UNIVERSIDADE DA CORUÑA

FACULTADE DE DEREITO

TRABAJO DE FIN DE MÁSTER

THE USE OF THE FORCE IN CYBERSPACE

EL USO DE LA FUERZA EN EL CIBERESPACIO

O USO DA FORZA NO CIBERESPAZO

MÁSTER UNIVERSITARIO EN DERECHO DIGITAL Y DE LA INTELIGENCIA ARTIFICIAL

(MUDDIA)

Curso académico: **2021/2022**

Autora: **Bonia Campos Rivero**

Directora: **Gabriela Alexandra Oanta Oanta**

Fecha de presentación: **12 de septiembre de 2022**

Índice

Siglas y abreviaturas

APT: Amenazas Persistentes Avanzadas

CIJ: Corte Internacional de Justicia

CCDCOE: Centro de Excelencia para la Ciberdefensa Cooperativa

CDI: Comisión de Derecho Internacional

CNEC: Comisión Nacional sobre la Estabilidad del Ciberespacio

CNPIC: Centro Nacional de Protección de Infraestructuras Críticas

CNU: Carta de las Naciones Unidas

DoS: Denegación de Servicio

DDos: Denegación de Servicio Distribuido

ICE: Infraestructura Crítica Europea

OTAN: Organización del Tratado del Atlántico Norte

PREHII: Proyecto de Artículos sobre la Responsabilidad del Estado por Hechos Internacionalmente Ilícitos

TAN: Tratado del Atlántico Norte

TIC: Tecnologías de la Información y la Comunicación

UE: Unión Europea

Introducción

La invasión de Rusia a Ucrania iniciada el 24 de febrero de 2022 supuso el estallido de una guerra entre los dos Estados que llevaba gestándose desde 2014. La escalada de las tensiones internacionales (con la participación de la Organización del Tratado Atlántico Norte, la OTAN), la crisis económica causada por la Covid-19 y la lucha por las regiones de Crimea y Dombás, entre otros factores, propiciaron el caldo de cultivo perfecto para que, lamentablemente, en pleno siglo XXI, haya surgido un nuevo conflicto bélico.

Las nuevas tecnologías, los sistemas de inteligencia artificial, el almacenamiento masivo de datos en las redes… han supuesto que una parte de la contienda ruso-ucraniana se desarrolle en el ciberespacio. A diario recibimos numerosas noticias que hablan de ciberataques rusos, de las vulnerabilidades de los sistemas, de los peligros que supone la red. Muchas de estas acciones cibernéticas son atribuidas a uno u otro Estado u Organización internacional: Rusia, Estados Unidos, China, la OTAN… Si bien no sabemos con certeza quién se encuentra realmente detrás de estos ataques, pero, sin duda, son una realidad que nos obligan a formarnos en ciberseguridad e invertir en una adecuada defensa cibernética.

El objeto de este Trabajo de Fin de Máster es el de que entendamos, ante una situación como la que estamos viviendo, qué sucede cuando un Estado ataca, mediante el uso de la red, a otro Estado. Si Internet es anónimo, ¿cómo se pueden atribuir los ciberataques, por ejemplo, a Rusia? Y en caso de que verifiquemos quién es el Estado agresor, ¿cuáles son las consecuencias? ¿Es posible que un Estado responda por estos ataques? Y en el caso de las Organizaciones internacionales, ¿sería ello posible? ¿Cómo?

Estas son algunas de las cuestiones que han motivado este trabajo y a las que trataremos de dar respuesta en sus diferentes apartados, si bien, por lo complicado y actual de la cuestión, no estará centrado en el conflicto ruso-ucraniano, sino que pretende servir de guía ante cualquier eventual uso de la fuerza en el ciberespacio.

1. El ciberespacio: cuestiones generales sobre el quinto espacio

1.1. El concepto de ciberespacio.

Es habitual relacionar el término *ciberespacio* con la ciencia ficción, pues fueron las películas y obras literarias de este género quienes lo popularizaron e introdujeron en un primer momento en la vida de millones de personas, en especial, de la mano de William Gibson en dos de sus obras, *Neuromante* (1984) *y Johnny Mnemonic* (1981)[1]. También es frecuente utilizarlo como sinónimo de *Internet*, aunque es necesario precisar que se tratan de conceptos distintos, pues este último hace referencia a la red informática descentralizada, es decir, a un sistema de redes interconectadas mediante los que se transmite información, mientras que el concepto de ciberespacio es mucho más amplio.

La Real Academia Española define el ciberespacio como "ámbito virtual creado por medios informáticos"[2]. No obstante, se pueden recoger otras definiciones, más complejas y completas, como la que ofrece MOLINA MATEOS al interpretarlo como un "conjunto de interconexiones electrónicas dispuestas en red, que constituye un espacio de relación integrado por componentes de naturaleza material de base tecnológica, de naturaleza inmaterial sustentada en la información y el conocimiento, a través del lenguaje, y de naturaleza antropológica fundamentada en la sociabilidad del ser humano, que ha devenido en medio y procedimiento para prestar servicios y ha generado un nuevo marco espacio-cultural con efectos económicos, políticos, jurídicos, sociales, culturales y de seguridad; que tiene como límites la seguridad, el desarrollo y el respeto a los derechos humanos"[3].

También podemos acoger a otras definiciones, más sencillas y directas, pero igual de globales: es una realidad virtual de la que forman parte los ordenadores, servidores y redes de todo el mundo[4]. Es decir, todo lo que sucede en Internet forma parte del ciberespacio, que es una especie de "lugar" inmaterial, pero el ciberespacio no se reduce a Internet.

Sea como fuere, lo que está claro es que el ciberespacio tiene una dimensión material muy distinta de la de otros espacios tradicionales. Se trata de espacio intangible creado de forma artificial, reconocido en la Cumbre de la OTAN de 2016 en Varsovia como un nuevo dominio de las operaciones, junto con tierra, mar, aire y espacio[5].

Asimismo, distintos Estados han ido asumiendo la realidad de este espacio, como sucede en la Estrategia de Ciberdefensa de los Países Bajos de 2012, que reconoce el

---

[1] COLABORADORES DE WIKIPEDIA. *Ciberespacio*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ciberespacio

[2] REAL ACADEMIA ESPAÑOLA. *Ciberespacio*. Diccionario de la lengua española, 23.ª ed., 2022 [fecha de consulta: 1 de septiembre de 2022]. Disponible en: https://dle.rae.es/ciberespacio

[3] MOLINA MATEOS, J.M. Aproximación jurídica al ciberespacio. *Boletín del Instituto Español de Estudios Estratégicos,* nº 57*,* 2015. Disponible en: https://www.ieee.es/temas/ciberseguridad/2015/DIEEEO57-2015.html, p. 3

[4] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio.* Navarra, Aranzadi, 2020. ISBN 978-84-1346-719-1, p.16.

[5] OTAN. *Comunicado de la Cumbre de Varsovia. Emitido por los Jefes de Estado y de Gobierno que participan en la reunión del Consejo del Atlántico Norte en Varsovia,* 9 de julio de 2016. . Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en, párrafo 70.

interés del Ministerio de Defensa en operar en el dominio digital[6], así como la Estrategia de Seguridad Nacional de Reino Unido de 2010, que reconoce el valor del ciberespacio en las interconexiones con sus aliados[7][8]

A diferencia de los otros espacios, la delimitación física del ciberespacio es, cuanto menos, difusa, y en él solamente actúa el ser humano mediante la tecnología que él mismo crea. Ello implica que el ciberespacio está sometido por completo a la voluntad del hombre, de forma que solo se modificará o evolucionará como este decida, ofreciendo ilimitadas posibilidades.

La falta de barreras o condicionamientos físicos impone un carácter global que permite operar en este espacio a diferentes actores, tanto estatales como no estatales, independientemente de su origen o régimen político. Entre los actores no estatales podemos mencionar a los ciudadanos de a pie, los hackers patrióticos, autores de malware, *cibervándalos* e incluso corporaciones. No obstante, como se analizará más tarde, puede suceder que sean los Estados o las Organizaciones internacionales quienes financien a alguno de estos actores para que sirvan a sus objetivos e intereses, con la evidente intención de dificultar que sea relacionarlos con dicho Estado (u Organización internacional)[9].

A pesar de todas las ventajas que puede proporcionar esta aparente libertad de movimiento, si la unimos a otros factores como el anonimato, la capacidad de actuar de forma simultánea por varios actores y sujetos internacionales (que pueden estar situados en diferentes jurisdicciones) y la rapidez de ejecución de algunas operaciones en la red, aumenta el riesgo de lo que la Estrategia de Seguridad Nacional española de 2019 determina como *ciberamenazas:* "disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos"[10].

---

[6]EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Netherlands*. *The National Cyber Security Strategy.* 2011. Disponible en: https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011, p.8.

[7] UNITED KINGDOM GOVERNMENT. *The national security strategy - a strong Britain in an age of uncertainty.* 2010. Disponible en: https://www.gov.uk/government/news/national-security-strategy, p. 21.

[8] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio, cit.,* pp. 15-16.

[9] GUTIÉRREZ ESPADA, C., *De la legítima defensa en el ciberespacio*. Granada, Comares, 2020. ISBN 978-84-1369-047-6., pp. 25-26.

[10] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD. *Estrategia Nacional de Ciberseguridad, 2019.* Disponible en: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019, p. 23.

1.2. Tipos de ciberamenazas: *ciberguerra* y ciberataques

La Estrategia de Nacional de Ciberseguridad española de 2019 destaca cuatro tipos de ciberamenazas: el ciberespionaje, el cibercrimen, el hacktivismo y las amenazas híbridas, donde incluye las acciones militares, los ciberataques y la manipulación de la información.

Tipos de ciberamenazas que recoge la Estrategia Nacional de Ciberseguridad de España (2019), p. 25.

En primer lugar, el ciberespionaje no difiere en su razón de ser del espionaje tradicional, pero sí de los medios, pues se efectúa a través de Tecnologías de la Información y la Comunicación (TIC), lo que, tal y como se menciona en la Estrategia Ciberseguridad, dificulta la atribución de la autoría. Además, es una amenaza que emiten, mayoritariamente y dada su complejidad, los actores estatales, bien mediante organismos de inteligencia o militares, que actúan mediante *Amenazas Persistentes Avanzadas* (APT), un tipo de *malware* muy sofisticado que permanece por un tiempo prolongado en el sistema de la víctima" de que se trate[11].

En segundo lugar, nos encontramos con la cibercriminalidad, el tipo de amenaza más extendido. Hace referencia al "conjunto de actividades ilícitas cometidas en el ciberespacio que tiene por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas". En función de su naturaleza, autoría, motivación o los daños resultantes, podremos distinguir entre ciberdelito, ciberterrorismo o hacktivismo[12].

En tercer lugar, el *hacktivismo* hace referencia a la fusión entre el hacking y el activismo, esto es, a la utilización de técnicas hackers para causas políticas o sociales[13].

En cuarto lugar, la Estrategia de Ciberseguridad española de 2019 recoge y define las amenazas híbridas como "acciones coordinadas y sincronizadas dirigidas a atacar de

[11] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD., *cit.,* p. 25.

[12] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD., *cit.,* p. 25.

[13] MAYORGA MARTÍN, J.L., Hacktivismo. *Cuadernos de la Guardia Civil: Revista de seguridad pública*. 2014. Nº49 (pp. 37-54), ISSN 1136-4645, p.40.

manera deliberada las vulnerabilidades sistémicas de los Estados democráticos y las instituciones" a través de las acciones militares, ciberataques, operaciones de manipulación, etc. Además, la Estrategia reconoce el uso de Internet, tanto de actores estatales como no estatales, para el desarrollo de capacidades ofensivas en el ciberespacio[14].

Por otra parte, y aunque la Estrategia de Ciberseguridad Nacional de 2019 no la recoge como tal, no podemos dejar de mencionar que, en la actualidad, la *ciberguerra* como una de las amenazas cibernéticas más significativas para la Comunidad internacional. El ciberespacio ha traído consigo un nuevo campo de batalla para las distintas potencias mundiales; se ha consolidado como un dominio estratégico en los conflictos, obligando a los Estados beligerantes a incorporar nuevas formas de actuación e inversión para prevenir y minimizar los daños.

1.2.1. La ciberguerra

Podemos entender la *ciberguerra* como una agresión, mediante sistemas informáticos, promovida por un Estado y dirigida a dañar las capacidades de otro, bien con la intención de imponer alguna condición o para sustraer información, alterar bases de datos o destruir sus sistemas de comunicación[15]. Es, en esencia, el traslado del conflicto al espacio cibernético.

SÁNCHEZ MEDERO recoge, como características de la ciberguerra o guerra cibernética, entre otras, la complejidad, los objetivos limitados, la corta duración, menores daños físicos y también la búsqueda de superioridad de información. No obstante, la más importante de todas es la asimetría, ya que lo relevante en este tipo de conflictos no es la cantidad de medios u ordenadores de los que pueda disponer un Estado, sino que estos sean los indicados y que su empleo resulte lo más efectivo posible[16].

Para poder considerar que estamos en *ciberguerra* y no ante *simples* ataques cibernéticos por parte de Estados, estos deberían afectar a las instalaciones, organismos públicos, centrales nucleares, infraestructuras nacionales, etc., cualquier objetivo que pueda causar daños y pérdidas incalculables[17], aunque en la realidad el objetivo más frecuente es inutilizar o reducir la efectividad de algún sistema o el robo de información.

