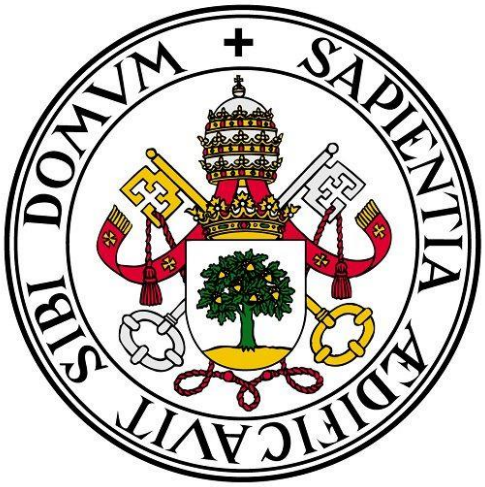

Universidad de Valladolid

Facultad de Ciencias Sociales, Jurídicas y de la Comunicación

Grado en Derecho

Aplicación del Derecho Internacional a las operaciones en el ciberespacio.

Presentado por: **Elena Cosgaya García**

Tutelado por: **María Esther Salamanca Aguado**

Fecha de presentación: **21 de junio de 2024**

Resumen

El ciberespacio ha adquirido en los últimos años un gran protagonismo en nuestras vidas, y en la de los Estados, que han tenido la necesidad de proteger su territorio e infraestructuras frente a los ciberataques. El ciberespacio se ha convertido en el nuevo campo de batalla, con la característica, a diferencia de otros tipos de ataques, de que es difícilmente posible conocer la identidad de aquellos sujetos que están detrás de estos ciberataques y de lo accesible que es el ciberespacio universalmente en comparación con otros campos de batalla.

A pesar de que no existe ningún marco jurídico específico que regule las ciberoperaciones, se aplica el Derecho Internacional ya existente, tomando como referencia el *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations,* obra de gran influencia que tiene como objetivo de estudiar la aplicación de las normas de Derecho Internacional al ciberespacio.

Siguiendo como modelo de referencia el citado Manual de Tallín 2.0, en este Trabajo Fin de Grado se recoge el procedimiento que se debe seguir para aplicar el Derecho Internacional, y el estudio de la posibilidad de atribuir la responsabilidad internacional a tales Estados o a aquellos actores no estatales que realizan ciberataques con la ayuda de los Estados.

Además, no sólo se analiza si resulta de aplicabilidad la legítima defensa frente a ciberoperaciones y los requisitos que deben contener los ciberataques para acogerse a ella; sino que también, al ubicar tales ciberoperaciones en hostilidades se ha procedido el estudio de la protección de los bienes que son objetivo militar de estos ciberataques aplicando también el Derecho Internacional Humanitario.

Palabras clave

Ciberespacio; ciberataques; responsabilidad internacional; legítima defensa; Derecho Internacional Humanitario; Manual de Tallín; hostilidades; uso de la fuerza.

Abstract

In recent years the cyberspace has gained great prominence in our lives, as well as in the lives of states, which have had the need to protect their territories and infrastructures against cyberattacks. Cyberspace has become the new battlefield, with the characteristic, unlike other types of attacks, that it is difficult to know the identity of those individuals behind these cyberattacks and how universally accessible cyberspace is compared to other battlefields.

Although there is no specific legal framework regulating cyber operations, existing International Law is applied, with reference to the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* a highly influential work that aims to study the application of international legal norms to cyberspace.

Following the model of the aforementioned Tallinn Manual 2.0, this TFG not only includes the procedure to follow to apply International Law, but also the study of the possibility of attributing international responsibility to such states or actions carried out by non-state actors with their help, or if legitimate defense applies and what requirements are necessary in cyberattacks to qualify for it; in addition, when locating these cyber operations in hostilities, the protection of assets targeted in these cyberattacks has also been studied by applying International Humanitarian Law.

Keywords

Cyberspace; cyberattacks; international responsibility; legitimate defense; International Humanitarian Law; Tallinn Manual; hostilities; use of force.

INDICE

ABREVIATURAS

PREHII: Proyecto sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos.

CIJ: Corte Internacional de Justicia.

OTAN: Organización del Tratado del Atlántico Norte.

ONU: Organización de las Naciones Unidas.

DIH: Derecho Internacional Humanitario.

CDI: Comisión de Derecho Internacional.

CIJ: Corte Internacional de Justicia.

INTRODUCCIÓN

En las últimas décadas Internet es una parte esencial en el funcionamiento de los Estados y de nuestra propia vida. Los Estados han tenido que buscar soluciones para proteger su infraestructura y territorio del ciberespacio pues este se ha convertido en el nuevo campo de batalla.

Es por este motivo por el que el Derecho Internacional se ha debido de dotar de un nuevo marco jurídico que regule este asunto, pues han sido frecuentes los ciberataques que han sufrido los Estados en los últimos años, motivación que ha conllevado la exigencia a la comunidad internacional de elaborar unas normas para responder frente a ellos.

A pesar de que en la actualidad no existe una norma específica internacional que regule el comportamiento que los Estados deben asumir frente a ciberataques por parte de otros Estados o actores no estatales, se acordó la aplicación por analogía del Derecho Internacional ya existente.

La aplicación del Derecho Internacional común a este ámbito y no uno específico para él ha conllevado una serie de problemas debido a las peculiares características del ciberespacio, pues este espacio no posee fronteras delimitadas ni es fácil descubrir la identidad que se esconde frente a tales ciberataques, por no hablar de lo accesible que es el ciberespacio universalmente en comparación con otros campos de batalla.

Las ciberoperaciones realizadas por Estados que generen un daño grave a otro Estado son objeto de responsabilidad internacional, al igual que si tales ataques ocurriesen a través de otros campos de batalla; sin embargo, cuestión más difícil de analizar son aquellos ciberataques realizados por actores no estatales, en los que aparece la ayuda o autorización de un Estado.

El objeto y finalidad de este Trabajo Fin de Grado es analizar la aplicación del Derecho Internacional al ciberespacio en los diferentes supuestos en los que este aparece envuelto como campo de batalla, concretamente cuando se ve envuelto en hostilidades. Este objeto de estudio no sólo conlleva el análisis del procedimiento que se debe seguir para aplicar el Derecho Internacional, sino también el estudio de la posibilidad de atribuir la responsabilidad internacional a tales Estados o a aquellos que son llevados a cabo por actores no estatales pero con la ayuda de ellos, o si resulta de aplicabilidad la

legítima defensa y qué requisitos hacen falta en los ciberataques para acogerse a ella; sino que también, al ubicar tales ciberoperaciones en hostilidades se ha procedido el estudio de la protección de los bienes que son objetivo militar de estos ciberataques aplicando también el Derecho Internacional Humanitario.

A pesar de que no existe una normativa específica reguladora de los ciberataques, se ha tomado como referencia para este estudio el *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations,* una obra escrita por un Grupo Internacional de Expertos (GIE) con el objetivo de estudiar la aplicación de las normas de Derecho Internacional al ciberespacio.

Es por ello, que el objetivo de mi Trabajo Fin de Grado es elaborar ciertas conclusiones a la elaboración de un marco jurídico a partir del Derecho Internacional específico para el ciberespacio, recogiendo las normas y la forma de aplicación del Derecho Internacional ya existente sobre la defensa de los Estados frente a los ciberataques hasta que la comunidad internacional consiga la unificación de un marco jurídico propio de este ámbito. Para ello me he apoyado no sólo de la obra *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations,* ya mencionada, sino que ha sido de gran ayuda el *Manual de Derecho Internacional Humanitario* aplicable a la guerra aérea, elaborado por el Ministerio de Defensa español, y del que ha sido partícipe Jerónimo Domínguez Bascoy, General Auditor experto en ciberespacio. También ha sido necesario el análisis doctrinal de obras académicas, así como de Asuntos sobre los que se ha pronunciado la Corte Internacional de Justicia a través de los cuales hemos podido sacar ciertas conclusiones mediante la aplicación de la analogía del Derecho Internacional al ciberespacio.

CAPÍTULO 1: CIBERESPACIO, EL NUEVO CAMPO DE BATALLA

1. Ciberespacio: definición y sus capas.

El término ciberespacio empezó a usarse a principios de los ochenta del S. XX por el escritor William Gibson, que lo acuñó para referirse a la red de ordenadores interconectados para unir personas y máquinas en una realidad virtual.

Cabe remarcar la distinción que existe entre ciberespacio e internet, siendo este último aquella red global creada mediante la conexión, a través de protocolos de TCP/IP, de numerosas redes informáticas y servidores, que permiten a los usuarios de éstas el intercambio de datos e información; es decir, internet se caracteriza por ser una infraestructura que existe en el mundo físico.

Sin embargo, el ciberespacio, no es tangible en el mundo físico, es un mundo virtual creado a partir de internet, donde los usuarios intercambian ideas y datos o realizando actividades que hasta hace pocos años sólo eran posibles en el mundo físico.[1]

Fue EEUU, a través de la creación del U.S. Cyber Command, en 2009, el primero que reconoció el ciberespacio como el quinto dominio de las operaciones militares, que se sumó a los campos de batalla terrestre, marítimo, aéreo y ultraterrestre. Posteriormente, en 2013, el Ejército Español creó el Mando Conjunto de Ciberdefensa (MCCD), para abordar los asuntos de los que este trabajo es objeto. Así, lo hizo también la OTAN en su declaración final tras la Cumbre de Varsovia en 2016[2], reconociendo el ciberespacio como un entorno operativo en el que la organización debe defenderse como lo hace en el resto de los campos de batalla.

[1] DOMÍNGUEZ BASCOY, Jerónimo.``Aplicación del derecho internacional a las operaciones en el ciberespacio´´. *Manual de Derecho Internacional Humanitario aplicable a la guerra aérea.* Madrid: Ministerio de Defensa, 2021, 1º ed, p.223

[2] 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*.
https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en, párrafo 70

En nuestro ordenamiento jurídico, se definió por primera vez el ciberespacio tras la Orden Ministerial 10/2013, del 19 de febrero, [3]orden por la cual se creó el MCCD, ``como un dominio global y dinámico compuesto por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de la información''.

El *Manual de Derecho Internacional Humanitario aplicable a la guerra aére*a, del que es referencia este estudio, nos ofrece un concepto del ciberespacio más exacto, entendido este como

> ``el dominio interactivo formado por redes digitales que es utilizado para almacenar, modificar y comunicar información, que incluye internet junto a otros sistemas de información utilizados para el funcionamiento de las infraestructuras, los negocios y otros servicios''.[4]

Para facilitar el entendimiento de este concepto es útil distinguir entre las diferentes capas que el ciberespacio presenta:

- Una capa física, el *hardware*, siendo parte de este aquellos aparatos que forman la infraestructura por la que se crea el ciberespacio. Al tratarse de una capa físicamente localizada, esto permite el ejercicio de poderes soberanos de los Estados donde dicha infraestructura se encuentra ubicada.

