras esenciales de un Estado por parte de softwares maliciosos podría considerarse en función de sus efectos[85], como supuestos de caso descritos en los artículos 3(a), 3(b), y 3 (d) de la Resolución 334 (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

[82] CH. C. DEMSHAK & P. DOMBROWSKI, *Rise of a Cybered Westphalian Age*, cit., p. 34.
[83] *Definición de agresión*, Doc. off AG UN, cit., art. 1.
[84] *Actividades militares y paramilitares en Nicaragua y contra Nicaragua contra los Estados Unidos de América*, cit., par. 195.
[85] P. CORNISH et. Al, *On Cyber Warface – A Chatham House report*, Chatam House, November 2012 en línea https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf [última consulta 3/1/2022]

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[86]. El artículo 3(c) de la Resolución 334 (XXIX) presenta el bloqueo naval como un acto de agresión. Ciertos autores ya han resaltado las similitudes existentes entre un bloqueo de servicios y un bloqueo naval[87]. Del mismo modo que, el bloqueo naval viola el derecho de acceso de un Estado al mar, los ataques por saturación violan el derecho de acceso de un Estado al ciberespacio. 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, las cosas han cambiado en el siglo XXI. Debido a la creciente dependencia de las sociedades modernas de Internet, un bloqueo de servicios de una cierta amplitud puede constituir una agresión en relación con los factores del contexto (tamaño del país, dependencia de internet) en el que se encuentre el país víctima de un ataque por saturación[88]. Buena prueba de ello es el caso de Estonia, país de pequeñas dimensiones y cuya dependencia de internet es muy alta: debido a su baja densidad de población, la realización de servicios administrativos a través de internet es básica para poder asistir las zonas rurales alejadas. En 2007, en el momento de los ataques, el 98% del territorio estonio tenía acceso a Internet y el 95% de las operaciones bancarias se realizaban on-line. La tasa de penetración de la telefonía móvil era de entorno a un 100% y el 86% de los habitantes realizaba sus declaraciones de impuestos a través de internet. Lo que explica que las autoridades de este país se sintieran víctimas de un acto de agresión[89].

Se puede establecer otra comparación entre los incidentes fronterizos descritos por la CIJ[90] y las intrusiones informáticas. Las intrusiones informáticas son operaciones

[86] *Asunto Estrecho de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte contra Albania*), cit, par. 18 y 22.
[87] S. HERZOG, *Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses*, in « Journal of Strategic Security », 49, p. 54.
[88] *Rapport d'information du Sénat*, cit., p. 30.
[89] TRAYNOR, *The Guardian*, cit.
[90] *Actividades militares y paramilitares en Nicaragua y contra Nicaragua contra los Estados Unidos de América*, cit., par. 195.

de ciber-explotación durante las cuales, el autor del ciberataque analiza las redes informáticas de la víctima con el fin de poner a prueba sus parámetros de defensa[91]. Mientras que las intenciones tras un incidente de frontera pueden discernirse fácilmente, no ocurre lo mismo con las intrusiones informáticas. Todo ciberataque comienza por una intrusión informática, con la particularidad de que, si durante la misma se instala un software malicioso de acceso diferido de forma subrepticia, es muy probable que pase desapercibido durante análisis del sistema. Dicha operación puede asimilarse a una operación de instalación de minas y 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"»[92]. 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 se encontraría condicionada a la satisfacción del criterio de "gravedad suficiente" de la Resolución 334 (XXIX).

Debido a la clandestinidad de los ataques, parece que no puede apreciarse la intencionalidad tras un ciberataque estatal hasta que el mismo se lleve a cabo y se investigue qué Estado(s) se han visto beneficiados del mismo: desde un punto de vista político o económico. 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 proporcionaron una ventaja a Rusia. Aunque, estos ciberataques no podrían haber sido considerados como operaciones cibernéticas de carácter militar, sus efectos podrían considerarse actos de agresión según 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) »[93]. Se trata de una aplicación de la doctrina de la acumulación de los hechos (*the needle prick*

[91] J. BARKHAM, *Information Warfare and International Law,* cit., p. 93.
[92] *Plataformas petrolíferas (República islámica de Irán contra Estados Unidos de América), sentencia de fondo de 6 de noviembre de 2003, CIJ Rec*. 161, par. 72.
[93] *Plataformas petrolíferas (República islámica de Irán contra Estados Unidos de América),* cit., par. 64.

doctrine) en virtud de la cual varios incidentes menores pueden acumularse con el fin de evaluar si procede el derecho a la legítima defensa[94]. 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 desde esta óptica de los ciberataques estatales 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, así como se podría apuntar sobre la base de informaciones fiables, que otros ataques de la misma naturaleza[95] se seguirán llevando a cabo en el futuro.