Entonces, un concepto clave en la definición de ciberguerra es el de *infraestructuras críticas*[18]. En España, estas son definidas por la Ley 8/2011, de 28 de abril como aquellas infraestructuras estratégicas "cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto

[14] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD. cit. p. 25

[15] SANCHEZ MEDERO, G., Los Estados y la ciberguerra. *Boletín de Información del Ministerio de Defensa.* N º317, 2010 (pp. 63-76) ISSN 0213-6864, p. 64.

[16] SANCHEZ MEDERO, G., Los Estados y la ciberguerra, *cit*., p. 64.

[17] SANCHEZ MEDERO, G., Los Estados y la ciberguerra, *cit*., p. 70-71.

[18] Algunos ejemplos de infraestructuras críticas son: las centrales nucleares, aeropuertos, depósitos, embalses o la asistencia médico-hospitalaria. Estas infraestructuras pueden ser tanto públicas como privadas, su calificación responde a la relevancia de los daños que un eventual ataque pudiera provocar en ellas.

sobre los servicios esenciales"[19]. Estas infraestructuras se integran en un Sistema de Protección de Infraestructuras Críticas, que se articula a través de una serie de planes para evitar o minimizar los daños que puedan sufrir estas infraestructuras si sufren algún tipo de ataque cibernético. Además, la Ley 8/2011 creó el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC),

En el ámbito de la Unión Europea (UE), la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[20], es la que establece una serie de criterios para que sus Estados miembros designen las infraestructuras críticas europeas (ICE). Las ICE son aquellas infraestructuras cuya perturbación o destrucción afectaría, al menos, a dos Estados miembros de la UE.

Por otra parte, tanto si hablamos de ciberguerra como de ataques cibernéticos a otros Estados, hemos de resaltar la importancia de dos conceptos: la atribución y la respuesta. Como veremos más adelante, no resulta fácil atribuir una operación cibernética a un determinado sujeto, y menos cuando se trata de Estados, ya que, a diferencia en los conflictos tradicionales, se busca ocultar la identidad de su autor. Ello también implica que sea difícil que el Estado agredido responda, ya que podría malinterpretarse su origen, e incluso podría utilizar un ciberataque como justificación para atacar a otro Estado[21].

Establecer cuándo estamos ante una ciberguerra o guerra cibernética no es sencillo ni está regulado, ya que la cuantificación de los daños que se pueden producir a través del ciberespacio es compleja.

Hasta el momento, el uso de la red para cometer este tipo de ofensivas se ha limitado, mayormente, al espionaje, a dañar sistemas de comunicación, a generar confusión, al robo de información, etc. Acciones que, pese a ser sancionables y en muchos casos, graves, en la práctica no han causado el mismo impacto que las armas tradicionales[22].

Uno de los casos más destacables es el de *Stuxnet,* un software malicioso, un gusano informático que, aprovechando vulnerabilidades en los sistemas operativos, es empleado para atacar infraestructuras críticas. Se mantiene latente en el equipo al que infecta, permitiendo al autor del ataque acceder al programa, extraer información, reprogramar los controles y ocultar los cambios. Fue descubierto en julio de 2010, y es considerada la primera arma cibernética, ya que no se limitó a actuar sobre los sistemas, sino que provocó fallos y daños en plantas de enriquecimiento de uranio en Natanz, Irán[23]. Si bien este

---

[19] ESPAÑA. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado.* 29 de abril de 2011. BOE Nº 102. pp. 43370-43380.

[20] UNIÓN EUROPEA. Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. *Diario Oficial de la Unión Europea*. 23 de diciembre de 2008. DOUE nº345. pp. 75-82.

[21] SAIN G., ¿Qué es la ciberguerra? *Revista Pensamiento Penal,* 2016. Disponible en: https://www.pensamientopenal.com.ar/etiquetas/ciberguerra, p. 2.

[22]SANCHEZ MEDERO, G. La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*. Nº 11, 2010 (pp. 124-133) ISSN-e 1988-2629, p. 129.

[23] FREDERICK RIVADENEIRA, E., Stuxnet, la primera ciberarma. *Revista Marina.* Volumen 133. Nº 951, 2016 (pp. 76-81) ISSN: 0719-4129, p. 76.

ataque afectó entorno al 11% de las centrífugas de Natanz, no se detuvo por completo el enriquecimiento de uranio e Irán pudo reponerse. Si bien Irán acusó a Israel (apoyado por Estados Unidos) de la autoría del ataque, doce años después no ha sido posible atribuir ninguna responsabilidad por ello.

En definitiva, hablar de ciberguerra, aunque es una posibilidad, puede resultar arriesgado, ya que es difícil establecer quién es el enemigo que está detrás de las ofensivas cibernéticas. En cualquier caso, hemos de tener en cuenta que aunque no haya regulación al respecto, es aplicable el Derecho internacional, que regula el uso de la fuerza, como veremos, y el Derecho internacional Humanitario vigente.

Sea como fuere, y aunque también presenta complejidades, lo que sí podemos hacer es intentar estrechar el marco de la responsabilidad de los Estados por el uso de la fuerza para dañar a otros Estados en el ámbito del ciberespacio.

1.2.2. Los ciberataques

Ciberamenaza y *ciberataque* son términos conectados entre sí, si bien el primero hace referencia a la posibilidad de que ocurra un ciberataque.

Para entender el alcance y funcionamiento de las amenazas mencionadas debemos definir qué es un ciberataque. Un ciberataque es cualquier maniobra o acto ofensivo deliberado que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático[24].

El Manual de Tallin sobre el Derecho Internacional aplicable a la Guerra Cibernética (Manual de Tallin o Manual 2.0)[25] define ciberataque como "una operación cibernética, tanto defensiva como ofensiva, de la que puede razonablemente esperarse que cause lesiones o muerte de personas o daños o destrucción de bienes". El profesor GUTIÉRREZ ESPADA, en el marco de los conflictos entre Estados, completa esta definición, añadiendo que se trata de "toda operación cibernética deliberada destinada a vulnerar un sistema crítico para la seguridad nacional, la independencia política o la integridad territorial de un Estado"[26].

Algunos de los tipos de ciberataque más comunes y frecuentes son:

- Ataque de denegación de servicio (llamado también *DoS,* por sus siglas en inglés, *Denial of Service*). Ataca a sistemas o computadoras de forma que su servicio sea inaccesible. Los atacantes saturan o sobrecargan el objetivo con peticiones, agotando el ancho de banda y provocando la ralentización o la inutilización del servicio. Pueden tener origen en múltiples servidores, de forma

[24] COLABORADORES DE WIKIPEDIA. *Ciberataque*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 9 de septiembre de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ciberataque

[25] INTERNATIONAL GROUP OF EXPERTS. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, Cambridge University Press, 2017. ISBN 978-1316630372

[26] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio, cit*., p. 24.

que se distribuye el origen del ataque aunque con un único destino. Esta modalidad se denomina *DDoS* (*Distributed Denial of Service*)[27].

- *Malware*. Se incluye en esta categoría a todo tipo de software malicioso. Algunos de los más conocidos son: los virus (secuencias de código que se reproducen en el dispositivo infectado), los gusanos (como Stuxnet, son capaces de autoejecutarse para explotar las vulnerabilidades del sistema e infectar a otros sistemas o dispositivos), los troyanos (aparentemente inofensivos, se introducen en el sistema para controlar el equipo) o los *ransomware* (secuestran y bloquean el acceso del dispositivo de que se trate, para posteriormente, pedir un rescate para poder recuperar los datos)[28].

- *Phishing*. Se trata de un método de ingeniería social, mediante el cual se engaña a la víctima para que esta, de forma voluntaria, efectúe alguna acción que no quería realizar, como puede ser revelar información confidencial creyendo que es una página de confianza[29].

- Inyección de código. En este tipo de ciberataques, un hacker inserta un código en una red para quebrantar las medidas de seguridad y acceder a bases de datos protegidos, llegando incluso a secuestrar la información de los usuarios[30].

- Fuerza bruta. Es un tipo de ciberataque poco sofisticado utilizado para descifrar claves o usuarios probando ilimitadas combinaciones hasta dar con la correcta[31].

1.2.3. El ciberespacio e *ius ad bellum*

Según los datos publicados en el año 2022, el número actual de usuarios de Internet alcanza aproximadamente los 4.850 millones de personas (el 62,5% de la población mundial)[32]. En el ciberespacio se generan, transmiten y circulan millones y millones de bytes en datos cada día. La ausencia de un espacio físico delimitado, la rapidez, la capacidad de acceder a una cantidad inmensa de información, de mantenernos conectados con el resto del mundo y de establecer estas comunicaciones en tiempo real son algunas de las características que han convertido Internet y el ciberespacio en el medio ideal para la transmisión y almacenamiento de datos.

---

[27] COLABORADORES DE WIKIPEDIA. *Ataque de denegación de servicio*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[28] COLABORADORES DE WIKIPEDIA. *Malware.* Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Malware

[29] COLABORADORES DE WIKIPEDIA. *Phishing*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Phishing

[30] COLABORADORES DE WIKIPEDIA. *Inyección de código*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Inyecci%C3%B3n_de_c%C3%B3digo

[31] COLABORADORES DE WIKIPEDIA. *Ataque de fuerza bruta*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

[32] Datos extraídos de: WE ARE SOCIAL. *Informe Digital 2022*. Disponible en: https://marketing4ecommerce.net/usuarios-de-internetmundo/#:~:text=En%20la%20edici%C3%B3n%202022%2C%20el,(7.910%20millones%20de%20personas).

No obstante, y precisamente en virtud de sus características, el ciberespacio es también un espacio frágil, susceptible de amenazas y ataques por parte de cualquier actor ciberespacial, de forma que cuanto más digitalizado esté un Estado, más vulnerable será[33].

La mayoría de los Estados han adoptado, en sus legislaciones internas, medidas para la prevención y sanción de ataques informáticos, así como otras normas de actuación en el quinto espacio. Sin embargo, cabe preguntarse qué sucede cuando es el propio Estado, el que, bien mediante de un organismo propio o mediante financiación a un tercero, quien actúa en el ciberespacio contra otro Estado. En este punto de la aplicación del *ius ad bellum*, es decir, de la regulación del uso de la fuerza en las relaciones internacionales[34], juga un importante papel el Derecho internacional, y, sobre todo, el Manual de Tallin.

Para entender el interés y relevancia del Manual 2.0 a efectos de nuestro Trabajo de Fin de Máster es necesario remontarse a su origen. En 2007 se produjeron una serie de ciberataques a Estonia que bloquearon las entidades bancarias, los medios de información y organismos públicos de modo masivo. La OTAN decidió crear entonces el Centro de Excelencia para la Ciberdefensa Cooperativa (CCDCOE, por sus siglas en inglés), que a su vez estableció un Grupo Internacional de Expertos compuesto por juristas y expertos técnicos. También participaron como observadores el Comité sobre Ciberespacio de Estados Unidos, el Comité Internacional de la Cruz Roja y la OTAN. Su misión fue establecer un conjunto de reglas, basadas sobre el Derecho internacional, que se pudiese aplicar al ciberespacio: el texto resultante fue el Manual de Tallin.

Se trata de un instrumento de *soft law*, que recopila con gran mérito tanto principios como normas aplicables en la materia, apoyado en el consenso del grupo de académicos, y que ha sido presentado en Londres en marzo de 2013[35]. En cuanto al posible carácter vinculante de las reglas recogidas por este Manual, cabe precisar que, si bien se afirma que no lo son, lo cierto es que algunos autores destilan lo contrario, ya que el Grupo de Expertos trató de codificar normas no escritas de Derecho internacional, y por ende, vinculantes[36].

Existen otros textos o instrumentos que pretenden aportar cierto orden a las actividades en el ciberespacio, a pesar de que no exista un tratado al respecto. El Informe del Grupo de Expertos Gubernamentales creado por la Asamblea General de Naciones Unidas de 2015 determina la aplicación del derecho internacional en el uso de las TIC[37].

---

[33] LLORENS, M.P., Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, vol. XVII, 2017 (pp. 785-816). ISSN 1870-4654, p. 787.

[34] LLORENS, M.P., *cit.,* p. 788.

[35] La versión actual del Manual de Tallin corresponde a una segunda edición, de 2017, de ahí el "2.0". La primera edición constaba de 95 reglas recogidas en dos partes, mientras que la edición de 2017 añade hasta 154 reglas, divididas en tres partes.

[36] GUTIÉRREZ ESPADA, C., *El espacio ultraterrestre y el manual de Tallin 2.0*., Murcia, Ediciones Laborum 2020. ISBN: 978-84-17789-58-9, pp. 69-70.

[37]NACIONES UNIDAS. *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*. A/70/174. 25 de julio de 2015. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False, p.15

También la Comisión Mundial sobre la Estabilidad del Ciberespacio (CMEC)[38], en su informe final de 2019, manifiesta la necesidad de adoptar normas, tanto estatales como no estatales, adhiriéndose al derecho internacional[39]. También la Estrategia de Ciberseguridad española de 2019 aboga por "la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados"[40].

[38] La Comisión Mundial sobre la Estabilidad del Ciberespacio fue un ente creado y apoyado por diversos organismos y ministerios de distintos países cuya misión era la de crear normas diplomáticas de no agresión gubernamental en el ciberespacio. Operó desde febrero de 2017, publicó su informe final en noviembre de 2019 y concluyó sus actividades en diciembre de 2021.