- Una capa lógica, o también llamada código, que abarca tanto el *software* como los protocolos que en él se incorporan. En esta capa también hay que destacar que se incluye el *malware*, siendo este aquel *software* malicioso.

- Una capa semántica o de los contenidos, en ella se reúne toda la información creada, capturada, almacenada y procesada en el ciberespacio.

- Una capa social, que la forman todas aquellas personas físicas y jurídicas que actúan en el ciberespacio con su identidad digital.

---

[3] ESPAÑA. MINISTERIO DE DEFENSA. *Orden Ministerial 10/2013, de 19 de febrero por la que se crea el Mando Conjunto de Ciberdefensa*. BOE. 2013.

[4] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 224

2. Ciberoperación y ciberataque

Para diferenciar estos conceptos vamos a empezar por definirlos:

Las ciberoperaciones son unas actividades en las que se emplean capacidades cibernéticas para alcanzar los objetivos que anteriormente nos habíamos planteado bien en el ciberespacio, o a través de él.

Las ciberoperaciones pueden tener consideración de ataque armado si consisten en Ataques a Redes Informáticas para destruir, interrumpir o dañar infraestructuras físicas, u otras infraestructuras que contengan información o redes de comunicación. En cambio, no reunirían los requisitos para ser calificados como ataque armado las Explotaciones de Redes Informáticas ni las Redes informáticas de Defensa.

Una ciberoperación, según sus características, puede ser considerada como una clara evidencia de incumplimiento del artículo 2.4 de la Carta de Naciones Unidas, y constituir por ello un uso de la fuerza prohibido por dicha Carta.

Hay que recordar que este artículo dice que:

> "Los miembros de la Organización, 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"[5].

Por todo esto, lo más importante es la escala y efectos de estas ciberoperaciones y no los medios que se han empleado. Si la escala y efectos son compatibles o similares a los resultados de una operación militar con armas convencionales, químicas, biológicas o nucleares, es lógico que la calificación y consecuencias, desde el punto de vista del Derecho Internacional, deberán ser idénticas.

[5] NACIONES UNIDAS. (1948). *Carta de las Naciones Unidas. Y estatuto de la Corte Internacional de Justicia.Artículo 2.4*. Naciones Unidas, Departamento de Información Pública

El tema principal, por lo tanto, será determinar cuándo una ciberoperación puede ser considerada como ataque armado a los efectos de su calificación jurídica, siendo este un tema todavía muy debatido y sobre el que no existe un consenso establecido.

Jurídicamente, una ciberoperación que causase mortandad en vidas humanas o bien destruyese infraestructuras podría ser respondida con una ciberoperación en las mismas proporciones por el Estado agredido amparándose en el Derecho Internacional contra el Estado agresor, en uso de la facultad que confiere el artículo 51 de la Carta de Naciones Unidas (derecho inmanente a la legítima defensa); o bien, que justificasen la intervención del Consejo de Seguridad de Naciones Unidas en virtud del Capítulo VII de la Carta.

Debe de quedar claro, que sólo se entenderán incluidas en el ámbito de aplicación de las normas del Derecho Internacional Humanitario o *Ius ad Bellum* las ciberoperaciones protagonizadas por Estados o agencias estatales contra otros Estados.

Los cibertaques, aunque sus consecuencias sean catastróficas, si no son llevados a cabo por Estados serán calificados como casos de ciberterrorismo o ciberdelincuencia y la respuesta del Derecho frente a estos ataques se deberá llevar a cabo mediante otros instrumentos jurídicos fuera del ámbito del Derecho Internacional Humanitario y del sistema de Naciones Unidas.

Otra cuestión primordial en esta materia es el derecho a la autodefensa en el ámbito del ciberespacio. Con carácter general, frente a una agresión llevada a cabo mediante ciberoperaciones la respuesta legítima por parte del Estado agredido se debe regir por los principios de necesidad y proporcionalidad, como sucede en el ámbito de los conflictos convencionales. La gran pregunta a hacerse con respecto a esta situación es si esa respuesta debe llevarse a cabo obligatoriamente mediante ciberoperaciones o puede ser utilizando la fuerza militar o acciones de disuasión o amenaza, respetando los principios anteriormente citados de necesidad y proporcionalidad.

Existe un gran vacío en la normativa y regulación jurídica de este nuevo contexto de enfrentamiento cibernético entre Estados. El conocido como Manual de Tallin, elaborado al amparo de la Organización del Tratado del Atlántico Norte (OTAN), es un buen avance desde el punto de vista teórico, pero carece de fuerza de obligar. Por ello, es necesario avanzar hacia la elaboración y

aprobación de un nuevo convenio que forme parte del Derecho de La Haya sobre *Ius in Bello* que regule esta materia.

El ciberataque sería

> ``aquella ciberoperación que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, la degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que lo soportan″ [6];

adquiriendo esta definición un sentido más específico cuando se emplea en el derecho internacional humanitario, como veremos con posterioridad.

También existen otras definiciones del ciberataque como esta que recoge la Estrategia de Ciberseguridad española de 2019: "acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los Estados democráticos y las instituciones" [7].

Otra definición es la que nos ofrece el Manual de Tallin sobre el Derecho Internacional aplicable a la Guerra Cibernética (Manual de Tallin o Manual 2.0) que 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".[8]

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″.[9]

A continuación, nos referiremos a los distintos tipos de ciberataques que han sido identificados en:

---

[6] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 225.

[7] ESPAÑA. MINISTERIO DE DEFENSA. (2013). *Orden pci/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [BOE n. º 103, 30/iv/2019]*, pp. 247-249.

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

[9] GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*, Cizur Menor, Thomson-Reuters Aranzadi, 2020, p. 24.

1. 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 que se distribuye el origen del ataque, aunque con un único destino.

2. 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)

3. 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.

4. 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

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

3. Fases de los ciberataques

Siguiendo el modelo militar de la *kill chain* sobre el que se estructura cualquier operación sobre un objetivo (Find*, Fix, Track, Target, Engage, Assess*), los científicos de la compañía *Lockheed-Martin*,

en 2011, desarrollaron el de la *cyber kill chain* para explicar las sucesivas fases en que se encuentra articulado el proceso de los ciberataques.

Por lo que, a raíz de esta estructura, la primera fase de los ciberataques es la conocida como "fase de reconocimiento", dirigida a la obtención de información sobre el objetivo, a partir de sitios web, redes sociales...

La segunda fase consiste en la creación del arma (*exploit*), adecuando el *malware* al medio con el que se buscará la infección del objetivo de la operación.

La siguiente fase es la del lanzamiento, la cual consiste en la transmisión de ese *malware* a través de algún medio, como, por ejemplo, archivos adjuntos de correo electrónico, sitios web o dispositivos USB.

La cuarta fase, de explotación, se basa en el aprovechamiento de alguna vulnerabilidad en el objetivo o de algún error humano, con el fin de ejecutar el *software* malicioso en el sistema contra el que se dirige el ataque.

En la quinta fase, de instalación, se trata de asegurar que el *software* malicioso podrá ejecutarse de forma permanente en el equipo infectado.

En la última fase se establece el mando y control sobre el sistema atacado, de forma que el atacante pueda manipular este a su gusto de forma remota.

Por último, una vez dentro del sistema víctima del ciberataque, se desarrollan las acciones sobre los objetivos, como, por ejemplo, una denegación de servicio o un robo o manipulación de datos.

4. Aplicación a las ciberoperaciones de las normas internacionales relativas al uso de la fuerza y a la conducción de hostilidades en situaciones de conflicto armado.

En la actualidad ya no existe debate acerca de que el vigente derecho internacional se debe aplicar a las ciberoperaciones con efectos transfronterizos, sin embargo, la comunidad internacional aún no ha alcanzado un consenso sobre la manera en la que han de aplicarse los principios y normas internacionales.

En 2018, a través de su *Attorney General*, el Reino Unido mantiene que, cuando los Estados y los individuos realizan ciberoperaciones hostiles, estas se hallan regidas por el derecho como lo están las actividades realizadas en cualquier otro dominio, lo que significa que los actores hostiles no pueden actuar por medios cibernéticos sin esperar consecuencias; además, de las disposiciones de la Carta de las Naciones Unidas relativas al uso de la fuerza, la aplicación del DIH a las ciberoperaciones ejecutadas durante conflictos armados proporciona tanto protección como claridad. El Reino Unido afirma el derecho de todo Estado a desarrollar una capacidad cibernética ofensiva soberana, lo cual no implica desestabilizar o militarizar el ciberespacio, siendo obligación de cada Estado asegurarse de que su uso y desarrollo tiene lugar en conformidad con el derecho internacional.[10]

Paralelamente, en la Estrategia de ciberseguridad de la UE, «Un ciberespacio abierto, protegido y seguro», de 2013, al hacerse referencia a las prioridades estratégicas y, concretamente, a la relativa a la creación de política internacional coherente del ciberespacio, afirma expresamente que: ¨En su política internacional del ciberespacio, la UE alentará las actividades de elaboración de normas de conducta y aplicará el derecho internacional existente en este campo˝.[11]

Por su parte, la OTAN, en la declaración final tras la Cumbre de Gales de 2014, reconoció que es política de la organización reconocer que ¨el derecho internacional, incluyendo el DIH y la Carta de las Naciones Unidas, se aplican en el ciberespacio˝.

4.1. Programa de las Naciones Unidas

Desde 1998 la seguridad en el ciberespacio ha formado parte del programa de las Naciones Unidas; desde ese momento se ha trabajado en el tema de «Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional», siendo lo más relevante son los informes emitidos por sucesivos grupos de expertos gubernamentales constituidos por diversas resoluciones de la Asamblea General.

[10] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 227.

[11] EUROPEAN COMMISSION. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

Es de gran calado el informe emitido en 2013 [12] por tales expertos que se mantuvieron unánimes en que "la aplicación de normas derivadas del derecho internacional vigente que son pertinentes para el uso de las tecnologías de la información y las comunicaciones por los Estados es una medida fundamental con el fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales", y que "el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías".

En el informe de 2015, que abarca la aplicación del DIH en el ciberespacio, se señala que «existen principios jurídicos internacionales establecidos, incluidos, si procede, los principios de humanidad, necesidad, proporcionalidad y distinción» que son aplicables al uso de las TIC por los Estados.

4.2. El Manual de Tallín

En el plano doctrinal, a la hora de determinar cómo se aplican las normas vigentes internacionales a las operaciones de los Estados en el ciberespacio es la desarrollada por dos grupos extranjeros de expertos, que, por invitación del Cooperative Cyber Defense Center of Excellence de la OTAN, han elaborado las hasta el momento dos ediciones del conocido Manual de Tallin.