10.- *Conclusiones*

Como es sabido, la sociedad internacional no condena la guerra hasta el pasado siglo, distinguiendo hasta entonces entre guerras justas e injustas. Esta situación será progresivamente abandonada en pro de una mayor y mejor regulación de los conflictos armados, *ius in bello* y *ius ad bellum*. Con el nacimiento de la ONU la comunidad internacional decide preservar a las generaciones venideras del flagelo de la guerra y proscribir el uso de la fuerza en las relaciones internacionales salvo para situaciones concretas y en servicio del interés común. De esta forma la paz y la seguridad internacionales pasan a ser un principio cardinal del orden internacional, siendo la Paz un concepto mucho más amplio que el derivado de la simple ausencia de conflicto armado.

Al día de hoy, como ha reconocido en la CIJ en su jurisprudencia, el *jus ad bellum* está compuesto de normas consuetudinarias y normas convencionales, destacando en entre estas últimas las contenidas en los artículos 2(4), 39 y 51 de la Carta de Naciones Unidas. Ahora bien, no podemos ignorar el hecho de que este texto fue redactado en un contexto histórico muy concreto con el fin de hacer frente a los peligros derivados de los conflictos

[94] 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 3/1/2022].
[95] K. ZIOLKOWSKI, *General principles of international law as applicable in cyberespace,* cit. p.160.

tradicionales de fuerte intensidad, como los acaecidos durante las guerras mundiales. Es por esta razón que, a primera vista, no parece responder a los desafíos jurídicos que representa el desarrollo fulgurante de las nuevas tecnologías en la sociedad internacional contemporánea y, en concreto, a los problemas planteados por la intervención de los Estados en el ciberespacio.

A pesar del contexto en el que se redactó la Carta de San Francisco, su artículo 2(4) tiene el mérito de poner obstáculos al comportamiento de los Estados en pro de la consecución de la seguridad y paz internacionales. Éstos no pueden recurrir a la fuerza ni realizar comportamientos contrarios a la soberanía, independencia e integridad territorial de otros Estados. Sin embargo, la realidad es otra. En la práctica algunos Estados han desarrollado métodos indirectos y sutiles con el ánimo de salvar los obstáculos que establece la citada norma. Estos métodos han tomado formas sofisticadas que se desarrollan en nuevos espacios de difícil mensuración, como el ciberespacio. En este contexto, la dificultad de calificar jurídicamente los ciberataques estatales reside en el carácter no físico de la mayoría de sus consecuencias y en la compleja determinación de su autoría. Circunstancia eta última que supone un límite en la concreción de responsabilidades.

Exigir la existencia de resultados físicos y cuantificables a los ataques informáticos como requisito para calificarlos de violación *primas facie* del artículo 2(4), supondría ignorar la necesidad creciente de afrontar este tipo de actividades en nuestros días. Asimismo, evaluar los ciberataques únicamente desde el prisma de la legítima defensa nos llevaría a la errónea conclusión de considerarlos incidentes puntuales, ignorando su verdadera naturaleza. Por esta razón, creemos que es necesario atender al espíritu teleológico de la norma internacional a la hora de llevar a cabo cualquier calificación. A nuestro juicio, la multiplicación de los ciberataques en tiempos de paz podría considerarse una especie de “guerra de desgaste”. Sin duda, se trata de actos de hostilidad que constituyen una amenaza para la paz y la seguridad internacional y como tal deberían tener una respuesta.

El amplio margen de apreciación del que dispone el Consejo de Seguridad para evaluar las circunstancias que suponen un peligro para la paz y seguridad internacional, especialmente en el caso de la determinación de la existencia o no de un acto de agresión, debería permitirle desarrollar en el futuro criterios propios y específicos para la calificación de lo que podría denominarse "agresión informática", utilizando para ello una escala de intensidad adaptada a esta nueva realidad[96]. A nuestro juicio, estos criterios serían compatibles con la definición de agresión que ofrece la AGNU en su Resolución 334 (XXIX), la cual reconoce el empleo ilícito indirecto de la fuerza, una de las particularidades de los ciberataques estatales.

[96] B. LOUIS-SYDNEY, *La dimension juridique du cyberespace*, « Revue International et Stratégique », 87, 3, 2012, p. 74.