[39] COMISIÓN MUNDIAL SOBRE LA ESTABILIDAD DEL CIBERESPACIO. *Impulsar la estabilidad. Informe 2019,* 12 de noviembre de 2019. Disponible en: https://cyberstability.org/report/, p. 22.

[40] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD. *cit*., p. 39.

2. El uso de la fuerza en el ciberespacio

El ciberespacio, como hemos visto, es un espacio intangible, en el que pueden presentarse múltiples y peligrosas amenazas. Una de ellas, el traslado de los conflictos entre Estados a la red, es una realidad que presenta múltiples particularidades por lo novedoso de la cuestión. Analizaremos a continuación las características y desafíos de la regulación del uso de la fuerza en el ciberespacio.

2.1. El uso de la fuerza: consideraciones generales.

Para evitar que se cometan agresiones internacionales indiscriminadas, el Derecho internacional ha regulado la prohibición del uso de la fuerza contra otro Estado.

El artículo 2.4 de la Carta de las Naciones Unidas (CNU)[41] establece que sus miembros "en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

¿A qué se refiere el artículo 2.4 con el *uso de la fuerza*? Se trata, sin duda, de una prohibición absoluta, de carácter vinculante, que tiene como objetivo proteger a los Estados ante cualquier posible vulneración por parte de otros Estados.

En un principio podríamos entender que el uso de la fuerza a la que se refiere este artículo es lo que activa el derecho a la legítima defensa de los Estados recogida en el artículo 51 de la Carta: "ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales".

No obstante, si observamos con detenimiento el artículo 51 CNU no se está refiriendo a la amenaza o al uso de la fuerza, sino al *ataque armado,* de forma que la cobertura jurídica que aporta la legítima defensa sólo podría activarse en ese caso.

Sobre qué ha de entenderse por ataque armado, la Corte Internacional de Justicia (CIJ), en el asunto *Nicaragua vs. Estados Unidos*, determinó que no sólo se refiere al uso de las fuerzas armadas o militares regulares de un Estado, sino que incluye, también, por ejemplo, el envío de bandas o grupos guerrilleros al territorio del otro Estado[42].

La Corte apoyó tal conclusión en la Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas[43], que define en su artículo 1 la agresión 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 CNU, tal como se enuncia en la presente Definición", estableciendo en su artículo 3 una

---

[41] NACIONES UNIDAS. Carta de las Naciones Unidas, 26 de junio de 1945. Disponible en: https://www.un.org/es/about-us/un-charter/full-text

[42] *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América).* CIJ. Fallo de 27 de junio de 1986. Disponible en: https://www.dipublico.org/116549/caso-relativo-a-las-actividades-militares-y-paramilitares-en-nicaragua-y-contra-nicaragua-nicaragua-contra-los-estados-unidos-de-america-fondo-del-asunto-fallo-de-27-de-junio-de-1986/, párrafos 187-201.

[43] NACIONES UNIDAS. *Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas. A/RES/29/2014, 14 de noviembre de 1974*. Disponible en: https://www.dipublico.org/4071/definicion-de-la-agresion-resolucion-3314-xxix-de-la-asamblea-general-de-las-naciones-unidas/

lista no exhaustiva de actos que se pueden considerar como agresión, como resultan, por ejemplo, los bombardeos, la invasión o ataque de fuerzas armadas, etc. De cualquier forma, hay que tener en cuenta que el Consejo de Seguridad de las Naciones Unidas tiene la potestad para determinar qué acciones constituyen actos de agresión y cuáles no.

Sin embargo, en el mismo fallo, el CIJ rechazó que el envío de armas o apoyo logístico a esos grupos, si bien puede ser considerado uso de la fuerza, y por tanto, prohibido por el artículo 2.4 de la Carta, fuera considerado un ataque armado[44], de forma que no se podría activar la respuesta de la legítima defensa.

Por ende, podemos concluir que no todo uso de la fuerza constituye un ataque armado, al menos en el sentido que recoge el artículo 51 CNU. Es necesario precisar, además, que el hecho de que para la CIJ estas dos conductas, el envío de grupos armados, íntimamente relacionado con el Estado atacante, quien les ha dado instrucciones, y el envío de ayuda logística, que no permite asegurar el control sobre esos grupos, aunque pueda constituir una agresión indirecta, supone graduar los *usos de la fuerza.*

Así pues, la Resolución 3314, artículo 3, letra g), exige que ante el envío por un Estado de grupos armados o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado, estos actos sean de una gravedad equiparable a los actos armados a los que se refiere el artículo 51 de la Carta, no admitiendo un *uso menor* de la fuerza[45].

2.2. Los ciberataques: armas cibernéticas

Tal y como mencionamos con anterioridad, la ciberguerra es una de las amenazas más peligrosas que existen en el ciberespacio. Las TIC impregnan hoy el ámbito militar de prácticamente cualquier Estado desarrollado. En el entorno del ciberespacio, las armas que se utilizan son las *cibernéticas,* en contraposición a las armas *cinéticas* o convencionales.

Entre las características de las armas cibernéticas, nos encontramos con que estas:

- No necesitan un lugar de lanzamiento, pues actúan a través de la red.
- Pueden ser creadas por cualquier persona, en cualquier lugar del mundo.
- Su prevención es muy difícil.
- Suelen ser complicadas de rastrear, ya que se utilizan técnicas de repercusión en diferentes lugares del mundo para aumentar su eficacia y la dificultad de ser detectadas[46].

En nuestra opinión, consideramos que es necesario definir qué se entiende por un arma cibernética es necesario para poder entender si esta puede integrar el contenido y alcance de la prohibición del artículo 2.4 CNU y activa la cobertura jurídica de la legítima defensa. No obstante, no es una tarea fácil: por un lado, debemos plantearnos cuáles son los actos o acciones cibernéticas que se puedan calificar como armas, habida cuenta de que las normas de derecho internacional vigentes no están pensadas para regular

[44] *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América), cit.,* párrafos 187-201.

[45] GUTIÉRREZ ESPADA, C., *De la legítima defensa en el ciberespacio,* c*it.,* pp. 6-8.

[46] GUTIÉRREZ ESPADA, C., *De la legítima defensa en el ciberespacio, cit.,* p. 28

instrumentos no físicos; por otro, de si estas acciones llegan a alcanzar la entidad o gravedad suficiente para constituir amenaza o fuerza armada en el sentido de la CNU.

Si bien no hay consenso ni jurídico ni político sobre la definición del concepto de *arma cibernética* en el escenario internacional, la doctrina ha apostado por distintas tesis:

a) Una concepción autónoma que atiende materialmente al instrumento, que entiende el arma cibernética como un instrumento que provoca daños a través del ciberespacio.

b) Una concepción finalista, atendiendo a la finalidad o los efectos que puede causar la ciberarma. Esta es la opción a la que atiende el Manual de Tallin.

c) Una concepción analógica, que equipara este tipo de armas a las convencionales.

d) La tesis negacionista, que no considera posible calificar una acción cibernética como *arma*, ya sea bien por la ausencia de prácticas interestatales en este aspecto o porque los efectos destructivos no son equiparables a las armas convencionales.

e) La tesis relativista, que aboga por entender que la concepción de arma depende en gran medida del daño o de su uso. Esto es lo que sucede, por ejemplo, con la calificación del desplazamiento de refugiados hacia Europa como el *arma humana* utilizada por ISIS[47].

A nuestro parecer, si algo tienen en común estas tesis doctrinales es que las mismas atienden a la importancia, bien del uso del arma, o bien a la intención con que se usa, contribuyendo a una aproximación funcional del concepto de *arma cibernética*.

Como señalábamos con anterioridad, el ciberespacio no es un espacio físico, como tampoco lo es una acción cibernética, por lo que no solo no es posible asimilarla a un objeto, sino que debemos indagar, precisamente, en su función y finalidad. ROBLES CARRILLO sostiene que: "una acción cibernética puede ser calificada como cibercriminalidad, ciberespionaje, ciberterrorismo o ciberguerra porque un mismo acto puede cumplir todas esas funcionalidades. La adscripción de ese acto dentro de esa tipología depende no sólo del acto mismo sino, también y sobre todo, de los sujetos, el autor y el destinatario, la intención y los efectos"[48].

De la posible multifuncionalidad de una acción cibernética deriva también que no podamos aplicar la distinción tradicional entre *arma* y *arma de guerra*, que, a su vez, parte de la distinción entre actos criminales y acciones bélicas, tradicionalmente atribuibles a individuos o a Estados. En el ciberespacio, no obstante, esta es otra frontera que se desdibuja: puede suceder que sea un particular el que acceda o realice una acción cibernética bélica.

Calificar una operación cibernética como arma cibernética, en el sentido de la prohibición establecida en el artículo 2.4 CNU, dependerá esencialmente de tres elementos: subjetivo (habrá de ser necesariamente una operación atribuible a un Estado

[47] ROBLES CARRILLO, M. El concepto de arma cibernética en el marco internacional: una aproximación funcional. *Boletín Instituto Español de Estudios Estratégicos,* Nº 4, 2016. Disponible en: https://www.ieee.es/contenido/noticias/2016/10/DIEEEO101-2016.html, p. 10-12.

[48] ROBLES CARRILLO, M., *cit.,* p.18.

contra otro Estado), material (aunque no hay consenso al respecto, el ataque ha de ser susceptible de causar algún daño) y teleológico[49].

Es, finalmente, este último elemento el que resulta determinante para calificar una acción cibernética como acción armada. Nos estamos refiriendo aquí a la intención del autor y sus efectos de su acción.

Este componente tampoco está exento de polémica: por un lado, la intencionalidad no entra en el régimen de responsabilidad internacional de los Estados. También habría que determinar cuál es la intención concreta del autor, tanto para definir si estamos efectivamente ante una acción armada como para delimitar su posición jurídica, la cual resulta una ardua tarea, ya que el origen de los ciberataques suele ser anónimo[50]. Por otra parte, los efectos de una acción cibernética, los daños que esta pueda llegar a producir, ayudan a definirla como arma, bien sea en su empleo como uso de la fuerza o ataque armado[51].

2.3. Los ciberataques como ataques armados

Hasta aquí, hemos visto que un acto o acción cibernética podría llegar a ser considerada *amenaza o uso de la fuerza* en el sentido del artículo 2.4 CNU. Pero ¿puede un ciberataque dar derecho a la legítima defensa? Como se ha adelantado, es necesario que estemos ante un *uso de la fuerza* con una entidad suficiente como para equipararse a una agresión o ataque armado en el sentido del artículo 51 de la Carta.

En un principio, equiparar un ciberataque al uso, por ejemplo, de tanques y bombas, podría parecer descabellado, pero lo cierto es que los efectos de las armas cibernéticas pueden ser todavía más devastadores. Por ello, el Manual de Tallin reconoce expresamente la posibilidad de que un ciberataque sea considerado ya no solo uso de la fuerza[52] (y por tanto, prohibido conforme al Derecho internacional), sino también ataque armado. Al respecto, la Regla 71 del Manual recoge que "a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."

En este sentido, en los comentarios a esta regla, el Grupo de Expertos afirmó por unanimidad que algunos ciberataques podrán tener la suficiente gravedad como para ser considerados ataque armado en el sentido de la CNU. Apoyaron esta conclusión en la *Opinión Consultiva sobre Armas Nucleares de 1996* de la CIJ en la que esta determina que la elección de los medios de ataque es irrelevante para determinar si una operación califica como ataque armado, ya que, tal y como determina la CIJ las disposiciones de la

[49] ROBLES CARRILLO, M., *cit.,* p. 14-18.

[50] ROBLES CARRILLO, M., *cit.,* p. 16.

[51] ROBLES CARRILLO, M., *cit.,* p. 17.

[52] Regla 69 del Manual 2.0: "A cyberoperation constitutes a use of force when its scale and effects are comparable to non-cyberoperations rising to the level of a use of forcé".

Carta no se refieren a armas específicas, sino que "they apply to any use of force, regardless of the weapons employed [53].

Así pues, y en consonancia con la sentencia de la CIJ en el caso Nicaragua, se necesitará que una acción cibernética tenga determinada entidad para ser considerada ataque armado, lo que implica un análisis pormenorizado en cada caso.

Entre otros, desde la doctrina[54] se han apuntado los factores que ayudan a determinar cuándo un ciberataque alcanza este nivel, a saber:

a) Gravedad (*severity*). La producción por la acción cibernética causa daños a personas o cosas. Este factor podría llegar incluso, por sí solo, a permitir la calificación de la operación como ataque armado.

b) Inmediatez (*immediacy*). Este factor se refiere a los efectos, es decir, cuando antes se manifiesten, más probabilidades de que se considere que un ciberataque es uso de fuerza.

c) Causación (*directness*). En cuanto a la relación entre el nexo causal entre el ciberataque y sus consecuencias, puede ser un indicio de un uso ilegal de fuerza.

d) Intrusión (*invasiveness*). Si la ciberoperación va dirigida a penetrar en sistemas protegidos de un Estado, es más probable que se considere uso de la fuerza.

e) Cuantificabilidad de efectos (*measurabilty of effects*). Cuanto más cuantificables sean los efectos del ciberataque, mayor probabilidad de alcanzar la entidad necesaria para ser considerado uso de fuerza.

f) Carácter militar (*military character*). Si el ciberataque es vinculable a una operación militar, aumenta la probabilidad de que se considere uso de fuerza.

g) Implicación estatal (*State involvement*). Cuando el ciberataque es vinculable a un Estado, es más probable que se impute el uso de fuerza a ese Estado.

h) Presunción de legalidad (*presumptive legality*). Si la acción cibernética goza de presunción de legalidad (esto es, no está prohibida por tratados o costumbre internacionales) es menos probable que se considere uso de fuerza.