La primera edición, redactada en 2013, se centró básicamente en el derecho internacional aplicable a la ciberguerra, esto es a la aplicación en el ciberespacio de las normas relativas al uso de la fuerza (ius ad bellum) y a la conducción de las hostilidades (ius in bello); aspectos que se tratarán en los siguientes capítulos de este trabajo.

La segunda edición, el Manual de Tallin 2.0, publicado en 2017, amplió el alcance de la obra original para abarcar también las reglas aplicables a las ciberoperaciones situadas por debajo del umbral del uso de la fuerza, en la práctica, las más habituales, refiriéndose, más en general, al derecho internacional aplicable a las ciberoperaciones.

4.3. La regulación del derecho aéreo internacional aplicado a las ciberoperaciones

[12] INFORME DEL GRUPO DE EXPERTOS GUBERNAMENTALES sobre *los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional,* Documentos oficiales de la Asamblea General, 70.º periodo de sesiones (A/70/174), pp. 2-20

Según nos explica Duncan B. Hollis [13], existen dos métodos predominantes cuando de lo que se trata es de regular jurídicamente el ciberespacio: a) la creación de normas específicamente adaptadas a las características del ciberespacio; b) la aplicación analógica al ciberespacio de normas jurídicas preexistentes; predominando este último tipo de normas en el Derecho Internacional a la hora de regular el ciberespacio, pues no existe dentro de este derecho una rama especial para la regulación de este ámbito material, debiendo acudir a la analogía de otros contextos para su regulación, siendo la única excepción el Convenio de Budapest sobre la ciberdelincuencia de 2001.

Marco Roscini mantiene que

> ``la ausencia de reglas *ad hoc* no significa que las ciberoperaciones puedan ser conducidas por los Estados sin restricciones. Cita la opinión del Magistrado Simma acerca de que el punto de vista según el cual lo que no está expresamente prohibido se encuentra permitido refleja una visión anacrónica y sumamente consensualista del Derecho internacional, anclada en el principio elaborado por la Corte Permanente en el asunto del Lotus''.[14]

Por ello, dice Roscini, las normas internacionales convencionales y consuetudinarias pueden extenderse por vía interpretativa a las ciberoperaciones no expresamente contempladas en aquéllas.

El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad para la búsqueda de un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías. La soberanía de los Estados y las normas y principios internacionales que de ella emanan son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio. Tras este reconocimiento de que las normas del Derecho Internacional vigente son aplicables al ciberespacio, particularmente las que disciplinan el *ius ad bellum* y el *ius in bello*, lo siguiente que hay que determinar es cómo se adaptan tales normas a las singularidades del ciberespacio y la elaboración más significativa que hasta la fecha

[13] HOLLIS, D. *Derecho Internacional y operaciones cibernéticas del Estado: Mejora de la transparencia*. Rio de Janeiro: Organización de los Estados Americanos. 2020. https://www. oas. org/en/sla/iajc/docs/CJI_doc_603-20_rev1. pdf.
[14] ROSCINI, Marco, *Cyber Operations and the Use of Force in International Law*. Oxford, 2014. p.19

se ha llevado a cabo a este respecto es el que ha plasmado en el conocido como Manual de Tallin sobre el Derecho internacional aplicable a la ciberguerra.

Este Manual, sin embargo, no alcanza a toda aquella ciberactividad que se desarrolla por debajo del umbral del *ius ad bellum*; queda, por tanto, fuera del Manual todo lo relativo a la cibercriminalidad y, por supuesto, la actividad relacionada con otras áreas del Derecho internacional tales como las relativas a los derechos humanos o al derecho de las telecomunicaciones. Así como lo explica Jerónimo Domínguez Bascoy[15], el Manual de Tallin se ha centrado en exclusiva en las ciberoperaciones más perjudiciales y destructivas, es decir, a las que cabe calificar como "ataques armados" y que, por tanto, permiten a los Estados responder en legítima defensa, así como en las que tienen lugar en el curso de conflictos armados.

El Manual de Tallín 2.0 examina la aplicación del derecho aéreo internacional a las ciberoperaciones, centrándose por un lado en la vulnerabilidad de las modernas aeronaves frente a interferencias con los sistemas de control de vuelo o con los instrumentos y sistemas de navegación y comunicaciones a bordo.

Por otro lado, al tiempo que las aeronaves pueden ser el blanco de ciberoperaciones, pueden también ellas mismas ser utilizadas como plataformas desde las que conducir ciberoperaciones o donde albergar ciberinfraestructuras de apoyo a la realización de acciones militares.

Se estudiará este tema siguiendo la explicación que redacta Domínguez Bascoy[16], existiendo tres reglas que parten de la regulación contenida en el Convenio sobre Aviación Civil Internacional y en la Convención de las Naciones Unidas sobre el Derecho del Mar, estas reglas pueden resumirse en:

> «1.ª. Todo Estado puede regular las operaciones de las aeronaves, incluidas aquellas que conducen ciberoperaciones, en su espacio aéreo nacional».

[15] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 230.

[16] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., pp.230-232.

Los expertos señalan sobre esta regla que, durante el vuelo por el espacio aéreo nacional de un Estado, las aeronaves civiles se encuentran sujetas a la plena jurisdicción del Estado, que puede obligarlas a aterrizar en un aeropuerto designado dentro de su territorio cuando se realicen acciones perjudiciales.

Mayoritariamente, las ciberoperaciones son conducidas desde aeronaves militares que, al ser aeronaves de Estado, no pueden sobrevolar el territorio de otro Estado sin autorización de este último; pues, el Estado autorizante podría, haciendo uso de las prerrogativas soberanas que ostenta sobre su espacio aéreo, prohibiendo aquellas ciberoperaciones que no estuvieren relacionadas con la seguridad del vuelo.

Los expertos fueron unánimes al establecer que, si esa aeronave estuviera conduciendo ciberoperaciones que alcanzaran el nivel de ataque armado contra el Estado subyacente, o este tuviera serias razones para concluir que aquella fuera a hacerlo de manera inminente, estaría autorizado a recurrir en legítima defensa a la fuerza necesaria y proporcionada para expulsar a la aeronave de su espacio aéreo.

Sin embargo, no existe unanimidad en los expertos en cuanto a la determinación de que actividades pueden ser calificadas como ataque armado; para el sector minoritario, la mera presencia de una aeronave militar extranjera afectando a los intereses de seguridad nacional del Estado subyacente, sin el consentimiento de este, constituiría per se un ataque armado. Para el sector mayoritario, sin embargo, si bien la presencia de una aeronave militar extranjera conduciendo ciberoperaciones sería, cuando menos, una clara violación de la soberanía del Estado subyacente, este solo podría recurrir a la fuerza si la aeronave estuviera de hecho realizando un ataque armado o tuviera razones para concluir que fuera a hacerlo de modo inminente.

> «2.ª. Con sujeción a las restricciones establecidas en el derecho internacional, todo Estado puede realizar ciberoperaciones en el espacio aéreo internacional»

En relación con esta segunda regla, los juristas comentan en la misma Convención que,

> ``mientras ejerzan los derechos de paso en tránsito aéreo por estrechos internacionales o por vías marítimas archipelágicas, conforme a los artículos 39 y 53 de la Convención de las Naciones Unidas

sobre el Derecho del Mar[17], las aeronaves deberán abstenerse de toda actividad que no esté relacionada con sus modalidades normales de tránsito rápido e ininterrumpido, salvo que resulte necesaria por fuerza mayor o por dificultad grave"[18].

Esta apuntación, viene a decir que no se encuentran autorizados a conducir ciberoperaciones dirigidas contras los Estados que bordean el estrecho o al propio Estado archipiélago; pero, sin embargo, sí podrán conducir ciberoperaciones que constituyen el modo normal de operación de la aeronave, como es la transmisión de ciertos datos.

En cuanto a esta regla, existió unanimidad por parte de los expertos en la materia en que una aeronave que sobrevuele un estrecho internacional o una ruta aérea archipelágica podrá conducir cuantas ciberoperaciones sean precisas para fines de *force protection* o de legítima defensa; además, independientemente de las restricciones que pueda imponer el Estado al que pertenecen, las aeronaves de Estado pueden, en principio, conducir ciberoperaciones en el espacio aéreo internacional en la medida en que no afecten a la seguridad de la navegación de las aeronaves civiles.

Pero a la hora de determinar el abarque del "modo normal de las ciberoperaciones", existe división entre los expertos; el sector minoritario entiende por "modo normal" de operación de las aeronaves diseñadas para conducir ciberoperaciones ofensivas incluye la realización de tales operaciones mientras se hallan en tránsito rápido e ininterrumpido por estrechos internacionales o por vías marítimas archipelágicas, siempre que aquéllas no sean dirigidas contra el Estado o Estados que bordean el estrecho o contra el Estado archipelágico. El sector mayoritario no compartía la anterior opinión de que el modo normal abarque la posibilidad de conducir ciberoperaciones ofensivas.

No hay que dejar pasar por alto que, aunque ha diferencia a diferencia de las aeronaves civiles, las aeronaves de Estado, incluidas las militares, no están regidas por el Convenio de Chicago y, por tanto, pueden conducir ciberoperaciones en el espacio aéreo internacional sin estar sujetas a las instrucciones de control del tráfico aéreo dentro de una región de información de vuelo (FIR),

[17] NACIONES UNIDAS. *Convención de las Naciones Unidas sobre el Derecho del Mar.*(1982). https://www.un.org/Depts/los/convention_agreements/texts/unclos/convemar_es.pdf

[18] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 231.

deberán en todo momento volar velando por la seguridad de otras aeronaves y respetar los derechos de otros Estados, por lo que es frecuente que cooperen con las autoridades de control del tráfico.

Existen ciertos Estados que, para garantizar su seguridad, han establecido zonas de identificación de defensa aérea (ADIZ), extendiéndose esta sobre el espacio aéreo internacional, pudiendo, teóricamente, dichos Estados prohibir la conducción de cierto tipo de ciberoperaciones dentro de la ADIZ como condición para penetrar en su espacio aéreo nacional; sin embargo, en ningún caso podrán tales condiciones interferir con la libertad de vuelo sobre la alta mar.

> «3.ª. Ningún Estado puede conducir ciberoperaciones que pongan en riesgo la seguridad de la aviación civil internacional».

Esta última regla hay que ponerla en correlación el artículo 3 bis del Convenio de Chicago, en el que los Estados parte «reconocen que todo Estado debe abstenerse de recurrir al uso de las armas en contra de las aeronaves civiles en vuelo», mostrándose de acuerdo los expertos en que el término arma comprende las ciberarmas.