Si bien, tal y como ya hemos advertido, la producción de daños físicos puede generar el derecho de defensa, ya que es el que nos permite identificar rápidamente la *escala* y *efectos* de la acción cibernética, debemos recordar que el ciberespacio no es un espacio tradicional, de forma que no siempre se producirán daños a las personas o cosas. De hecho, si consideramos este criterio como determinante, un ataque al sistema financiero de un país que provoque graves daños en su economía no permitiría invocar el derecho a la legítima defensa. No obstante, algunos Estados, como el Reino Unido[55] y

---

[53] *Opinión Consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares*. CIJ. Opinión Consultiva de 19 de junio de 1996. Disponible en: https://www.icj-cij.org/en/case/95/advisory-opinions párrafo 39.

[54] SALAS CLAVER, J. De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio. *Cuadernos de estrategia,* Nº 201, 2019 (pp. 133-176) ISSN 1697-6924, p. 149.

[55] El Ministerio de Defensa británico incluyó los ataques a su sistema financiero como ejemplo del uso de la fuerza: "Such as a sustained attack against the UK banking system, which could cause severe financial damage to the state leading to a worsening economic security situation for the population". (MINISTRY

Francia[56], recogen la posibilidad de que un ataque a sus sistemas financieros sea considerado uso de la fuerza.

A falta de una regulación específica, y a modo de recapitulación, concluiremos que un ciberataque, cuando alcance un cierto nivel de afectación, bien sea por daños físicos o a sistemas o servicios de un Estado, puede ser considerado uso de la fuerza equivalente a un ataque armado en el sentido del artículo 51 CNU, permitiendo al Estado afectado invocar la legítima defensa, que, de acuerdo con la regla 72 del Manual 2.0, habrá de ser necesaria y proporcional.

OF DEFENCE. *Development, concepts, and doctrine centre*. Cyber Primer. Disponible en: https://www.gov.uk/government/publications/cyber-primer, p. 12).

[56] En el caso de Francia, el Ministerio de Defensa, además de mencionar la posibilidad de que una operación cibernética que no tenga efectos físicos sea considerada uso de fuerza, establece una serie de criterios para poder evaluar el nivel del ataque: "Toutefois, la France n'exclut pas la possibilité qu'une cyberopération dénuée d'effets physiques puisse être également qualifiée de recours à la force. En l'absence de dommages physiques, une cyber-opération peut être considérée comme un recours à la force à l'aune de plusieurs critères, notamment les circonstances qui prévalent au moment de l'opération, tels que l'origine de l'opération et la nature de l'instigateur (son caractère militaire ou non), le degré d'intrusion, les effets provoqués ou recherchés par l'opération, ou encore la nature de la cible visée. Ces critères ne sont, bien entendu, pas exhaustifs. À titre d'exemple, le fait de pénétrer des systèmes militaires en vue d'atteindre les capacités de défense françaises, ou de financer, voire d'entraîner des individus afin que ces derniers perpètrent des cyberattaques contre la France pourrait, ainsi, être qualifié de recours à la forcé" (MINISTÈRE DES ARMÉES, *Droit International appliqué aux opérations dans le cyberespace*. Disponible en: https://www.justsecurity.org/search-results/?searchwp=droit+international+appliqu%C3%A9+aux+operations, p. 6).

3. La responsabilidad por los ciberataques

Una vez tenemos claro cuándo y en qué circunstancias un ciberataque puede constituir un ilícito internacional, hemos de analizar cuándo éste puede generar responsabilidad internacional.

Una de las principales características del ciberespacio es el anonimato. Si bien autoridades y medios de comunicación se han hartado de transmitir al grueso de la población que cualquier acción en la red deja su huella (y de hecho esto no es falso), lo cierto es que en el nivel que operan los actores que pueden realizar una operación cibernética ofensiva contra un Estado, la incógnita, además de una realidad, es un problema añadido a la hora de atribuir responsabilidades.

Con respecto a la generación de responsabilidad, parece claro que los Estados serán responsables de una acción cibernética ofensiva cuando esta les sea atribuible. No obstante, la mayoría de las veces el nexo entre el Estado y el hecho ilícito es difuso y difícil de demostrar; más aun teniendo en cuenta que es habitual que los Estados actúen a través de civiles para evadir la responsabilidad.

Esta vinculación Estado-acción y las dificultades que entraña demostrar la conexión Estado-sujeto no es un inconveniente exclusivo de la acción cibernética, sino que ya se encontraba presente en ataques físicos relacionados con el terrorismo. Pero sí que supone una complicación a mayores, puesto que, si no se demuestra la responsabilidad de un Estado en el ataque, no se podrá activar la legítima defensa del artículo 51 CNU.

Sobre la base de estas consideraciones, en este apartado de nuestro Trabajo de Fin Máster analizaremos, en primer lugar, el supuesto de atribución cuando un Estado actúa a través de sus órganos, y, en segundo lugar, cuándo la actuación de actores no estatales pueden ser imputadas a un Estado.

3.1. La responsabilidad de los Estados.

Curiosamente, los ciberataques sufridos por Estonia en 2007 que motivaron la elaboración del Manual de Tallin 2.0., pese a constituir una primera base para la atribución de responsabilidad internacional por el uso de la fuerza en el ciberespacio, nunca llegaron a ser vinculados a ningún autor en concreto. La atribución es, de hecho, la piedra angular de la responsabilidad, y al mismo tiempo, el requisito más escurridizo.

Antes de comenzar a indagar en las especialidades de la responsabilidad que generan los ciberataques, es preciso mencionar que un Estado puede incurrir en dos grandes tipos de responsabilidades: la que emana de un hecho ilícito que le es atribuible, y la que surge de la realización de actos no prohibidos cuando este produzca daños a terceros.

En lo que aquí nos ocupa, nos interesa la responsabilidad internacional por hechos internacionalmente ilícitos. El gran marco normativo de la responsabilidad internacional lo contiene el Proyecto sobre Responsabilidad del Estado por Hechos Internacionalmente

Ilícitos (PREHII) elaborado por la Comisión de Derecho Internacional (CDI)[57], que fue anexada por la Asamblea General en su Resolución 56/83[58].

El artículo 1 PREHII prevé que de todo hecho internacionalmente ilícito emana responsabilidad internacional, mientras que el artículo 2 conceptualiza el hecho ilícito como una acción u omisión de la que se derivan dos elementos, que tradicionalmente se han conocido como elemento subjetivo y elemento objetivo.

El primero de ellos es la atribución, que requiere que sea un comportamiento por el cual se incumpla la normativa internacional que este actúa a través de sus órganos, bien sean individuales o colectivos, de forma que le sea atribuible dicha actuación.

La CDI recogió una serie de sujetos o agentes por cuyos actos habría de responder un Estado:

a. Sus propios órganos (artículo 4 PREHII). Bien tengan funciones legislativas, ejecutivas, judiciales o de otra índole. Se trata de los órganos estatales más representativos, que tengan esta consideración según el derecho interno de cada estado, bien sean centrales o pertenezcan a entidades públicas territoriales. A este respecto, la CIJ, en el caso Lagrand, ya había condenado a Estados Unidos ya que, si bien la no adopción de medidas cautelares había sido una decisión del Gobernador de Arizona, y como parte de un Estado federal, tenía cierta autonomía, este debía haber cumplido con sus obligaciones con la Comunidad internacional y haber cumplido con el Convenio de Viena sobre medidas cautelares[59].

b. Personas o entidades en el ejercicio de atribuciones del poder público (artículo 5 PREHII) . Las personas, tanto físicas como jurídicas, pueden generar responsabilidad internacional, siempre y cuando se cumplan tres criterios: actúen en el marco de las competencias que les haya autorizado el Derecho interno del Estado en cuestión, sean funciones propias de un poder público y dicho acto se enmarque en esa función pública, no siendo ni privado ni comercial[60].

c. Órganos de otros Estados a disposición del Estado (artículo 6 PREHII). Nos referimos aquí a los mismos sujetos que en el apartado a, pero que pertenezcan a un Estado extranjero, siempre y cuando actúe en las atribuciones propias de poder público que le confiera el Estado receptor.

---

[57] NACIONES UNIDAS. *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones*. A/56/10, 12 diciembre 2001. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F56%2F10(SUPP)&Language=E&DeviceType=Desktop&LangRequested=False

[58] NACIONES UNIDAS. *Resolución 56/83 de la Asamblea General de las Naciones Unidas. A/RES/56/83, de 28 de enero de 2002.* Disponible en: https://www.dipublico.org/4076/responsabilidad-del-estado-por-hechos-internacionalmente-ilicitos-ag5683/

[59] *Caso Lagrand (Alemania contra los Estados Unidos de América)*. CIJ. Fallo de 27 de junio de 2001. Disponible en: https://www.dipublico.org/117214/caso-lagrand-alemania-contra-los-estados-unidos-de-america-cuestiones-de-fondo-fallo-de-27-de-junio-de-2001/ Párrafo 128 en relación con los párrafos 1-12.

[60] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*. *cit.,* p.79.

De otra parte, nos encontramos que la CDI recoge en el Proyecto otros supuestos en los que un Estado puede responder por hechos llevados a cabo por sujetos que no son ni sus órganos ni los de otro Estado puesto a su disposición:

d. Órganos y personas y entidades extralimitadas en sus funciones (artículo 7 PREHII). Se considerará atribuible a un Estado las actuaciones de estos sujetos cuando, aun excediéndose en sus funciones, estén actuando en la condición de poder público.

e. Sujetos particulares o colectivos bajo la dirección o control del Estado (artículo 8 PREHII) .

f. Personas o grupos de personas que actúen por cuenta del Estado en ausencia de autoridades oficiales (artículo 9 PREHII)

g. Personas que actúan en el marco de movimientos insurreccionales (artículo 10 PREHII).

Además, en virtud del artículo 11 PREHII, cualquier comportamiento que no se encuadre en los supuestos anteriores, podrá ser atribuible a un Estado siempre y cuando este lo reconozca y adopte como propio.

En relación con ello, nos gustaría señalar que, en cuanto a la responsabilidad que puede emanar por actuaciones en el ciberespacio, el Manual de Tallin 2.0 sigue los mismos criterios para poder imputar a un Estado una acción u operación cibernética; nos estamos refiriendo a sus reglas de 15 a 17. Así, la regla 15[61] del Manual hace referencia a los artículos 4 y 5 PREHII, imputando a un Estado las ciberoperaciones llevadas a cabo bien por sus órganos o por personas con poderes públicos[62]. Por su parte, la regla 16[63] acoge la misma premisa que el artículo 6 del Proyecto de la Comisión. Por último, la regla 17[64] acoge la responsabilidad en caso de que el ciberataque lo causen actores no estatales que sigan las instrucciones o estén bajo el control efectivo[65] de un Estado, así como la que generan aquellas ciberoperaciones que el Estado reconozca como propias.

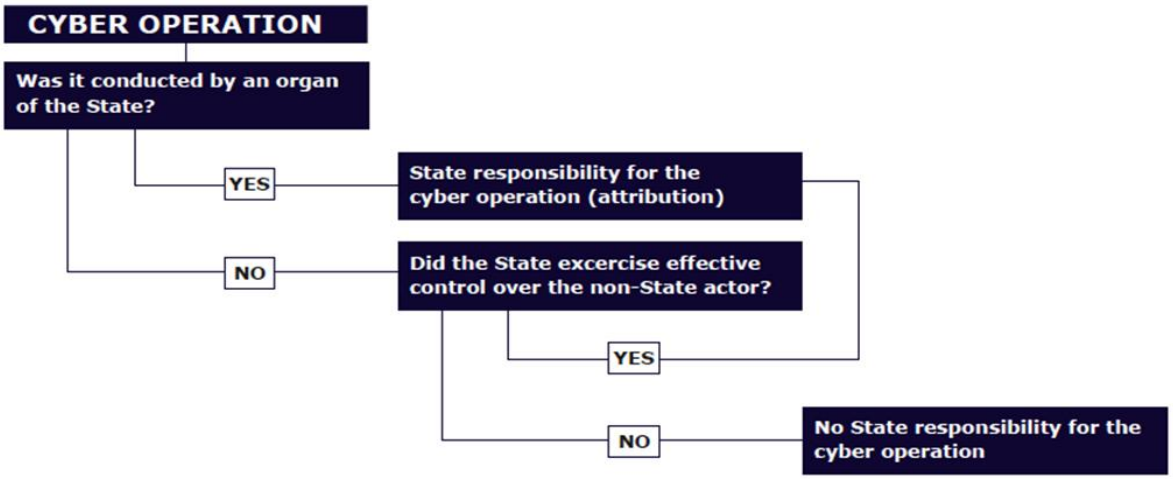
[61] Regla 15 del Manual de Tallin: "Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State".

[62] En ambos casos se incluyen los supuestos *ultra vires*.

[63] Regla 16 del Manual de Tallin: "Cyber operations conducted by an organ of a State that has been placed at the disposal of another State are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the State at the disposal of which it is placed".

[64] Regla 17 Manual de Tallin: "Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own".

[65] El Grupo de Expertos del Manual de Tallin, en el comentario 7, ejemplifica este control *efectivo:* "considérese el caso de que un Estado planea y supervisa una operación de actualizaciones de software para implantar nuevas vulnerabilidades en el software ampliamente usado por otro Estado en sus ordenadores gubernamentales. El anterior Estado concierta un contrato confidencial para compartir los resultados con la compañía que reproduce el software y entonces dirige el proceso para ponerlo en práctica". En este caso, la conducta sería imputable al Estado que ejerce el control. Véase: INTERNATIONAL GROUP OF EXPERTS *, cit.,* p. 96.



Esquema de la atribución de la responsabilidad a un Estado. Fuente: *WIETEKE THEEUWEN, LL.M. Attribution for the purposes of State responsibility.* Ministerie van Defensie, *2018. Disponible en: https://puc.overheid.nl/mrt/doc/PUC_248325_11, p. 9.*

3.2. El caso de los actores no estatales

Tal y como advertíamos, en el caso de los actores no estatales, la regla general es que los Estados respondan sólo por los actos de sus órganos, de personas o entidades en el ejercicio de atribuciones de poder público o de órganos de otros Estados puestos a su disposición. De hecho, el régimen actual de la CNU no permite activar la legítima defensa del artículo 51 ante actores no estatales, aunque, como veremos, hay excepciones cuando estos sujetos actúan bajo el control efectivo de un Estado, pues la actuación del particular le sería imputable.

El Proyecto de Artículos de 2001 de la CDI recoge ciertas excepciones en las que los Estados pueden responder por actos de particulares cuando estos actúan por su cuenta o bajo su dirección o control, ante la ausencia de autoridades (y se hacen cargo de competencias del poder público y ante movimientos insurreccionales.

En esencia, el Derecho internacional recoge que un Estado puede responder por hechos de entes privados o particulares cuando haya una específica vinculación de forma que se considere responsable, pero resulta interesante detenerse en los dos supuestos que recoge el artículo 8 PREHII, relativo a las personas o grupo de personas que actúen por instrucciones o bajo la dirección y control.

En primer lugar, estaríamos hablando del supuesto en que un Estado instruye o contrata a algún tipo de persona privada, a un hacker, para llevar a cabo cualquier tipo de actuación.

En segundo lugar, nos encontramos con el caso en que aquellos sujetos actúan bajo la dirección o control. El grado de control o influencia exigible para que pueda nacer la atribución de responsabilidad de un Estado ha sido objeto de controversia jurisprudencial,

con dos posiciones mayormente enfrentadas: la tesis del control *efectivo* y la del control *global o general*[66].

La tesis del control efectivo nace en el Caso de las actividades militares y paramilitares en Nicaragua y contra Nicaragua. La CIJ determinó que, si bien Estados Unidos influía en las actuaciones de los *contras,* no podía imputarse todo acto:

"Pese a los considerables subsidios y otras formas de asistencia que les proporcionaban los Estados Unidos, no hay pruebas claras de que los Estados Unidos ejercieran realmente en todos los ámbitos un grado de control suficiente para justificar que se considerara que los contras actuaban por cuenta de los Estados Unidos... Todas las formas de participación de los Estados Unidos antes mencionadas, e incluso el control general por el Estado demandado sobre una fuerza que depende en gran medida de ese Estado, no implicarían por sí solas, sin pruebas adicionales, que los Estados Unidos dirigieron u ordenaron la perpetración de los actos contrarios a los derechos humanos y el derecho humanitario que denuncia el Estado demandante. Es muy posible que esos actos hayan sido cometidos por miembros de los contras sin el control de los Estados Unidos. Para que ese comportamiento dé lugar a la responsabilidad jurídica de los Estados Unidos, debería en principio probarse que ese Estado ejercía un control efectivo de las operaciones militares o paramilitares en el curso de las cuales se cometieron las presuntas violaciones"[67].

De otra parte, la tesis del control *general* fue defendida en varias ocasiones por el Tribunal Penal Internacional para la Antigua Yugoslavia, que consideró que la tesis del control *efectivo* no era apropiada en relación con las actuaciones de grupos organizados y estructurados, ya que en estos casos bastaba un control general (facilitando así la atribución de responsabilidad), no siendo necesario que, además de apoyo logístico y equipamiento (pues sí debe haber cierta colaboración) se impartan instrucciones u órdenes por parte del Estado controlador al grupo[68].

No obstante, la CIJ rechazó el criterio del control *general o global*, ya que no considera que esta tesis sea adecuada para imputar a un Estado comportamientos de unidades paramilitares que no forman parte de su sistema militar, al abarcar supuestos demasiado ajenos al principio de que un Estado responde por su propio comportamiento[69].

En el caso de los ciberataques, y dada la especialidad del ciberespacio, si bien no existe consenso, la doctrina apuesta mayoritariamente por la tesis del control *efectivo* dado el sinfín de supuestos por los que un Estado habría de tener que responder[70].

---

[66] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio, cit.,* p. 83.

[67] *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América), cit*., párrafos 109-125.

[68] *Caso Duško Tadić*. TPIY. Fallo de 15 de junio de 1999. Disponible en: https://www.icty.org/en/case/tadic/

[69] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio, cit.,* pp. 84-85.

[70] LLORENS, M., *cit*., p. 100.

3.3. La responsabilidad internacional por complicidad

Si bien en el Derecho Internacional rige el principio de que un Estado responde sólo por sus propios actos (vistas las excepciones ante actores no estatales), debemos analizar qué sucede ante la posibilidad de que un Estado sea *cómplice* en un ciberataque lanzado por otro Estado.

El Proyecto de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos de la CDI regula tres supuestos en los que esta *complicidad* puede dar lugar a responsabilidad en relación con hechos de otros estados: la ayuda o asistencia (artículos 16), la dirección y control en la comisión del hecho (artículo 17) y la coacción (artículo 18). En los tres casos se exige, como requisitos, que el hecho de que se trate sea internacionalmente ilícito y que el Estado que ayuda, controla o coacciona actué conociendo las circunstancias del hecho.

El Grupo de Expertos Gubernamentales de Naciones Unidas también reconoce, en su Informe de 2015, la complicidad en el uso de las TIC, al señalar que ningún Estado debería apoyar de forma deliberada actividades en ese ámbito contrarias a las obligaciones internacionales que puedan ocasionar daños en infraestructuras fundamentales o en sistemas de información de equipos autorizados[71].

En el ámbito concreto del ciberespacio, el Manual 2.0 recoge en la regla 18 los supuestos que describe el PREHII. Ambos textos distinguen entre tres figuras: la ayuda, la dirección o control y la coacción para cometer un hecho ilícito.

En los últimos dos supuestos, el Estado que dirige o controla o que coacciona, además de hacer frente a la responsabilidad que nace de esa cooperación, también tendrá que responder por el ciberataque que realice el otro Estado.

En cuanto a la ayuda que describe el artículo 16 PREHII, es, probablemente, la figura o el caso más recurrente en la realidad, dadas las complejidades técnicas de la informática. Son numerosos los virus y ataques de los que se ha especulado que tengan su origen en una *colaboración* entre dos o más Estados (presentado, por ejemplo, la capacidad tecnológica, el uso de redes, etc.).

Si la ayuda o asistencia en la comisión de un ilícito internacional de otro Estado es tan determinante que sin ella no se hubiese cometido, el Estado que presta esa ayuda podría responder por dos ilícitos: el que deriva de la ayuda o *complicidad*, y el que comete formalmente el Estado que recibe la ayuda (pues el Estado víctima puede dirigirse a cualquiera de los dos)[72].

3.4. Las dificultades de la atribución de la responsabilidad internacional

Después de determinar los principales sujetos por los que un Estado puede llegar a incurrir en responsabilidad, debemos prestar atención a una cuestión que no es baladí: la dificultad ya no solo de identificar a ese mismo sujeto, sino también de atribuirle la responsabilidad.

---

[71] NACIONES UNIDAS. *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, cit.,* párrafo 13, letras f y k.

[72] GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza en el ciberespacio, cit., p*. 102-103

Si bien cada año que pasa, gracias a una mejora exponencial de la tecnología, la identificación del origen de un ciberataque se hace más precisa (por ejemplo, a través de la identificación de la dirección IP), también los ciberataques son cada vez más sofisticados.

Los atacantes suelen ocultar sus identidades y dispersar el origen de sus ataques para hacer que parezcan causados por múltiples sujetos. Averiguar de dónde proceden los ataques es una tarea difícil y costosa que no tiene por qué conducir al autor material del ilícito, y aún más compleja será la tarea de vincular la operación con un Estado.

Por si fuera poco, la comunidad internacional tampoco ha logrado llegar a un consenso sobre la prueba necesaria para imputar un ataque cibernético, ni sobre si esta atribución debiese ser pública[73]. A este respecto, un Grupo de Expertos Gubernamentales sobre la Evolución del Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de las Naciones Unidas determinó que: "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated"[74].

Debemos tener en cuenta, además, que para que un Estado pueda ejercitar la legítima defensa, se han de cumplir ciertos requisitos, los cuales terminan por exigir que se haya reunido material probatorio suficiente.

Hay algunos casos muy conocidos en los que la falta de prueba de que un Estado es responsable de una acción cibernética ha permitido su impunidad. Es el caso del ciberataque Stuxnet, cuando Irán sufrió una serie de ciberataques que causaron daños significativos en sus centrales nucleares. Irán llegó a señalar a Israel como autor, pero la falta de pruebas impidió depurar responsabilidades. En este caso, incluso, podríamos estar ante un uso de la fuerza en el ciberespacio, pero lo cierto es que las mencionadas dificultades para practicar la imputación han permitido que los autores no sufran las consecuencias.

A nuestro entender, son dos, por tanto, las grandes dificultades de la atribución de un ciberataque a un Estado.

La primera de estas cuestiones es técnica, y la misma deriva de las propias características del ciberespacio: el anonimato y la ausencia de barreras físicas. tal y como mencionábamos con anterioridad, es relativamente fácil ocultar la identidad y el origen de una operación cibernética, pero además, el quinto espacio se trata de un ente libre de jurisdicción, por lo que se incrementa la posibilidad de implementar nuevas técnicas sin restricciones y de dispersar el origen de la ofensiva por todo el mundo.

Además de incrementar el riesgo de confusión a la hora de atribuir la responsabilidad, detectar un ataque cibernético lleva más tiempo que identificar un ataque

[73] BANKS, W., Cyber Attribution and State Responsibility. *International Law Studies*, vol. 97, Nº 1, 2021 (pp. 1040-1068) ISSN 2375-2831, p. 1046.

[74] NACIONES UNIDAS. *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional., cit,,* p.13.

cinético, lo que incide en los requisitos de inmediatez y necesidad requeridos para poder invocar la legítima defensa por el Estado víctima[75].

Un ejemplo es el conocido ciberataque WannaCry[76], un *ransomware* detectado en mayo de 2017, que afectó a miles de dispositivos en cerca de 150 países. El Departamento de Justicia de Estados Unidos señaló a Corea del Norte como el autor del ciberataque, en septiembre de 2018.

Estados Unidos, un país líder en desarrollo e innovación tecnológica, tardó meses en analizar el ataque y poder hacer una atribución segura de la responsabilidad. No obstante, de haberse tratado de un caso de uso de la fuerza, no podrían invocar la legítima defensa para actuar al respecto, ya que no se cumpliría el requisito de la inmediatez[77].

La segunda de las cuestiones que dificulta la atribución de la responsabilidad internacional es de naturaleza jurídica y se refiere a los actores no estatales que, actuando en el ciberespacio, generan responsabilidad internacional a un Estado.

La ausencia de soberanía y jurisdicción, la facilidad de acceso, la velocidad y disponibilidad hacen que lanzar una ofensiva cibernética tenga un bajo coste para particulares, de forma que son el tipo de ciberataque más frecuente. No obstante, como hemos visto, no es posible invocar la legítima defensa ante ataques de individuos. Por si fuera poco, si ya de por sí es técnicamente laborioso encontrar el origen de un ciberataque y atribuirle un autor material, rara vez se podrá demostrar la vinculación de este sujeto con un Estado: sería necesario demostrar el control *efectivo*.

Si bien esta tesis, como ya se ha comentado, parece la más acertada a aplicar en el caso de los ciberataques, también se discute que pueda llegar crear un umbral de atribución demasiado alto, pues demostrar la vinculación en un espacio en el que impera el anonimato es extremadamente difícil, por lo que muchas operaciones ofensivas quedarían (y en la práctica, quedan) impunes, llevando a los Estados víctima a actuar fuera del marco legal para defenderse[78].

Bajar el umbral, por otra parte, podría llevar a la imputación errónea, con las peligrosas consecuencias que ello acarrearía, sobre todo en casos de uso de la fuerza en el ciberespacio, ya que el Estado víctima podría activar la legítima defensa.

Lo que sí parece claro es que en el ámbito de la atribución de los ciberataques hay más incógnitas que respuestas, y dada su relevancia y actualidad, es necesario que la comunidad internacional establezca en consenso los pasos y requisitos para poder probar la atribución.

---

[75]FINLAY, L.; PAYNE, C. The attribution problem and cyber armed attacks. *American Journal of International Law*, vol. 113, 2019 (pp. 202-206), pp. 203-204.