Domínguez Bascoy. J, autor del manual de referencia de este trabajo, explica que "estas pueden, en efecto, tener consecuencias destructivas sobre una aeronave en vuelo y las personas a bordo, como ocurriría en el caso de un malware que afectará a los sistemas de control de la aeronave que, sin necesidad de verse físicamente afectados, podrían verse privados de funcionalidad"[19].

La regla general sobre prohibición de conducir ciberoperaciones que pongan en riesgo la seguridad de la aviación civil internacional admite, no obstante, excepciones en aquellos casos autorizados por el derecho internacional, tal como sucede cuando se dan las condiciones para una actuación en legítima defensa.[20]

[19] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 231.

[20] CASANOVAS, O.; RODRIGO, A.J. Compendio de derecho Internacional Público. Madrid: Tecnos, 2017

CAPÍTULO 2: LAS CIBEROPERACIONES Y EL *IUS AD BELLUM*

1. Umbral de las ciberoperaciones y los resultados de aplicar el uso de la fuerza

Como hemos puesto en conocimiento en el capítulo anterior de este trabajo, la legalidad de las ciberoperaciones no es hoy en día objeto de regulación específica a pesar de su gran capacidad para perturbar la paz y la seguridad internacional; es por ello, que se ha visto obligado a examinar las ciberoperaciones desde el marco del *ius ad bellum*, es decir, de aquellas normas internacionales que establecen los requisitos en que es jurídicamente admisible el uso de la fuerza.

En 1996, en la *Opinión consultiva sobre la legalidad de la amenaza o el uso de armas nucleares*[21] que realizó el Tribunal Internacional de Justicia, ya puso de manifiesto que los artículos de la Carta de las Naciones Unidas sobre la prohibición del uso de la fuerza (artículo 2.4) y sobre la legítima defensa (artículo 51) son aplicables «a cualquier uso de la fuerza independientemente de las armas empleadas». Lo mismo fue reiterado posteriormente por el Manual de Tallín[22], explicando que, aunque en vez del uso de un arma tradicional se haga uso de un ordenador durante una operación es irrelevante a la hora de calificar esa operación como un «uso de la fuerza» en aquellos casos en que, a la vista de sus consecuencias, pueda considerarse que la ciberoperación en cuestión ha alcanzado dicho umbral.

Así como manifiesta el artículo 2.4 de la Carta de las Naciones Unidas, aquellas ciberoperaciones que constituyan una amenaza o un uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o que en cualquier otra forma sean incompatibles con los propósitos de las Naciones Unidas, estarán prohibidas.

Existe unanimidad doctrinal en que la expresión ¨uso de la fuerza"[23] se refiere exclusivamente a la fuerza armada, con exclusión de la coerción política o económica, que carece de la potencialidad

[21] CORTE INTERNACIONAL DE JUSTICIA. (1996). *Legalidad de la amenaza o uso de armas nucleares*. https://www.icj-cij.org/case/95/advisory-opinions

[22] SCHMITT, M. N. (Ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013

[23] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., pp.233-234

físicamente destructiva de aquella, como pueden ser ciberoperaciones psicológicas dirigidas a socavar la confianza en un gobierno ni la prohibición del comercio electrónico con otro Estado con el fin de dañarlo económicamente.

Otra aclaración que realiza el Manual de Tallín, es que no es necesario que este uso de la fuerza provenga de las Fuerzas Armadas de un Estado para calificarlo como tal; para ello se apoya en las consideraciones que el Tribunal Internacional de Justicia realizó en el fallo del caso de las actividades militares y paramilitares en y contra Nicaragua (1986), pues, en dicho fallo se dijo, armar y entrenar a una guerrilla que conduce hostilidades contra otro Estado constituye también un uso de la fuerza prohibido por el derecho internacional; del mismo modo que lo sería, en este ámbito de estudio de las ciberoperaciones, el proporcionar a un grupo armado organizado *malware*, instruyéndole sobre cómo utilizarlo, cuando las ciberoperaciones llevadas a cabo por ese grupo contra un Estado con ese malware e instrucción proporcionadas por otro Estado alcanzan el umbral del uso de la fuerza.

Abordando la cuestión de cuándo las ciberoperaciones alcanzan el umbral del uso de la fuerza, se entiende que es el mismo que cuando se usa la fuerza armada por medios tradicionales y producen efectos como son muerte, lesiones, daños o destrucción.

El debate se plantea en relación con aquellas ciberoperaciones que no matan o lesionan a personas ni dañan o destruyen objetos, pero que, sin embargo, causan perjuicios importantes como, por ejemplo, los de naturaleza económica que se producirían en el caso de que mediante una ciberoperación se perturbará gravemente el funcionamiento del sistema bancario de un Estado, más allá de los casos de causación de meras molestias, irritación o inconveniencia, como sucedería con un ataque de denegación de servicio de duración limitada.

En el Manual de Tallin se recogen ciertos criterios que podrían influir a la hora de calificar por los Estados si una ciberoperación es uso de la fuerza.

Así, la severidad de los efectos causados por la ciberoperación, la inmediatez con que se manifiestan tales efectos, la existencia de una relación directa entre el acto inicial y sus consecuencias, el grado de invasividad en los intereses del Estado víctima, la mensurabilidad de los efectos producidos, el carácter militar de la operación, el grado de involucración del Estado en ella y, finalmente, la presunta

legalidad de la ciberoperación, que excluiría su consideración como uso de la fuerza, tal como ocurre con la mera propaganda, las operaciones psicológicas, el espionaje o la simple presión económica.

2. Legítima defensa frente a ciberoperaciones susceptibles de ser calificadas de ataque armado.

2.1 Concepto de ataque armado

La respuesta más acertada que proporciona el derecho internacional a aquellos Estados víctima de ciberoperaciones lesivas para sus intereses es el ejercicio del derecho a la legítima defensa, recogido en el artículo 51 de la Carta de las Naciones Unidas por el cual podrá recurrir ese Estado cuando la ciberoperación en cuestión alcance un nivel tal que permita calificarla como ataque armado 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".[24]

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

[24] NACIONES UNIDAS. (1948). *Carta de las Naciones Unidas. Y estatuto de la Corte Internacional de Justicia. Artículo 51.* Naciones Unidas, Departamento de Información Pública

Unidas; y, en tercer lugar, la respuesta del Estado víctima debe ser comunicada inmediatamente al Consejo de Seguridad.[25]

El primer criterio que ha de concurrir en una ciberoperación para calificarla como ataque armado es que esta tenga un carácter transfronterizo. Esto conlleva que no serán consideradas como ataque armado las ciberoperaciones llevadas a cabo por un grupo de *hackers* que opera dentro de los confines de un Estado contra infraestructuras públicas o privadas emplazadas en ese mismo Estado.

El segundo criterio para calificarlo de ataque armado, la ciberoperación debe producir unos daños que superen un determinado umbral de severidad.

A pesar de ser dominante la opinión que distingue entre uso de la fuerza y ataque armado, los Estados Unidos de América no reconocen tal distinción y así, en el Manual de derecho de la guerra, al tratar de las ciberoperaciones, se afirma que el derecho inmanente a la legítima defensa se puede aplicar contra cualquier uso ilegal de la fuerza, por lo que una ciberoperación que pueda calificarse de tal podrá ser respondida mediante las acciones necesarias y proporcionadas en legítima defensa.[26]

En resumen, estaríamos ante ataques armados cuando las ciberoperaciones de forma directa o indirecta, lesionan gravemente o matan a cierto número de personas, o dañan significativamente o causan la destrucción de propiedades.

Sin embargo, existe debate entre los expertos que redactaron el Manual de Tallín, sobre la calificación o no de ataques armados a aquellas ciberoperaciones que no produjeran los efectos anteriormente descritos pero que sí son las culpables de otras consecuencias negativas. Algunos de estos expertos, mantuvieron que para hablar de ataque armado deben necesariamente concurrir aquellos efectos dañinos o destructivos en personas y bienes. Otro sector de la doctrina no se centra tanto en la naturaleza de tales efectos sino en la extensión de las consecuencias, pudiendo, a su juicio, como ejemplo, calificarse de ataque armado una ciberoperación dirigida contra una bolsa de valores. El

[25] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p.235.

[26] OCHOA-RUIZ. N; SALAMANCA-AGUADO. E, *Exploring the Limits of International Law relating to the Use of Force in Self-defence;* European Journal of International Law, Volume 16, Issue 3, June 2005, pp.499- 524, https://doi.org/10.1093/ejil/chi128

último sector minoritario sostuvo el punto de vista de que las ciberoperaciones dirigidas contra infraestructuras críticas que causan efectos severos, aunque no destructivos, también son susceptibles de ser calificadas de ataques armados.

2.2 Operaciones realizadas por actores no estatales

Otro tema de debate en esta materia, que intentaremos esclarecer en este trabajo según la opinión de los expertos es aquella relativa a si las ciberoperaciones dañinas realizadas por actores no estatales que actúan por su cuenta, al margen de cualquier implicación de un Estado, pueden ser calificadas como ataques armados que generan el derecho a responder en legítima defensa.

Como explica Jerónimo Domínguez Bascoy[27], la opinión sobre este debate se ha visto modificada a partir de 2001, esto es a consecuencia de los ataques del 11 de marzo de tal año por parte de Al Qaeda contra los Estados Unidos. Antes de que ocurriera tal suceso, los actos violentos llevados a cabo por actores no estatales quedaban al margen del ius ad bellum y se denominaban actos criminales a los que se ha hecho frente con el aparato policial-judicial estatal.

Esta opinión se modificó a raíz de los atentados del 11-M de 2001, pues la comunidad internacional lo caracterizó como ataques armados, dando inicio a una práctica proclive a considerar que también cabe ejercer el derecho utilizar la fuerza en legítima defensa frente a ataques de actores no estatales. Los Estados Unidos han dejado clara su postura al respecto, manifestando en el citado Manual de derecho de la guerra, del Departamento de Defensa, que «el derecho de un Estado a adoptar en legítima defensa la acción necesaria y proporcionada en respuesta a un ataque armado originado a través del ciberespacio se aplica tanto si el ataque es atribuible a un Estado como si lo es a un actor no estatal»

2.3 Requisitos del uso de la fuerza para la aplicación de la legítima defensa

[27] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p.236.

Existen unos requisitos que deben concurrir a la hora de ejercitar el derecho a usar la fuerza en legítima defensa frente a ciberoperaciones calificadas como ataques armados, estas exigencias son la inminencia, inmediatez, necesidad y proporcionalidad.

2.3.1 La inminencia

Existe una tendencia generalizada en el derecho internacional que admite actuar en legítima defensa anticipadamente de manera defensiva frente a un ataque armado inminente, sin necesidad de esperar a que este haya ocurrido.

Aunque tradicionalmente, la inminencia ha sido considerada como proximidad temporal en cuanto al ataque armado, en el ámbito de las ciberoperaciones esto no es práctico pues estas pueden ejecutarse en milésimas de segundo.