[76] *WannaCry* es un ciberataque dirigido a redes corporativas de todo el mundo que utilizaban el sistema Microsoft Windows. Este programa secuestró y cifró los archivos de dispositivos a escala mundial, que solo descifraba a cambio de un pago en moneda Bitcoin. Entre otras, afectó a empresas del calibre de Iberdrola, Telefónica y Gas Natural en España, afectando también al sistema de salud pública de Rein. Unido. Consúltese: COLABORADORES DE WIKIPEDIA. *Ataques ransomware WannaCry*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry).

[77] FINLAY, L; PAYNE, C. *cit.,* p. 204

[78] FINLAY, L; PAYNE, C. *cit.,* pp. 205-206.

4. Las consecuencias internacionales de los ciberataques

Una vez definido qué es un ciberataque, cuando éste es considerado uso de la fuerza y cuándo un Estado puede incurrir en responsabilidad por él, es necesario analizar las posibles consecuencias de sus actos en el ciberespacio.

Si bien en el Derecho internacional se han ido regulando distintas instituciones y mecanismos para dar respuesta a este tipo de afrentas, lo cierto es que en materia de *ius ad bellum* en lo referente a su aplicación en el ciberespacio, como hemos visto, no hay un marco de actuación definido, sino que habrá de analizarse caso por caso.

4.1. La legítima defensa

La legítima defensa es una institución tradicional del Derecho internacional, presente también en los ordenamientos jurídicos internos de los Estados, de naturaleza tanto convencional como consuetudinaria. En su vertiente convencional, es un derecho que se puede ejercitar tanto individual como colectivamente, reconocido por las Naciones Unidas y recogido por esta organización internacional en 1945 en su Carta, que permite repeler conforme a Derecho ataques ilegítimos de otros Estados.

En caso de que una ciberoperación ofensiva sea considerada ataque armado, se abre la posibilidad a que el Estado víctima invoque la legítima defensa que recoge el artículo 51 CNU y a tenor del cual: *"*Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales".

Según la redacción de este precepto de la Carta, son tres criterios los que un Estado debe cumplir: en primer lugar, es necesario la constatación de un ataque armado previo; en segundo lugar, la legítima defensa ha de ser provisional y subsidiaria a las medidas del Consejo de Seguridad de las Naciones Unidas; y, en tercer lugar, la respuesta del Estado víctima debe ser comunicada inmediatamente al Consejo de Seguridad.

4.1.1. Los requisitos de la Carta de las Naciones Unidas

En primer lugar, los criterios que permiten identificar cuando un ciberataque alcanza la suficiente entidad para poder considerar que estamos ante un ataque armado en el sentido de este artículo ya han sido analizados en con anterioridad, por lo que nos limitaremos ahora a recordar que la producción de daños físicos, si bien puede ser determinante para que una acción cibernética ofensiva goce de esta calificación, no siempre será necesaria.

En cuanto a la necesidad de que el ataque armado sea *previo* a la actuación de defensa, analizaremos ahora la posibilidad de una legítima defensa *preventiva* o *anticipada.*

Si bien la CNU no la reconoce de forma expresa, en el caso de los ciberataques el Grupo de Expertos decidió incluirla en el Manual 2.0. Así, la regla 73 del Manual de

Tallin, reconoce la legítima defensa anticipada ante la amenaza de un ataque cibernético no materializado[79], aunque requiere que su producción vaya a ser inmediata. Ello nos parece especialmente relevante en el escenario internacional y en el estado de desarrollo del actual Derecho internacional.

El artículo 51 de la Carta activa la legítima defensa en caso de que *ocurra* un ataque armado, es decir, cuando este ataque ya se ha materializado o está a punto de causar daños, es decir, cuándo ya se ha lanzado. Debemos cuestionarnos, entonces que implica la legítima defensa anticipada o *preventiva,* esto es, una respuesta armada anterior a la producción del ataque[80]

La mayoría del Grupo de expertos entendió que, si bien la Carta no menciona la defensa anticipada, un Estado puede actuar desde que un ciberataque es inminente. Basaron esta postura en el concepto de *inminenci*a articulado en el siglo XIX en Estados Unidos por el Secretario del Estado Webster, tras el *incidente Caroline*, según la cual la legítima defensa se aplicará solo cuando la necesidad de defenderse sea abrumadora, sin dejar elección de medios ni ningún momento para deliberar.

No obstante, en cuanto a la anticipación, las opiniones del Grupo de Expertos son diversas. Por un lado, un enfoque requiere que el ataque armado esté *a punto* de lanzarse, de forma que se impone un estricto análisis temporal.

Del otro lado, un Estado podrá incluso actuar en legítima defensa *preventiva* contra un ciberataque cuando el atacante esté *comprometido* a lanzar el ataque, de forma que si el Estado víctima no actúa de inmediato, perderá la oportunidad de defenderse de forma efectiva. Es decir, en este caso la cuestión determinante no es la proximidad temporal de la acción defensiva al ataque, sino que la falta de esa defensa en un momento concreto diera lugar a que el Estado no pudiera defenderse efectivamente cuando suceda realmente el ataque[81].

En opinión del profesor GUTIÉRREZ ESPADA ambas posturas son válidas y habrá que atender a cada caso en concreto, de forma que, teniendo en cuenta la evolución y rapidez de la tecnología, si un Estado está planeando un ataque de forma que su producción esté decidida, bien sea por el tiempo o porque espera la mejor oportunidad de ataque, cuando el Estado víctima active la legítima defensa (bajo su propio riesgo), esta habrá de aceptarse[82].

En segundo lugar, es necesario que el ciberataque sea atribuible a otro Estado para poder activar la legítima defensa. Si bien este es un criterio que no aparece mencionado expresamente en la Carta, para poder ejercer este derecho es necesario atribuir el ataque a un Estado. No obstante, como se comentó en el apartado relativo a la atribución, puede suceder que sea un actor no estatal el que lance la operación, en cuyo caso será necesario que se demuestre el nexo entre el Estado y ese sujeto[83].

---

[79] Regla 73 del Manual de Tallin: "The right to use forcé in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy*".*

[80] GUTIÉRREZ ESPADA, C. *De la legítima defensa anticipada en el ciberespacio, cit.,* p. 9.

[81] INTERNATIONAL GROUP OF EXPERTS. *cit.,* pp. 350-354.

[82] GUTIÉRREZ ESPADA, C. *De la legítima defensa en el ciberespacio, cit.,* p. 45-47.

[83] En el contexto de la creación de la Carta de las Naciones Unidas (1945), se planteó la legítima defensa como un derecho a ejercer en conflictos entre Estados. En la actualidad, los particulares pueden operar

El tercer requisito de la legítima defensa del artículo 51 CNU está compuesto de dos elementos: la provisionalidad y la subsidiariedad de la defensa hasta que el Consejo de Seguridad adopte las medidas necesarias para mantener la paz.

Las medidas que puede adoptar el Consejo de Seguridad son tres: medidas provisionales (artículo 40 CNU), medidas que no implican el uso de la fuerza (artículo 41 CNU) y medidas que impliquen el uso de fuerza armada (artículo 42 CNU).

Una cuestión controvertida es cuándo se considera que el Consejo ha adoptado las medidas necesarias, momento en el que dejaría de estar activa la legítima defensa. En relación con ello, cabe señalar que, el 2 de agosto de 1990, Iraq invadió parte del territorio de Kuwait, por lo que el Consejo de Seguridad exigió a Iraq su retirada del territorio. Como era de esperar, Iraq hizo caso omiso, por lo que el Consejo adoptó sanciones (que se irían ampliando) contra el Estado iraquí el 6 de agosto. Finalmente, el 29 de noviembre, el Consejo de Seguridad de las Naciones Unidas autorizó el uso de la fuerza de otros Estados para obligarle a retirarse. En ese momento fue crucial el debate acerca de si esas medidas constituían las necesarias para mantener la paz, o si durante ese período el Estado de Kuwait había podido actuar dentro de la legítima defensa.

Si bien en la primera resolución del Consejo de Seguridad en la que se adoptan las sanciones a Iraq se había reconocido el derecho de legítima defensa en respuesta al ataque armado del Iraq contra Kuwait, varios Estados (entre ellos, Rusia, Italia y Cuba) se opusieron a la consideración de que el Consejo de Seguridad no había tomado aún las medidas adecuadas, y que, de hecho, autorizar el uso de la fuerza de otros Estados se ampara en la legítima defensa colectiva, por lo que la respuesta no habría de ser solo de los países contra los que se cometió la ofensa, sino de toda la comunidad internacional representada en el Consejo de Seguridad[84].

El cuarto y último requisito que recoge la CNU es la obligación de informar al Consejo de Seguridad. Al igual que la provisionalidad y subsidiaridad, tiene carácter procesal, pero en este caso es una exigencia posterior a la actuación del Estado víctima, por lo que no implica que de no cumplirse, no exista un efectivo derecho a defenderse.

4.1.2. La legítima defensa en el Manual de Tallin

En el concreto ámbito del ciberespacio, el Manual de Tallin 2.0. recoge la legítima defensa individual en la regla 71, mientras que la regla 74 reconoce la legítima defensa colectiva.

La primera de ellas ya fue mencionada en el apartado relativo al uso de la fuerza, ya que esta regla reconoce expresamente que un ciberataque puede alcanzar el nivel de ataque armado, de forma que activa el derecho inherente a la legítima defensa, de acuerdo con lo dispuesto en la CNU.

En cuanto a la regla 74, esta determina que la legítima defensa puede ejercitarse de forma colectiva sólo "at the request of the victim State and within the scope of the request". Es decir, el Estado que presta ayuda sólo puede actuar con el consentimiento y

también en conflictos internacionales, a través de, por ejemplo, ofensivas terroristas, pero para que pueda operar la legítima defensa del artículo 51 CNU debe vincularse a un Estado.

[84] REGUEIRO DUBRA, R. *La evolución del concepto de legítima defensa en Derecho Internacional contemporáneo*. Tesis doctoral, Universidad Complutense de Madrid, 2012. pp. 100-103.

en los términos que consienta el Estado víctima, que puede, por ejemplo, limitar esta asistencia al uso de armas no cinéticas o a una defensa pasiva. Además, el ejercicio de legítima defensa colectiva puede ejercerse tanto en base a un acuerdo o tratado previo como en un arreglo *ad hoc*, como resulta ser el caso de los Estados miembros de la OTAN[85].

Por otra parte, y también en consonancia con la CNU, la regla 75 también recoge la obligación de reportar las medidas adoptadas en el ejercicio a la legítima defensa ante ciberataques al Consejo de Seguridad de las Naciones Unidas.

4.1.3. Los principios de necesidad y proporcionalidad

Si bien la CNU no los recoge, ante la legítima defensa es necesario el respeto a dos principios básicos: los principios de necesidad y de proporcionalidad.

De hecho, ambos forman parte del Derecho consuetudinario, reconocidos en importantes sentencias de la CIJ, como en la mencionada del caso *Nicaragua*[86] o en el caso relativo a las *plataformas petrolíferas (la República Islámica de Irán contra los Estados Unidos de América*)[87].

En el caso de los ciberataques, el Manual de Tallin 2.0 recoge los dos principios en la regla 72[88].

La *necesidad*, según el Grupo de Expertos, requiere que el uso de la fuerza sea preciso para repeler con éxito un ataque armado inminente o que ya se está produciendo, y si bien ello no implica que la fuerza sea la única vía, sí que las medidas alternativas sean insuficientes. La clave para analizar la necesidad es que las otras opciones, bien sean cibernéticas o cinéticas, sean capaces de evitar la acción ofensiva sin alcanzar el nivel del uso de la fuerza. Además, es también imprescindible que este principio se analice desde la perspectiva del Estado víctima, en atención a sus circunstancias[89].

De otra parte, la *proporcionalidad* arrastra consigo un problema, ¿cuál es el nivel de fuerza permitido, una vez se ha constatado la necesidad de su uso? Este requisito determina la escala, el alcance, la duración y la intensidad de la respuesta en la legítima defensa. Además, para el Grupo de Expertos, la proporcionalidad tampoco requiere que

---

[85] INTERNATIONAL GROUP OF EXPERTS. *cit.,* pp. 339-340.

[86] *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América)., cit.,* párrafo 176.

[87] *Caso de las plataformas petroleras (La República Islámica de Irán contra los Estados Unidos de América) CIJ.* Fallo de 6 de noviembre de 2003. Disponible en: https://www.dipublico.org/117284/plataformas-petroleras-la-republica-islamica-del-iran-contra-los-estados-unidos-de-america-fallo-de-6-de-noviembre-de-2003/ , párrafos 73-77.

[88] Regla 72 del Manual de Tallin 2.0: "A use of force involving cyber operations undertaken by a Estate in the exercise of its right of self-defence must be necessary and proporcionate".

[89] El Grupo de Expertos ejemplifica la necesidad en el caso de que un Estado A ciberataque las infraestructuras de un Estado B, después de que intentar negociar la detención de los ataques sin éxito. El Estado B decide defenderse lanzando ciberataques al Estado A. Sin saberlo, el Estado A ya había detenido sus ataques, pero como la necesidad debe de ser observada desde la perspectiva del Estado víctima, en este caso, el Estado B, no se afectado su derecho a la legítima defensa. (Véase: INTERNATIONAL GROUP OF EXPERTS. *cit.,* pp. 348-349.

la defensa tenga la misma naturaleza que el ataque armado, de forma que un arma cinética podría responder a un ciberataque y viceversa.

Lo importante, entonces, es determinar cuando el ejercicio de la legítima defensa se encuadra dentro de los límites que marcan estos dos principios. Así pues, puede suceder que la acción defensiva sea mayor que la atacante, de forma que habrá de determinarse la licitud de la defensa en base a su aptitud para evitar el mal. De hecho, el Estado víctima podría llegar incluso a ejercer la fuerza en el territorio del Estado atacante, al menos hasta que el Consejo de Seguridad de las Naciones Unidas actúe para protegerlo[90].

No podemos utilizar los mismos niveles y criterios para todos los ciberataques, es necesario analizar caso por caso. Así pues, podría suceder que un Estado atacase a otro de forma sucesiva, pero de manera que ninguna de las acciones ofensivas tuviese por sí sola entidad suficiente. La doctrina de la acumulación de eventos defiende que esta sucesión de ataques de baja intensidad permitan invocar la legítima defensa del artículo 51 CNU, sobre todo cuando estos permitan anticipar o prever un futuro ataque[91].

4.1.4. La legítima defensa en otros textos convencionales

Por último, hemos de mencionar que la legítima defensa es una figura que no sólo ha sido reconocida en la CNU, sino que también aparece en otros textos convencionales, como resulta ser el proyecto de la CDI y el Tratado del Atlántico Norte (TAN). Como hemos visto en apartados anteriores, el lanzamiento de una operación cibernética ofensiva puede dar lugar a responsabilidad internacional, pero la legítima defensa puede conformar una causa de exclusión de la ilicitud del hecho.

Así pues, el Proyecto de la CDI establece en el artículo 21 que: "la ilicitud del hecho de un Estado queda excluida si ese hecho constituye una medida lícita de legítima defensa tomada de conformidad con la Carta de las Naciones Unidas". En los comentarios a este artículo, la Comisión matiza que, no obstante, la legítima defensa no excluye la licitud en todos los casos o respecto a todas las obligaciones.

De otra parte, la OTAN también reguló la legítima defensa colectiva en el artículo 5 del TAN, en el que las partes convienen que un ataque a cualquiera de ellas se considerará un ataque dirigido contra todas, de forma que "cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 CNU, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte".

Así pues, haciendo expresa referencia al derecho reconocido por la CNU, en virtud de lo dispuesto en este artículo , cuando nos encontremos ante un ciberataque que cumpla con los requisitos ya vistos, un Estado miembro de la Alianza podrá invocar ya no sólo actuar amparado en el marco de las Naciones Unidas, sino que, además, podrá recabar la ayuda para su defensa de alguna de las otras Partes firmantes.

Este artículo ha de completarse con el artículo 4 TAN, según el cual: "las partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la

[90] BERMEJO GARCÍA, R.; DÍAZ LÓPEZ JACOISE, E., *La ciberseguridad a la luz del jus ad bellum y el jus in bello,* Navarra, Eunsa, 2020. ISBN 978-8431335427, pp. 85-86.

[91] BERMEJO GARCÍA, R.; DÍAZ LÓPEZ JACOISE, E., *cit,* pp. 86-87.

independencia política o la seguridad de cualquiera de las Partes fuese amenazada", de forma que se permitiría consultar cuándo una ciberataque puede constituir una amenaza a la seguridad. Lo cierto es que sobre si se ha puesto en práctica este artículo, se ha discutido que los debates del Consejo del Atlántico Norte acerca de los ataques a Estonia en 2007 caigan bajo su umbral (aunque el Consejo no lo haya admitido)[92].

El amparo en esta legítima defensa es una decisión política y propia para cada Estado parte de la OTAN. De hecho, la única ocasión en la que han respondido al amparo de este artículo fue tras el ataque terrorista del 11S en Estados Unidos[93]. Además, la concreta posición de la OTAN resulta muy ambigua en cuanto a si este deber de asistencia a las partes opera en el ciberespacio. No obstante, entre las armas no convencionales está cada vez más extendida la idea de que el uso de armas en el ciberespacio puede activar esta legítima defensa[94]. En cualquier caso, decidir si un ciberataque, como arma no convencional, activa el artículo 5 TAN corresponderá al Consejo de Seguridad de la Alianza.

Y por último, la legítima defensa colectiva también aparece recogida en los Tratados de la Unión Europea, a través de una cláusula de asistencia, cuya activación solicitó por primera vez Francia tras los atentados de París de 2015. Esta cláusula figura en el artículo 42 apartado 7 TUE: "si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas".

La aplicación de este artículo es automática (pues no necesita un acuerdo previo) y la ayuda requerida no será necesariamente militar, pero deberá ser coherente con los compromisos adoptados en el marco de la OTAN.

Asimismo, también se regula una cláusula de solidaridad en el artículo 222 del Tratado de Funcionamiento de la Unión, según el cual la UE y sus miembros actuarán conjuntamente si un Estado miembro es víctima de un ataque terrorista o víctima de otro tipo de catástrofe, movilizando incluso los medios militares de los Estados miembros. En este caso, la actuación es colectiva en todo caso, y constituye una suerte de cláusula que permite operar a los Estados miembros ante amenazas no convencionales.

De la lectura de estos dos artículos podemos desprender que la cláusula de asistencia del TUE permitiría a los Estados Miembros actuar en caso de ciberataques que alcancen el nivel y la gravedad que exige la Carta, mientras que la cláusula de solidaridad podría operar en casos en los que un ciberataque no alcance la entidad requerida.

4. 2. Las contramedidas

Otra vía a la que puede acudir el Estado agredido por un ciberataque, tanto si este adquiere la fuerza necesaria para poder ser considerado ataque armado como si no, es a las *contramedidas*: es decir, podrá incumplir sus obligaciones internacionales con el Estado atacante en consecuencia o como reacción a su ofensiva. Es una causa de exclusión

[92] HAUBLER, U. Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO. *International Cyber Security Legal & Policy Proceedings,* 2010 (pp. 100-125), pp. 104-105.

[93] HAUBLER, U., *cit*., p.108.

[94] OTAN. *Análisis y Recomendaciones del Grupo de Expertos Sobre un Nuevo concepto Estratégico para la OTAN,* 17 de mayo de 2010. Disponible en: https://www.nato.int/cps/en/natohq/topics_85961.htm, p. 9.

de la ilicitud, siempre y cuando las medidas que el Estado víctima adopte no entrañe el uso de fuerza[95].

Tanto la CIJ como la CDI legitiman las contramedidas (también entendidas como *represalias[96])* siempre y cuando se cumplan con una serie de condiciones.

La primera de estas condiciones es la existencia de un hecho ilícito[97]. Es necesario volver a resaltar aquí que no todas las operaciones en el ámbito del ciberespacio que afecten a otros Estados son hechos ilícitos, como el ciberespionaje[98].

La segunda de estas condiciones es cumplir con una serie de requisitos de carácter procesal que la CDI recogió en el artículo 52 PR:

> - Haber requerido previamente al Estado infractor que cese o repare la violación de sus obligaciones internacionales.
> - Notificar al Estado responsable cualquier decisión de tomar contramedidas y tratar de negociar con ese Estado (a menos que sea urgente tomar las medidas).
> - No iniciar o suspender las contramedidas en caso de que el ilícito que las originó haya cesado o si la controversia está sometida a un tribunal cuyas decisiones sean vinculantes para las partes. Este último requisito no aplica si el Estado que violó la obligación no actúa de buena fe en la resolución de las controversias.

La tercera de las condiciones para no incurrir en la ilicitud de las contramedidas es la proporcionalidad (artículo 51 PREHII). Esta es una condición que en el ámbito del ciberespacio se complica. Si bien es razonable esperar que un Estado que ha sido víctima de un ciberataque reaccione, por ejemplo, enviando algún tipo de malware para inutilizar o contrarrestar los dispositivos donde se ha producido el ataque, las consecuencias de esta respuesta también pueden ser impredecibles y difíciles de controlar: el malware se puede propagar sin control, o en el caso de ataques cuyo origen sea disperso (por ejemplo, en caso de ataques DoS) afectar incluso a dispositivos situados en el propio Estado víctima[99].

---

[95] NACIONES UNIDAS. *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones*, *cit.,* comentario Nº1 al artículo 22, p. 183.

[96] Tal y como señala la CDI en el comentario Nº 3 al artículo 22, este término ya no se utiliza, debido a su asociación con el uso de represalias bélicas que entrañan uso de la fuerza. Véase: NACIONES UNIDAS. *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones*., cit., comentario Nº3 al artículo 22, p.183.

[97] Por ejemplo, en el asunto *Proyecto Gabcikovo-Nagymaro,* la CIJ analizó si las contramedidas adoptadas por Eslovaquia contra Hungría eran legítimas ya que deben adoptarse en respuesta a un hecho internacionalmente ilícito cometido anteriormente por otro Estado. Caso *Proyecto Gabcikovo-Nagymaro (Hungría contra Eslovaquia*). CIJ. Fallo de 25 de septiembre de 1997. Disponible en: http://www.worldcourts.com/icj/eng/decisions/1997.09.25_gabchkovo.htm, párrafos 83-85.

[98]ROSCINI, M. World Wide Warfare. Ius ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law,* Vol. 14, 2010. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1683370, p. 113.

[99] ROSCINI, M., *cit*., p. 113-114.

4.3. El Consejo de Seguridad de las Naciones Unidas

Otras de las posibilidades que tiene un Estado víctima de un ciberataque es acudir al Consejo de Seguridad de las Naciones Unidas, según el artículo 35 CNU[100] para el arreglo de la controversia o conflicto.

El Consejo, en virtud de lo dispuesto en el artículo 36 CNU, recomendará a las partes implicadas los procedimientos o métodos de resolución de conflicto que estime necesarios (mediante la negociación, la investigación, mediación, arbitraje, etc.) para el arreglo pacífico del conflicto.

El Consejo también puede establecer cuando una situación es una amenaza a la paz, quebranta la misma o constituye una agresión en virtud del artículo 39 CNU[101] y establecer las medidas que estime necesarias. Estas medidas que fueron mencionadas al estudiar la legítima defensa, que recordemos, tiene carácter provisional a la decisión del Consejo de Seguridad.

La adopción de una u otra medida dependerá de las circunstancias de cada caso. Si el Consejo califica un ciberataque como una amenaza a la paz, podría adoptar medidas bajo el artículo 40 a fin de evitar que la situación se agrave, o incluso medidas que impliquen o no el uso de la fuerza (artículos 41 y 42 CNU).

En particular, resulta especialmente útil en el caso de los ciberataques la disposición del artículo 41, acerca de las medidas que no impliquen el uso de la fuerza armada para hacer efectivas las decisiones del Consejo, que especifica "podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas". Ello faculta al Consejo a imponer un *ciberbloqueo* por parte de los Estados miembros al Estado responsable de un ataque para evitar que produzca o continúe con los daños[102].

4.4 Los tribunales internacionales

Por último, una posible vía a la que puede acudir un Estado víctima de un ciberataque, una vez identificado el Estado responsable, es a los tribunales internacionales. La idea es obtener la reparación por los daños causados por el Estado atacante que infringe tanto el artículo 2.4 CNU como el principio de no intervención[103].

Los daños causados a través del ciberespacio por los que puede responder un Estado no son fáciles de cuantificar. Ya cuando hablamos de utilizar los daños como medida para calificar un ciberataque como uso de la fuerza nos encontramos que, al no tratarse de un espacio tradicional, y ante la ausencia de regulación, un ataque a un sistema financiero

[100] El artículo 35 CNU, apartados 1 y 2, distingue dos situaciones, dependiendo de si el Estado es miembro o no de las Naciones Unidas. En caso de no serlo, sólo podrá "llevar a la atención del Consejo de Seguridad o de la Asamblea General toda controversia en que sea parte, si acepta de antemano, en lo relativo a la controversia, las obligaciones de arreglo pacífico establecidas en la Carta".

[101] Artículo 39 CNU: "El Consejo de Seguridad determinará la existencia de toda amenaza a la paz, quebrantamiento de la paz o acto de agresión y hará recomendaciones o decidirá qué medidas serán tomadas de conformidad con los artículos 41 y 42 para mantener o restablecer la paz y la seguridad internacionales"

[102] ROSCINI, M. *cit.,* p.111.

[103] ROSCINI, M. *cit*., p. 111.

podría considerarse que no tiene la suficiente gravedad como para activar la legítima defensa, pero ese tipo de lesiones encuentran en los tribunales internacionales una posible reparación.

Entre los tribunales internacionales a los que se puede acudir destacaremos la CIJ, establecida en 1945 por la CNU y principal órgano judicial de las Naciones Unidas. Este tribunal tiene dos tipos de procedimientos: contencioso y consultivo Pueden ser parte en el primer tipo tanto los Estados firmantes del Estatuto de la CIJ (entre ellos, y como resulta lógico, todos los Estados Miembros de las Naciones Unidas) y aquellos que acepten su jurisdicción[104].

Según el Reglamento de la CIJ, artículo 40.1, la solicitud de incoación de procedimiento (la demanda) "deberá indicar la parte que la hace , el Estado contra quien se proponga la demanda y el objeto de la controversia", por lo que es imprescindible que, antes de acudir a este tribunal, hayamos identificado con éxito un ciberataque al Estado demandado.