Es por ello, que la mayoría de los expertos que redactaron el Manual de Tallín descartaron la concepción tradicional basada en el análisis temporal, optando por el estándar de la «última ventana de oportunidad».

Esta concepción de inminencia requiere la confluencia de tres factores: en primer lugar, el posible atacante debe tener la capacidad precisa para lanzar una ciberoperación con el nivel de ataque armado; en segundo lugar, debe haber manifestado su intención de hacerlo, y, en tercer lugar la potencial víctima del ataque estaría autorizada a actuar defensivamente, con fuerza cinética o cibernética, solo hasta aquel punto en que dejar de hacerlo frustraría la oportunidad de defenderse de manera efectiva.[28]

2.3.2 La inmediatez

[28] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 237.

La inmediatez es aquel requisito que nos permite diferenciar un acto de legítima defensa que uno que es una represalia, pues hace referencia al periodo subsiguiente a un ataque armado durante el cual sería lícito responder ante este acogiéndose a la legítima defensa.[29]

Este requisito debe interpretarse con matices, debido a la corta duración que pueden tener los ciberataques, es por eso que, si el Estado víctima pudiera razonablemente concluir que el atacante va a proseguir conduciendo en su contra ciberoperaciones en el nivel de ataque armado, podría considerar las operaciones en su conjunto como una campaña en curso, de forma que estaría legitimado para actuar de forma defensiva en cualquier punto de esta campaña.

También pueden ocurrir situaciones donde se tarde cierto tiempo en percatarse de que se ha producido o está produciéndose un ciberataque, al igual que conocerla identificación del atacante; en estos casos, el Manual de Tallín expresa que en estas situaciones no concurre la inmediatez.

2.3.3 La necesidad

El tercer requisito, engloba que el uso de la fuerza bien sea cinética o cibernética, satisfaría la exigencia de la necesidad cuando no fuera suficiente el uso de medidas no coercitivas para frenar el ataque armado.

Por lo que, si el ataque pudiera frustrarse efectivamente con el empleo de este tipo de medidas, denominadas de ciberdefensa pasiva, el Estado atacado no estaría autorizado a lanzar una respuesta en el nivel del uso de la fuerza.

2.3.4 La proporcionalidad

El último requisito para poder ejercitar el uso de la fuerza como legítima defensa es la proporcionalidad, haciendo éste referencia a cuánta fuerza, cinética o cibernética, es permisible utilizar en esa respuesta. Lo que la proporcionalidad delimita es la escala, alcance, duración e intensidad de la respuesta defensiva.

---

[29] RIPOLL CARULLA, S. ``*Protección del espacio aéreo y nueva política de Defensa Nacional´´*. Revista Española de Derecho Militar. 2006, n.º 88, pp. 57-89

El uso de la fuerza de manera excesiva para hacer frente a un ataque armado es considerado un ilícito internacional; lo mismo ocurre cuando, a modo de ejemplo, si un ciberataque puede ser repelido mediante fuerza dirigida exclusivamente contra la ciberinfraestructura desde la que aquel fue lanzado, no sería legítimo conducir operaciones que impliquen el uso de la fuerza a lo largo de todo el Estado atacante, en vez de centrar la legítima defensa exclusivamente frente a la ciberinfraestructura causante del daño.

2.4 La legítima defensa en el Manual de Tallin

El Manual de Tallin 2.0. recoge la legítima defensa individual en la regla 71 y la legítima defensa colectiva en la regla 74.

La regla 71 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 Carta de las Naciones Unidas.

La regla 74, sin embargo, determina que la legítima defensa puede ejercitarse de forma colectiva cuando se dé el supuesto de que el Estado que presta ayuda sólo puede actuar con el consentimiento y en los términos que consienta el Estado víctima; esto 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.[30]

La regla 75 del Manual de Tallín 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.

[30] INFORME DEL GRUPO DE EXPERTOS GUBERNAMENTALES sobre los *Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en el Contexto de la Seguridad Internacional*, 2015. Pp 339-340. https://undocs.org/es/A/70/174

Aunque la Carta de las Naciones Unidas no los recoge, existen dos principios básicos para ejercitar la legítima defensa, principios que ya hemos explicado en el epígrafe anterior, siendo estos los de necesidad y proporcionalidad, recogidos en la regla 72 del Manual.[31]

Según el Grupo de Expertos, ¨la necesidad 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¨.

Hay que analizar este principio desde la perspectiva del Estado víctima, en atención a sus circunstancias, siendo indispensable que el resto de las opciones que tenga el Estado víctima sean capaces de evitar la ofensa sin acudir al uso de la fuerza.[32]

La proporcionalidad 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 la defensa tenga la misma naturaleza que el ataque armado.

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; pudiendo 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.[33]

No se pueden usar los mismos criterios para todos los ciberataques, 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; es por ello que la doctrina de la acumulación de eventos defiende que esta sucesión de ataques de baja intensidad permita invocar la legítima defensa del artículo 51 CNU, sobre todo cuando estos permitan anticipar o prever un futuro ataque.[34]

---

[31] 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"

[32] INFORME DEL GRUPO DE EXPERTOS GUBERNAMENTALES sobre los *Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en el Contexto de la Seguridad Internacional,* 2015. https://undocs.org/es/A/70/174. cit., (pág 348-349)

[33] 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.

[34] *Ibid.,* pp. 86-87.

2.5 La legítima defensa en otros textos convencionales

La legítima defensa no sólo aparece exclusivamente recogida en la CNU o en el Manual de Tallín 2.0, sino que aparece en otros textos convencionales, como resulta ser el Proyecto de la CDI y el Tratado del Atlántico Norte (TAN).

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".[35] 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".[36]

Lo recogido en este artículo conlleva a que 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 5 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 independencia política o la seguridad de cualquiera de las Partes fuese amenazada".[37]

---

[35] *Texto del proyecto de artículos sobre la responsabilidad de las organizaciones internacionales* (2011) -Derecho Internacional Público.dipublico.org.https://www.dipublico.org/8237/texto-del-proyecto-de-articulos-sobre-la-responsabilidad-de-las-organizaciones-internacionales-2011/

[36] Relations, U. S. C. S. C. o. F. (1949). *North Atlantic Treaty: Documents Relating to the North Atlantic Treaty*.Artículo 5.

[37] 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)

El amparo en esta legítima defensa es una decisión política y propia para cada Estado parte de la OTAN; la única ocasión en la que han respondido al amparo de este artículo fue tras el ataque terrorista del 11S en Estados Unidos.[38]

En cualquier caso, decidir si un ciberataque activa el artículo 5 TAN corresponderá al Consejo de Seguridad de la Alianza.

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 42.7 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".[39]

La aplicación de este artículo es automática, siendo innecesario 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.

También se regula una cláusula de solidaridad en el artículo 222 del Tratado de Funcionamiento de la Unión[40], 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.

De estos dos artículos de los Tratados de la UE podemos concluir 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.

---

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

[39] *Tratado de la Unión Europea. (1992). Artículo 42.7.* Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002

[40] *Tratado de Funcionamiento de la Unión Europea.* (1992). *Artículo 222.* Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002

3. La responsabilidad de los ciberataques

El anonimato es una de las principales características del ciberespacio, pues, a pesar de que las autoridades han transmitido a la población que cualquier acción en la red deja huella, al nivel en el que operan los actores de las ciberoperaciones ofensivas contra los Estados la autoría de estas es un problema añadido a la hora de atribuir responsabilidades.

Aunque parece claro que los Estados serán responsables de una acción cibernética ofensiva cuando esta les sea atribuible, la mayoría de las veces el nexo entre el Estado y el hecho ilícito es difuso y difícil de demostrar, pues 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 es una complicación, puesto que, si no se demuestra la responsabilidad de un Estado en el ataque, no se podrá activar la legítima defensa del artículo 51 de la Carta de las Naciones Unidas.

Es acerca de este tema sobre el que vamos a hablar en este apartado de mi Trabajo Fin de Grado, analizando, en primer lugar, el supuesto de atribución cuando un Estado actúa a través de sus órganos, y, cuándo la actuación de actores no estatales puede ser imputada a un Estado.

3.1 La Responsabilidad Internacional de los Estados en el Derecho Internacional Público

Uno de los hechos que motivaron a la elaboración del Manual de Tallín 2.0 fueron los ciberataques sufridos por Estonia en 2007, aunque constituyeron 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.

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.

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), que fue anexada por la Asamblea General en su Resolución 56/83.[41]

El artículo 1 de este proyecto recoge que de todo hecho internacionalmente ilícito emana responsabilidad internacional, mientras que el artículo 2 define 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 cuestión de la atribución es, en consecuencia, un elemento imprescindible a analizar para determinar la Responsabilidad Internacional de los Estados por los ciberataques lanzados por actores no estatales desde sus territorios.

Previamente al análisis de la atribución de la responsabilidad de los ciberataques, es necesario concretar el marco jurídico-teórico de la atribución en el Derecho Internacional. En este sentido, resulta pertinente hacer mención del comentario 2º del texto *Draft articles on Responsibility of States for Internationally Wrongful Acts, witch commentarie*s, en el cual los miembros de la Comisión de Derecho Internacional analizan el contenido de los artículos del PREHII . La cuestión que aborda este comentario es muy relevante, puesto que indica que: "In theory, the conduct of all human beings, corporations or collectivities linked to the State by nationality, habitual residence or incorporation might be attributed to the State, whether or not they have any connection to the Government"[42].

Si se aplicara esta interpretación doctrinal de la atribución, el problema de la responsabilidad internacional de los Estados por los ciberataques lanzados por actores no estatales desde sus territorios estaría solucionado, bastando una simple conexión de nacionalidad o residencia para que la atribución de la responsabilidad fuera posible. Sin embargo, el mismo comentario indica, posteriormente, que la responsabilidad se limita a aquellas conductas que implican al Estado como

[41] COMISIÓN DE DERECHO INTERNACIONAL NACIONES UNIDAS. (2001). *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*. PREHII.

[42] *Draft articles on Responsibility of States for Internationally Wrongful Acts, witch commentaries*, 2001, comentario 2º.

organización, bien de forma directa a través de los órganos o autoridades individuales que lo componen, bien de forma indirecta a través de individuos contratados o instigados por los sujetos anteriores. Resumidamente, para que exista Responsabilidad Internacional del Estado en relación con las actuaciones de actores no estatales es necesario que exista una mínima vinculación entre los órganos o autoridades del Estado y los actores no estatales.

Este elemento crea una serie de inconvenientes pues, por un lado, las dificultades de la atribución de la responsabilidad por los ciberataques cometidos por actores no estatales respecto de los cuales existe una vinculación probada con el Estado y, por otro lado, la cuestión de qué sucede con los ciberataques perpetrados por actores no estatales al margen del Estado o cuya vinculación no puede ser probada.