Ha de tenerse en cuenta que los tribunales internacionales tienen jurisdicción limitada para obligar a los Estado a cumplir con sus fallos, dado que las partes deben someterse a aceptar sus sentencias. En el caso de la CIJ, a través de acuerdos especiales o *compromisos,* tratados o convenciones vigentes o mediante la *cláusula facultativa* prevista en el artículo 36.2 del Estatuto de la CIJ, anexado a la CNU, según la cuál un Estado reconoce como obligatoria de forma inmediato y sin convenio especial la jurisdicción de la CIJ respecto de cualquier otro Estado que haya suscrito alguna declaración aceptándola[105].

Por último, un Estado u Organización internacional puede acudir a la Asamblea General o el Consejo de Seguridad para que soliciten a la CIJ que emita una Opinión Consultiva (artículo 96 CNU) acerca de si un ciberataque infringe el Derecho internacional, aunque es discutible la fuerza o el carácter obligatorio de las Opiniones de la CIJ. Si bien difieren de las sentencias en que carecen de fuerza obligatoria según el propio Estatuto, algunos instrumentos internacionales le conceden fuerza vinculante, como la Convención sobre privilegios e inmunidades de las Naciones Unidas[106], que establece en su artículo IX que en la resolución e interpretación de controversias sobre el propio Convenio, la opinión de la CIJ será aceptada por las partes como decisiva[107].

[104] CIJ. *Funcionamiento de la Corte*. Naciones Unidas. Disponible en: https://www.un.org/es/icj/how.shtml

[105] DIEZ DE VELASCO, M. *Instituciones de Derecho Internacional Público*. Madrid, Tecnos, 2009. ISBN 978-84-309-4950-2, pp. 994-995.

[106] ESPAÑA. Instrumento de Adhesión de España a la Convención sobre Privilegios e Inmunidades de los Organismos Especializados, aprobada por la Asamblea General de las Naciones Unidas el 21 de noviembre de 1947. Boletín Oficial del Estado. 25 de noviembre de 1974. BOE Nº 282. pp.23871-23878.

[107] DIEZ DE VELASCO, M., *cit.,* p. 999-100.

Conclusiones

Como hemos ido discerniendo a lo largo de este Trabajo de Fin de Máster, una de las mayores dificultades que se deriva ante el uso de la fuerza en el ciberespacio es la ausencia de regulación a escala internacional. Si bien es cierto que podemos aplicar el Derecho internacional vigente, y que el Manual de Tallin 2.0. arroja luz sobre la materia, como hemos visto, en el quinto espacio no son pocas las cuestiones que aún están por resolver, de las que a continuación, concluiremos algunas:

En primer lugar, cuando un Estado lance una ciberoperación ofensiva a otro Estado será considerada uso de la fuerza, y por tanto, prohibida por el Derecho internacional, cuando sea susceptible de provocar daños físicos, bien a infraestructuras críticas, bien en las cosas o personas, e incluso cuando pueda provocar agravios en su sistema económico o financiero.

No obstante, se requiere que este tenga una determinada entidad, equiparable a un ataque armado en el sentido del artículo 51 CNU, para que pueda llegar a activar la legítima defensa. Recordemos que la Comunidad internacional no ha llegado a establecer unos criterios concretos que nos ayuden a establecer cuando una ciberoperación alcanza esta fuerza, por lo que, hasta el momento, habrá de analizarse caso por caso.

En segundo lugar, es necesario que, antes de que el Estado agredido pueda actuar, se atribuya o impute dicha ofensiva a un Estado, lo cual, teniendo en cuenta la realidad del quinto espacio, su complejidad y el anonimato, no siempre será posible. Además, el Estado puede actuar ya no solo a través de sus órganos, sino también de personas tanto jurídicas como privadas, en cuyo caso, para poder atribuir el ciberataque, será necesario demostrar también el nexo o conexión entre el Estado y los sujetos no estatales.

En tercer lugar, cuando el ciberataque alcance el nivel de ataque armado, y ante el eventual caso de que sea posible atribuir una ciberoperación ofensiva a un Estado, el Estado víctima podrá activar la legítima defensa del artículo 51 CNU. En su defensa, podrá emplear tato medidas cibernéticas como cinéticas, pero siempre con el respeto a los principios de proporcionalidad, necesidad e inmediatez. De igual forma, en el caso de ejercer la legítima defensa colectiva, los Estados que auxilien al Estado agredido deberán respetar los límites que este imponga.

Por otra parte, tanto si el ciberataque ha alcanzado el nivel de ataque armado requerido en el artículo 51 CNU como si no, el Estado víctima podrá responder a través de las contramedidas que regula en PREHII, siempre y cuando no actúe a través del uso de fuerza, o acudir al Consejo de Seguridad de las Naciones Unidas para que intervenga en la controversia estableciendo las medidas que considere necesarias.

Además, ante un ciberataque, el Estado agraviado podrá acudir a los tribunales internacionales, como la CIJ, para buscar que el Estado atacante compense los daños que le haya provocado.

Hasta la fecha, hemos actuado ante los ciberataques (como Stuxnet o WannaCry) de forma improvisada: pero el riesgo de que un Estado sufra un ataque cibernético por parte de otro Estado es real, latente (como ha puesto de manifiesto el conflicto ruso-ucraniano) y cada vez más frecuente.

El Derecho internacional contemporáneo ha ido adaptando su aplicación a las actividades del ciberespacio, pero este no deja de ser demasiado ambiguo para un ámbito con tantas especialidades como es el quinto espacio. Si bien el Manual de Tallin 2.0.

arroja luz sobre la materia, lo cierto es que nos parece cada vez más necesario que la Comunidad internacional formule normas y criterios específicos que permitan prevenir y delimitar un marco de actuación ante este tipo de ofensivas ciberespaciales, para evitar que, en base al halo de incertidumbre que genera el ciberespacio, estos actos queden impunes.

Bibliografía

DIEZ DE VELASCO, M. *Instituciones de Derecho Internacional Público*. Madrid, Tecnos, 2009. ISBN 978-84-309-4950-2.

BERMEJO GARCÍA, R.; DÍAZ LÓPEZ JACOISE, E., *La ciberseguridad a la luz del jus ad bellum y el ius in bello*, Navarra, Eunsa, 2020. ISBN 978-8431335427.

GUTIÉRREZ ESPADA, C., *De la legítima defensa en el ciberespacio*, Granada, Comares, 2020. ISBN 978-84-1369-047-6.

GUTIÉRREZ ESPADA, C*., El espacio ultraterrestre y el manual de Tallin 2.0,* Murcia, Laborum 2020. ISBN: 978-84-17789-58-9.

GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio,* Navarra, Aranzadi, 2020. ISBN 978-84-1346-719.

Artículos y trabajos académicos

BANKS, W., Cyber Attribution and State Responsibility. *International Law Studies*, vol. 97, Nº 1, 2021 (pp. 1040-1068).

FINLAY, L.; PAYNE, C. The attribution problem and cyber armed attacks. *American Journal of International Law*, vol. 113, 2019 (pp. 202-206).

FREDERICK RIVADENEIRA, E., Stuxnet, la primera ciberarma. *Revista Marina*. Volumen 133. Nº 951, 2016 (pp. 76-81).

HAUBLER, U. Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO. *International Cyber Security Legal & Policy Proceedings,* 2010 (pp. 100-125).

LLORENS, M.P., Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, vol. XVII, 2017 (pp. 785-816).

MAYORGA MARTÍN, J.L., Hacktivismo. *Cuadernos de la Guardia Civil: Revista de seguridad pública*. Nº49, 2014 (pp. 37-54).

MOLINA MATEOS, J.M., Aproximación jurídica al ciberespacio. *Boletín del Instituto Español de Estudios Estratégicos,* Nº 57, 2015.

REGUEIRO DUBRA, R. La evolución del concepto de legítima defensa en Derecho Internacional contemporáneo. *Tesis Doctoral, Universidad Complutense de Madrid*, 2012.

ROBLES CARRILLO, M. El concepto de arma cibernética en el marco internacional: una aproximación funcional. *Boletín Instituto Español de Estudios Estratégicos,* Nº 4, 2016.

ROSCINI, M. World Wide Warfare. Ius ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010.

SAIN G., ¿Qué es la ciberguerra? *Revista Pensamiento Penal*, 2016.

SALAS CLAVER, J. De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio. *Cuadernos de estrategia,* Nº 201, 2019 (pp. 133-176).

SANCHEZ MEDERO, G., Los Estados y la ciberguerra. *Boletín de Información del Ministerio de Defensa*. N º317, 2010 (pp. 63-76).

SANCHEZ MEDERO, G. La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*. Nº 11, 2010. (pp. 124-133).

WIETEKE THEEUWEN, LL.M., Attribution for the purposes of State responsibility. *Ministerie van Defensie*. 2018.

Informes, resoluciones y otras publicaciones

COMISIÓN MUNDIAL SOBRE LA ESTABILIDAD DEL CIBERESPACIO. *Impulsar la estabilidad. Informe 2019*. Disponible en: https://cyberstability.org/report/ .

EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Netherlands. The National Cyber Security Strategy. 2011.* Disponible en: https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

MINISTÈRE DES ARMÉES, *Droit International appliqué aux opérations dans le cyberespace*. Disponible en: https://www.justsecurity.org/search-results/?searchwp=droit+international+appliqu%C3%A9+aux+operations

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD. *Estrategia Nacional de Ciberseguridad, 2019*. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.

MINISTRY OF DEFENCE. *Development, concepts, and doctrine centre. Cyber Primer*. Disponible en: https://www.gov.uk/government/publications/cyber-primer)

NACIONES UNIDAS. *Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas.* A/RES/29/2014, 14 de noviembre de 1974. Disponible en: https://www.dipublico.org/4071/definicion-de-la-agresion-resolucion-3314-xxix-de-la-asamblea-general-de-las-naciones-unidas/

NACIONES UNIDAS. *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.* A/70/174. 25 de julio de 2015. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False

NACIONES UNIDAS. *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones*. A/56/10, 12 diciembre 2001. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F56%2F10(SUPP)&Language=E&DeviceType=Desktop&LangRequested=False

NACIONES UNIDAS. *Resolución 5683 de la Asamblea General de las Naciones Unidas. A/RES/56/83,* de 28 de enero de 2002. Disponible en: https://www.dipublico.org/4076/responsabilidad-del-estado-por-hechos-internacionalmente-ilicitos-ag5683/

OTAN. *Análisis y Recomendaciones del Grupo de Expertos Sobre un Nuevo concepto Estratégico para la OTAN*, 17 de mayo de 2010. Disponible en: https://www.nato.int/cps/en/natohq/topics_85961.htm

OTAN. *Comunicado de la Cumbre de Varsovia. Emitido por los Jefes de Estado y de Gobierno que participan en la reunión del Consejo del Atlántico Norte en Varsovia,* 9 de julio de 2016. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

UNITED KINGDOM GOVERNMENT. *The national security strategy - a strong Britain in an age of uncertainty. 2010.* Disponible en: https://www.gov.uk/government/news/national-security-strategy

Legislación

ESPAÑA. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Boletín Oficial del Estado. 29 de abril de 2011. BOE Nº 102. pp. 43370-43380.

ESPAÑA. Instrumento de Adhesión de España a la Convención sobre Privilegios e Inmunidades de los Organismos Especializados, aprobada por la Asamblea General de las Naciones Unidas el 21 de noviembre de 1947. Boletín Oficial del Estado. 25 de noviembre de 1974. BOE Nº 282. pp.23871-23878.

NACIONES UNIDAS. Carta de las Naciones Unidas, 26 de junio de 1945.

UNIÓN EUROPEA. Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Diario Oficial de la Unión Europea. 23 de diciembre de 2008. DOUE Nº345. pp. 75-82.

Jurisprudencia internacional

Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América). CIJ. Fallo de 27 de junio de 1986.

Opinión Consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares. CIJ. Opinión Consultiva de 19 de junio de 1996.

Caso *Duško Tadić*. TPIY. Fallo de 15 de junio de 1999.

Caso Lagrand (Alemania contra los Estados Unidos de América). CIJ. Fallo de 27 de junio de 2001.

Caso de las plataformas petroleras (La República Islámica de Irán contra los Estados Unidos de América) CIJ. Fallo de 6 de noviembre de 2003.

Otros recursos

CIJ. *Funcionamiento de la Corte.* Naciones Unidas. Disponible en: https://www.un.org/es/icj/how.shtml

COLABORADORES DE WIKIPEDIA. *Ataque de denegación de servicio*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

COLABORADORES DE WIKIPEDIA. *Ataque de fuerza bruta*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

COLABORADORES DE WIKIPEDIA. *Ataques ransomware WannaCry*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry

COLABORADORES DE WIKIPEDIA. *Inyección de código*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Inyecci%C3%B3n_de_c%C3%B3digo

COLABORADORES DE WIKIPEDIA. *Ciberespacio*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Ciberespacio

COLABORADORES DE WIKIPEDIA. *Malware*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Malware

COLABORADORES DE WIKIPEDIA. *Phishing*. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 20 de agosto de 2022]. Disponible en: https://es.wikipedia.org/wiki/Phishing

REAL ACADEMIA ESPAÑOLA. *Ciberespacio*. Diccionario de la lengua española, 23.ª ed., 2022 [fecha de consulta: 1 de septiembre de 2022]. Disponible en: https://dle.rae.es/ciberespacio

WE ARE SOCIAL. *Informe Digital 2022*. Disponible en: https://marketing4ecommerce.net/usuarios-de-internetmundo/#:~:text=En%20la%20edici%C3%B3n%202022%2C%20el,(7.910%20millones%20de%20personas)