En Derecho Internacional, el concepto de atribución "alude a la operación jurídica necesaria para entender si una cierta conducta de uno o más individuos, consistente en una acción u omisión, es reconducible a un Estado según el Derecho Internacional"[43]. Para poder realizar esa atribución en Derecho Internacional hay que diferenciar entre dos subtipos de atribución: por un lado, la atribución técnica, referida a la parte informática y tecnológica del asunto, y, por otro lado, la atribución jurídica, que comprende aquellos criterios jurídicos necesarios para imputar un acto a un Estado determinado. La Comisión de Derecho Internacional recogió los criterios de atribución de un hecho ilícito una serie de sujetos o agentes por cuyos actos habría de responder un Estado[44]:

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.

b) Personas o entidades en el ejercicio de atribuciones del poder público (artículo 5 PREHII). Las personas, pueden generar responsabilidad internacional, cuando concurran estos criterios: actúen en

[43] COCCHINI, A. ``Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados: Non-State Actors' Cyberattacks and States' "Cyber-due diligence."´´ *Revista UNISCI / UNISCI Journal,* 55, p.77

[44] COMISIÓN DE DERECHO INTERNACIONAL NACIONES UNIDAS. (2001). *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*. (PREHII)

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.[45]

c) Órganos de otros Estados a disposición del Estado (artículo 6 PREHII). Siendo estos 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.

La Corte de Derecho Internacional recoge en este Proyecto otros supuestos de responsabilidad de los Estados cuando los ciberataques los llevan a cabo 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).

Según el artículo 11 del PREHII, cualquier actuación que no se recoja en los supuestos anteriores, podrá ser atribuible a un Estado siempre y cuando este lo reconozca y adopte como propio.

El Manual de Tallin 2.0, como analizaremos en el siguiente subepígrafe sigue los mismos criterios para poder imputar a un Estado una acción u operación cibernética; concretamente las reglas 15 a 17 de dicho Manual. La regla 15 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. La regla 16 acoge la misma premisa que el artículo 6 del Proyecto de la Comisión. Por último, la regla 17 acoge la responsabilidad en caso de que el ciberataque lo causen actores no estatales

45 GUTIÉRREZ ESPADA, C. "*La responsabilidad internacional*"... op. cit., p.79.

que sigan las instrucciones o estén bajo el control efectivo de un Estado, así como la que generan aquellas ciberoperaciones que el Estado reconozca como propias.

3.2. La responsabilidad de los actores no estatales desde la perspectiva del Manual de Tallín 2.0

Como hemos explicado en varias ocasiones en apartados anteriores de este trabajo, el *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* es un documento no oficial desarrollado por un grupo de expertos de la OTAN, realizando un análisis e interpretación de la normativa existente y determinar su aplicación al ámbito del ciberespacio conforme a los términos previstos en la legislación ya establecida a nivel internacional; es por ello, que este Manual no tiene carácter vinculante.

Reafirmando lo manifestado en el subepígrafe anterior el Manual aborda la responsabilidad internacional de los ciberataques llevados a cabo por actores no estatales en su regla 15 a 17.

Nos centraremos en el análisis de la regla 17, prevé lo siguiente:

¨Rule 17 – Attribution of cyber operations by non-State actors

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; o

(b) the State acknowledges and adopts the operations as its own˝

Al estar el Manual de Tallín basado en la Resolución 56/83, por la cual sigue los mismos criterios de atribución de responsabilidad, la anterior regla mencionada, regla 17, concluye que las ciberoperaciones realizadas por actores no estatales no pueden atribuirse a los Estados, salvo en dos excepciones: cuando actúen bajo las instrucciones o control directo del Estado, en cuyo caso pasarían a considerarse órganos auxiliares de la propia entidad estatal; o cuando el Estado reconozca esa operación como propia.

Con el término "instrucciones" el Manual de Tallin 2.0 se refiere a cuando el Estado solicita la ayuda del actor no estatal para abordar una situación determinada, lo que lo convierte en un auxiliar del

Estado. De esta forma, intenta diferenciar esta figura de aquellos actores que han sido expresamente autorizados por el Estado para realizar una acción determinada y de aquellos sobre los que tiene un control efectivo.

En el caso que explicamos anteriormente acerca de aquellos sujetos que actúan bajo la dirección o control, es importante saber el grado de control o influencia exigible para que pueda nacer la atribución de responsabilidad de un Estado, asunto que ha sido objeto de controversia jurisprudencial, con dos posiciones mayormente enfrentadas: la tesis del control efectivo y la del control global o general.[46]

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".[47]

Sin embargo, la otra posición, es la tesis del control general, que fue defendida en varias ocasiones por el Tribunal Penal Internacional para la Antigua Yugoslavia, considerando que la tesis del control efectivo no era apropiada en relación con las actuaciones de grupos organizados y estructurados, ya

[46] GUTIÉRREZ ESPADA, C. *"La responsabilidad internacional"*... op. cit., p.83.

[47] CORTE INTERNACIONAL DE JUSTICIA. *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua* (Nicaragua contra los Estados Unidos de América). 1984. párrafos 109-125.

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.

A pesar de la posición que adoptó el Tribunal Penal Internacional, la Corte Internacional de Justicia rechazó el criterio del control general por considerarla inadecuada 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.[48]

Es por esto que la doctrina mayoritaria en el ámbito de los ciberataques apuesta por la tesis de control efectivo, a la cual ya hemos hecho alusión en párrafos anteriores.

La regla 17 del Manual de Tallín recoge la interpretación de la Corte Internacional de Justicia sobre el criterio de control efectivo respecto de la responsabilidad internacional de los Estados por hechos internacionalmente ilícitos cometidos por actores no estatales. Es por ello que el Manual señala que

> "Un Estado posee el control efectivo de una ciberoperación específica realizada por un actor no estatal cuando sea el propio Estado el que determine la ejecución y el curso de esa operación determinada y que la actividad cibernética desarrollada por el actor estatal sea una parte integral de esa".[49]

Concluyendo que para que un Estado pueda ser considerado responsable por las actuaciones de un actor no estatal, requiere que este tenga la capacidad, no sólo de generar el daño a través de los ciberataques, sino además de ordenar su cese, conforme a la jurisprudencia de la Corte Internacional de Justicia en el caso *Nicaragua;* y llevándolo a nuestro ámbito de estudio, un ejemplo de ello es que la provisión de un malware por parte del Estado no sería generadora de responsabilidad estatal si no concurre el criterio de control efectivo, sin embargo, la provisión de malwares sí que supondría la vulneración de principios de Derecho Internacional en aplicación de la Regla 66, que establece que "un Estado no intervendrá, incluyendo medios cibernéticos, en los asuntos tanto internos como

---

[48] GUTIÉRREZ ESPADA, C. *"La responsabilidad internacional"*... op. cit., pp. 84-85.

[49] SCHMITT, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. (p.95).

externos de otro Estado"[50], puesto que, aunque una actuación de un Estado en el ámbito del ciberespacio no sea generadora de responsabilidad internacional, sí que podría quebrar una obligación internacional en otro ámbito y sancionarse por esa vía.

El criterio actual del control efectivo limita en exceso las oportunidades de disuasión, control y sanción de la responsabilidad internacional de los Estados en el ciberespacio, al restringir la atribución de la responsabilidad a supuestos muy específicos y de especial intervención estatal; es por ello, que se requiere la aplicación de un nuevo condicionante que analizaremos en el siguiente capítulo de este trabajo, se trata de la diligencia debida, para abordar todos aquellos actos internacionalmente ilícitos en el ciberespacio y que no quedan comprendidos dentro de la figura de la responsabilidad internacional.

3.3. La responsabilidad internacional por complicidad

A pesar de que, en el Derecho Internacional, a excepción de lo analizado acerca de la responsabilidad de actores no estatales, rige el principio de que un Estado responde sólo de sus propios actos, es importante 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).

Los tres supuestos comparten que es necesario como requisito 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 Manual de Tallín se manifiesta acerca de este asunto, en su regla 18, limitándose a compartir los tres supuestos que recoge el PREHII en sus artículos 16-18.

[50] SCHMITT, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

En cuanto a la ayuda que describe el artículo 16 PREHII, la más frecuente en la realidad, se recoge en esta regla que, 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).[51]

3.4. La dificultad de la atribución de la responsabilidad internacional

Como hemos explicado con anterioridad, la principal dificultad de atribución de la responsabilidad con las ciberoperaciones es el de la trazabilidad y el anonimato; pues es la propia estructura tecnológica de la red la que dificulta esta atribución a una persona o entidad determinada. Dentro de esta estructura, destacan, a grandes rasgos, el anonimato que proporciona a los atacantes, el poder lanzar varios ataques simultáneos desde diferentes Estados y jurisdicciones y la velocidad con la que se realizan.

A través de las direcciones IP se pueden identificar los dispositivos que se han utilizado para realizar las acciones específicas a través de la red, siempre que no hayan sido manipuladas u ocultada; es por ello que, la estructura actual de la red no exige que exista realmente una dirección de retorno o de origen en las acciones de envío de datos, sino que los datos que se envían a través de Internet únicamente necesitan saber su destino para funcionar, no su origen. Este factor, unido a la existencia de aplicaciones y mecanismos para ocultar o hacer irrastreable la actividad en la red, es la base del anonimato en Internet y el principal obstáculo para conseguir una trazabilidad fiable y clara de los perpetradores de un ciberataque.

Aunque se pudiera identificar a la persona concreta que ha realizado el ciberataque, la atribución del mismo, únicamente podría producirse en aquellos casos en los que pudiera identificarse y probarse que existe un nexo legal suficiente entre el actor y el Estado, como explica la Resolución 56/83 y el Manual de Tallín.

---

51 GUTIÉRREZ ESPADA, C. *"La responsabilidad internacional"*... op. cit., pp. 102-103

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[52]. 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"[53].

Existen casos donde la falta de prueba de que un Estado es responsable de un ciberataque ha permitido su impunidad, como 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, permitiendo que los autores no sufran las consecuencias.

4. Las contramedidas frente a los ciberataques.

Además de la legítima defensa, existe otra circunstancia que excluye la ilicitud de la actuación de un Estado que han sufrido un ciberataque, tanto si este adquiere la fuerza necesaria para poder ser considerado ataque armado como si no; esta vía es las contramedidas, que permiten al Estado víctima del ciberataque incumplir sus obligaciones internacionales con el Estado atacante como reacción a su ofensiva; siendo estas una causa de exclusión de la ilicitud, siempre y cuando las medidas que el Estado víctima adopte no entrañen el uso de la fuerza[54].

---

52 BANKS, W., *Cyber Attribution and State Responsibility. International Law Studies*, vol. 97, Nº 1, 2021. P.1046.

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

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

La Corte Internacional de Justicia y la Comisión de Derecho Internacional, legitiman las contramedidas, o también denominadas represalias, siempre que se cumplan una serie de requisitos.

El primer requisito es la existencia de un hecho ilícito cometido por parte de un Estados.

El segundo requisito conlleva al cumplimiento de una serie de condiciones de carácter procesal que recogió la Comisión de Derecho Internacional en su artículo 52[55]:

" - 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. "

El tercer requisito para la consideración de la licitud de las contramedidas es la proporcionalidad, que se recoge en el artículo 51 del Proyecto sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (PREHII), al que ya hemos hecho mención en varias ocasiones de este capítulo. Como ya hemos explicado, la proporcionalidad es un requisito complicado de delimitar en el ámbito de las ciberoperaciones; 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[56].

[55] INTERNATIONAL LAW COMMISSION. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 52*. 2001. https://www.refworld.org/legal/otherinstr/ilc/2001/en/20951

[56] ROSCINI, M. World Wide Warfare. *Ius ad Bellum and the Use of Cyber Force*. Max Planck Yearbook of United Nations Law, Vol. 14, 2010. pp. 113-114

5. El Consejo de Seguridad de las Naciones Unidas y los tribunales internacionales.

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 de la Carta de las Naciones Unidas para la solución del conflicto. Este artículo 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".

El Consejo, en virtud de lo dispuesto en el artículo 36 de su Carta, 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 de la Carta y establecer las medidas que estime necesarias tomadas de conformidad con los artículos 41 y 42; cuyas medidas tendrán carácter provisional a la decisión del Consejo de Seguridad. 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).

Muchos de los expertos en la materia coinciden en que el artículo 41 de la Carta de las Naciones Unidas es de gran ayuda su aplicación en los ciberataques, acerca de las medidas que no impliquen el uso de la fuerza armada para hacer efectivas las decisiones del Consejo, pues especifica que

> "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".

Esto atribuye la facultad al Consejo a imponer un ciberbloqueo por parte de los Estados miembros al Estado responsable de un ciberataque para evitar que produzca o continúe con los daños.[57]

[57] ROSCINI, M. World Wide Warfare. *Ius ad Bellum and the Use of Cyber Force*. Max Planck Yearbook of United Nations Law, Vol. 14, 2010. p.111

Otra vía a la que puede acudir un Estado víctima de un ciberataque una vez se ha identificado al Estado responsable, es a los tribunales internacionales con el fin de obtener la reparación por los daños causados por el Estado atacante que infringe tanto el artículo 2.4 de la Carta de las Naciones Unidas como el principio de no intervención.

Entre los tribunales internacionales a los que se puede acudir destacaremos la Corte Internacional de Justicia, establecida en 1945 por la Comisión de las Naciones Unidas y principal órgano judicial de las Naciones Unidas. Este tribunal tiene dos tipos de procedimientos: contencioso y consultivo; pudiendo ser parte en los procedimientos contenciosos tanto los Estados firmantes del Estatuto de la Corte Internacional de Justicia (entre ellos, todos los Estados Miembros de las Naciones Unidas) y aquellos que acepten su jurisdicción.[58]

Según el artículo 40.1 del Reglamento de la CIJ, la solicitud de incoación de procedimiento, lo que sería la demanda, "deberá indicar la parte que la hace, el Estado contra quien se proponga la demanda y el objeto de la controversia"[59], por lo que es imprescindible que, antes de acudir a este tribunal, hayamos identificado al Estado responsable de ese ciberataque para que pueda convertirse en la parte demandada.

Como bien explica DIEZ DE VELASCO, M, "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 cual, un Estado reconoce como obligatoria de forma inmediata y sin convenio especial la jurisdicción de la CIJ respecto de cualquier otro Estado que haya suscrito alguna declaración aceptándola".[60]

Por último, los Estados víctima pueden acudir a la Asamblea General o el Consejo de Seguridad para que soliciten a la CIJ que emita una Opinión Consultiva, como faculta el artículo 96 CNU, acerca de si un ciberataque infringe el Derecho internacional, aunque es discutible el carácter obligatorio

[58] NACIONES UNIDAS. CORTE INTERNACIONAL DE JUSTICIA. *Funcionamiento de la Corte.* https://www.un.org/es/icj/how.shtml

[59] UNIT NATIONS INTERNATIONAL COURT OF JUSTICE. (1945*). Statute of the International Court of Justice, Art. 40*.

[60] DIEZ DE VELASCO, M. *Instituciones de Derecho Internacional Público*. Madrid, Tecnos, 2009. pp. 994-995.

de las Opiniones de la CIJ; pues algunos instrumentos internacionales le conceden fuerza vinculante, como la Convención sobre privilegios e inmunidades de las Naciones Unidas, 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, según nos explica DIEZ DE VELASCO, M en el mismo manual de referencia.[61]

[61] DIEZ DE VELASCO, M. *Instituciones de Derecho Internacional Público*. Madrid, Tecnos, 2009. pp 999-1000.

CAPÍTULO 3: LAS CIBEROPERACIONES Y EL *IUS IN BELLO*

1. Presupuestos necesarios para la aplicación del Derecho Internacional Humanitario a las ciberoperaciones

1.1. Ámbito material

Como hemos reiterado en varias ocasiones en este trabajo, una ciberoperación queda sujeta al Derecho Internacional Humanitario (DIH) es si esta se ha conducido en el contexto de, o guarda un nexo, con un conflicto armado.

Es más fácil determinar la aplicabilidad del DIH cuando la ciberoperación tenga lugar con el trasfondo de un preexistente conflicto armado tradicional, donde se aplicarán las normas del DIH que regulan ese conflicto armado en atención a su carácter internacional o no internacional.

El asunto se complica cuando son las ciberoperaciones por sí solas las que desencadenan un conflicto armado; hay que atender a la existencia de dos tipos de conflictos armados que regula el DIH: los internacionales, en los que se enfrentan Estados, y los no internacionales, en los cuales uno de los beligerantes, al menos, es un actor no estatal.[62]

Las ciberhostilidades constituirán un conflicto armado internacional cuando las ciberoperaciones sean atribuibles a un Estado y equivalgan al uso de fuerza armada contra otro Estado.

En cuanto a los criterios de atribución jurídica a un Estado de las ciberhostilidades realizadas por actores privados, se aplica el artículo 8 PREHII al que ya hemos hecho alusión en varias ocasiones en el capítulo anterior de este trabajo,

¨se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento"[63],

---

62 ÑO LUCO, R. ``La guerra aérea y el derecho internacional humanitario´´, *Derecho internacional humanitario y temas de áreas vinculadas. Lecciones y Ensayos*. 2003, nº 78, pp. 201-237

63 COMISIÓN DE DERECHO INTERNACIONAL. ``*Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos´´*. PREHII. *Resolución 56/83 de la Asamblea General de las Naciones Unidas*. A/RES/56/83, de 28 de enero de 2002. Art 8.
https://www.dipublico.org/4076/responsabilidad-del-estado-porhechos-internacionalmente-ilicitos-ag5683/

sabiendo que los expertos consideran más optimo aplicar a este precepto la teoría del control efectivo frente a la teoría del control general para la atribución de responsabilid

1.2. El criterio de la equivalencia

El segundo criterio que deben cumplimentar las ciberoperaciones para desencadenar un conflicto armado y poder aplicar el DIH, es el de que sean equivalentes a un uso de fuerza armada contra otro Estado.

Este requisito no plantea problemas cuando esas ciberoperaciones tienen efectos físicamente destructivos, pero se puede complicar cuando estos ciberataques pese a no causar esos efectos, producen consecuencias altamente lesivas, como, por ejemplo, sucedería si mediante un ciberataque se interrumpiera el suministro de servicios esenciales; en este último caso de daños producidos por ciertos ciberataques sí que entrarían en juego la aplicación de las normas de DIH al causar esto ataques graves consecuencias desde el punto de vista humanitario.

1.3 Los conflictos armados sin carácter internacional

Nos encontramos ante un conflicto armado no internacional cuando existe una situación de violencia armada continuada entre fuerzas gubernamentales y grupos armados organizados, o entre estos últimos dentro de un Estado; pero siempre es requisito fundamental para estar ante este tipo de conflictos armados que el actor no estatal alcance un mínimo nivel de organización y que la violencia armada supere un umbral de cierta intensidad.

No serán considerados actores no estatales aquellos grupos de hackers activos en el ciberespacio que de forma cooperativa llevan a cabo ciberoperaciones conjuntas, pues para ello es preciso contar con una estructura de mando, con una jerarquía y disciplina suficientes que permitan llevar a cabo ciberhostilidades de forma sostenida y hacer cumplir las reglas básicas del DIH, de la que tales grupos carecen; es más adecuado considerar que la respuesta a las acciones de dichos grupos debe provenir del aparato policial-judicial estatal, dada su naturaleza esencialmente criminal, como nos explica Jerónimo Domínguez Bascoy.[64]

[64] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., pp. 240-241.

Existen pocas posibilidades de que se produzcan ciberataques considerados como ataques armados llevados a cabo por actores no estatales, pues como recoge el art 1.2 del Protocolo Adicional II a los Convenios de Ginebra,

> `` la existencia de un conflicto armado no internacional desencadenado únicamente mediante ciberoperaciones requiere que estas superen un umbral de intensidad que vaya más allá de la violencia propia de los disturbios interiores, tales como los motines, los actos esporádicos y aislados de violencia y otros actos análogos, que no constituyen conflictos armados´´[65].

Independientemente de que las ciberoperaciones fueran consideradas como conflictos armados internacionales o no, las reglas de aplicación a ambos conflictos sería el Protocolo Adicional I a los Convenios de Ginebra.

2. Aplicación de las reglas sobre conducción de hostilidades a las ciberoperaciones

Las reglas del Protocolo Adicional I a los Convenios de Ginebra contienen apartados que hacen referencia a las operaciones militares en general, atendiendo a los principios de distinción, proporcionalidad y precaución, regulando las hostilidades en general, que incluirían, además de los ataques, todas aquellas operaciones se llevan a cabo durante un conflicto armado con el propósito de dañar al adversario.

Como casi la totalidad de las reglas del Protocolo sobre conducción de las hostilidades están referidas a los «ataques», el artículo 49.1 del Protocolo Adicional I establece que ``se entiende por ataques los actos de violencia contra el adversario, sean ofensivos o defensivos´´. Se concluye que la violencia requerida para que un acto sea calificado como ataque no es la ejercida en el acto en sí, sino en sus consecuencias.

En el Manual de Tallin el ciberataque se define como ``una ciberoperación ofensiva o defensiva de la que cabe razonablemente esperar que cause lesiones o muerte a personas o daños o destrucción a objetos´´.[66]

---

[65] INTERNATIONAL COMMITTEE OF THE RED CROSS. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*. Art 1.2

[66] SCHMITT, M. ``*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations´´*. Cambridge: Cambridge University Press. 2017.

El grupo de expertos que redactaron el Manual coincidieron en que en los ciberataques la pérdida de funcionalidad equivale al daño físico que éstos produzcan siempre que como consecuencia de esta la ciberinfraestructura atacada quede permanentemente inoperativa o precise de una significativa reparación; al igual que acordaron que no serían ciberataques aquellos que simplemente produjeran una denegación de servicio de duración limitada, que causan meras inconveniencias o irritaciones. Al igual que no entiende el DIH como ataque aquellos medios de guerra psicológica o económica, o la interferencia de las comunicaciones, tampoco lo hace el Manual de Tallín en el ámbito de las ciberoperaciones.

Sin embargo, no hay acuerdo entre los expertos, en calificar con ataques aquellas ciberoperaciones que hacen que sea preciso reinstalar el sistema operativo o que borran, corrompen o alteran datos que son esenciales para que una infraestructura puede realizar correctamente la función para la que fue diseñada.

3. Las ciberoperaciones y los distintos principios exigidos

3.1. El principio de diligencia debida y su aplicación en el ciberespacio

El principio de diligencia debida se erige como la mejor alternativa a la limitada figura de la responsabilidad internacional, a la que hace referencia el CIJ en el Asunto Nicaragua, ya comentado en capítulos anteriores del trabajo, por el que estableció que ¨para que los Estados Unidos fueran jurídicamente responsables, tendría que probarse que ese Estado tenía un control efectivo de las operaciones durante las que se habían cometido las presuntas violaciones"[67].

Esto supondría, como ya hemos aclarado, y cuya interpretación recoge también el Manual de Tallín, que únicamente habría responsabilidad internacional del Estado si se prueba que tenía control efectivo de las operaciones, excluyendo actividades tales como la financiación, organización equipamiento y planificación de las acciones armadas de un actor no estatal, admitiendo como excepciones los supuestos de control efectivos planteados por la CIJ.

[67] CORTE INTERNACIONAL DE JUSTICIA. *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América*). Fallo de 27 de junio de 1986.Párrafo 115. https://www.dipublico.org/cij/doc/79.pdf

La doctrina opina que el principio de diligencia debida es el que mejor aborda la cuestión de la responsabilidad de los Estados por actos cometidos por actores no estatales, hasta que los Estados acuerden un marco jurídico específico que sea aplicable al ciberespacio o se consolide una *opinio juris* en una dirección determinada.[68]

La jurisprudencia acerca de este principio nació en 1872, con el caso Alabama Claims, se establecía en el Tratado de Washington que los Estados debían ejercer toda diligencia para impedir que, en su jurisdicción, se construyeran, alistaran o salieran del puerto navíos sobre los que se tuvieran fundadas sospechas de estar destinados a hacer la guerra contra una potencia con la que se encuentra en paz. Por ello, recogió el tribunal que efectivamente Reino Unido había incumplido las obligaciones derivadas del principio de diligencia debida, puesto que los "insufficient legal means cannot justify failure of due diligence".[69]

Sin embargo, fue con el caso Trail Smelter [70] cuando este principio tuvo mayor relevancia, el Tribunal aceptó la existencia de un estándar de diligencia debida con el objeto de evitar daños transfronterizos; se podría afirmar que este principio tiene su origen en jurisprudencia nacional, puesto que el propio Tribunal se refiere en la sentencia a resoluciones del Tribunal Supremo de Estados Unidos, pero ha sido aceptado por la opinio juris de la comunidad internacional.

Fue en 1949, con el caso de Corfú, cuando la Corte Internacional de Justicia nos brindó una definición del principio de diligencia, "es la obligación de todo Estado no permitir adrede que su territorio sea usado para actos contrarios a los derechos de otros Estados"; es decir, que los Estados controlen la actividad que sucede dentro de sus territorios con el fin de proteger los derechos de los demás Estados que podrían verse comprometidos por ellas.

---

[68] PIERNAS, J. ``El principio de diligencia debida en Derecho internacional y su aplicación al contexto cibernético´´. *Anales de Derecho*, *41*(1), 2024, pp.66–95. https://doi.org/10.6018/analesderecho.594441

[69] PATRICK, C. ``Debugging the Tallin Manual 2.0's Application of the Due Diligence Principle to Cyber Operations´´. *Washington International Law Journal, 28(2*), pp.581-604

[70] COCCHINI, A. ``Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados: Non-State Actors' Cyberattacks and States' "Cyber-due diligence."´´ *Revista UNISCI / UNISCI Journal, 55*, 2021, pp.69–98

La CIJ, con el caso Pulp Mills, en 2010, determinó que dentro del principio de diligencia existía otro principio, el de prevención, que definió como

"Un Estado está, por tanto, obligado a usar todos los medios a su disposición con el objeto de prevenir actividades que tengan lugar en su territorio, o en cualquier área bajo su jurisdicción, y causen un daño significativo al medioambiente de otro Estado. Esta Corte ha establecido que esta obligación es ahora parte del cuerpo de derecho internacional relativo al medioambiente", [71]

estableciendo la obligación de prevenir actividades que puedan causar un daño significativo al medioambiente.

Los requisitos esenciales para considerar que un Estado ha cumplido el principio de diligencia es que la responsabilidad por un daño únicamente se aplica cuando el Estado desde cuyo territorio se produzca el daño tuviera conocimiento de tales acciones y que el perjuicio causado sea de una determinada gravedad; el otro es que se considera que un Estado no habrá cumplido con el principio de diligencia debida cuando no haya adoptado todas las medidas necesarias de las que fuera capaz para prevenir el daño; es por ello que este principio sea flexible y se interprete conforme a las capacidades técnicas y materiales de cada Estado.

3.1.1. La aplicación del principio de diligencia debida según el Manual de Tallín

El Manual de Tallin 2.0 recoge, en su Regla 6, el principio de diligencia debida como principio general aplicable al ciberespacio, la cual establece que

> "Un Estado debe ejercer la diligencia debida para no permitir que su territorio, el territorio o la ciberinfraestructura bajo el control gubernamental sean utilizados para la realización de ciberoperaciones que afecten los derechos de otros Estados y produzcan consecuencias adversas graves a estos"[72].

---

[71] INTERNATIONAL COURT OF JUSTICE. ``*Pulp Mills on the River Uruguay (Argentina v. Uruguay)´´*. ICJ Reports 2010, pp. 14. **Pulp Mills on the River Uruguay (Argentina v. Uruguay) (icj-cij.org)**

[72] SCHMITT, M. ``*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations´´*. Cambridge: Cambridge University Press. 2017. Rule 6.

El grupo de expertos redactores del Manual, aplica este principio al ámbito del ciberespacio por analogía de su aplicación en otros ámbitos del Derecho Internacional hasta que se cree una normativa específica que resuelva los vacíos legales y problemáticas de este ámbito; este grupo ha establecido que la base del principio de diligencia debida es que el Estado debe controlar las actividades que se realicen en su territorio y puedan afectar a los derechos o territorios de otros Estados, aunque se produzcan por actores no estatales, debiendo producir a ese Estado un daño severo.

En cuanto a la aplicación de este principio, el propio Manual de Tallín manifiesta que

> ¨la regla 6 se aplica cuando alguno de los siguientes actores está involucrado: el Estado objetivo de la ciberoperación, el Estado territorial sujeto a la norma y la tercera parte que es el autor de la ciberoperación, incluyendo en este último grupo los individuos, entidades privadas y otros actores no estatales¨.[73]

Del párrafo anterior deducimos que este principio no solo es de aplicación a aquellos ciberataques llevados a cabo por actores no estatales desde el territorio de un Estados causando daños a otro Estado, sino también resultaría de aplicabilidad a los Estados de tránsito, en virtud del principio de soberanía, entendidos estos como aquellos cuya ciberinfraestructura se utiliza para lanzar una ciberoperación de forma remota, sin que en el territorio de dicho Estado se encuentren los autores del ciberataque ni que sea el objetivo del mismo, aunque es muy complicado que un Estado de tránsito sea declarado responsable de quebrantar el principio de diligencia debida por un ciberataque para el que se ha usado su ciberinfraestructura, puesto que conlleva una cierta complejidad probar que este Estado tenía conocimiento de que dichas acciones se estaban produciendo.

El Manual de Tallín 2.0 crea un concepto al que denomina constructive knowledge, a través del cual argumenta que ¨la obligación de diligencia debida se sigue aplicando cuando el Estado no tuviera conocimiento de la ciberoperación específica, pero objetivamente debería haber sabido sobre ella¨.

La regla 7 del Manual aborda cuándo los Estados están cumpliendo el principio de diligencia debida:

---

73 SCHMITT, M. ``*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations´´*. Cambridge: Cambridge University Press. 2017. Rule 6.

> ¨El principio de diligencia debida exige al Estado que adopte todas las medidas que sean factibles dependiendo de las circunstancias con el objeto de poner un fin a las ciberoperaciones que afecten un derecho de un Estado o produzcan consecuencias graves adversas para otros Estados¨. [74]

Esta regla explica que el principio de diligencia debida se quebranta no por acción, sino por omisión, pues el incumplimiento de esta obligación ocurre cuando el Estado no haya adoptado las medidas necesarias que sean factibles, dependiendo del caso específico, para detener las ciberoperaciones que comprometan los derechos de otros Estados o supongan un daño grave para ellos.

El Manual de Tallín expresa que ¨Teniendo en cuenta la dificultad de crear medidas efectivas contra cualquier posible amenaza cibernética, no sería razonable afirmar que existe la obligación de prevención en el ciberespacio¨; pues no resulta razonable exigir a los Estados el desarrollo y preparación de personal e infraestructuras destinadas única y exclusivamente a prevenir ciberoperaciones.

Según el criterio que adopta el grupo de expertos, el conocimiento efectivo es requisito fundamental para que se produzca la violación del principio de diligencia debida, pero esto sería un requisito que no convendría aplicar al ámbito de las ciberoperaciones puesto que un Estado no puede conocer de los ciberataques que aún no han sido planificados, y así lo reitera el Manual cuando recoge que

> ¨Extender esta regla a un deber general de prevención supondría que el requisito de conocimiento – respecto del cual todos los expertos han determinado que es necesario para el quebrantamiento de la obligación – irrelevante¨.

Resumiendo, según las reglas y jurisprudencia recogidas en este subepígrafe, se puede concluir que el principio de diligencia debida es aplicable al ciberespacio, pero esto no significa que el Estado territorial tenga la obligación de prevenir y detener todas las posibles ciberoperaciones que supongan un riesgo para la seguridad y derechos de otros Estados, sino únicamente aquellos sobre los cuales tenga o debiera tener un conocimiento efectivo o constructivo.

---

[74] SCHMITT, M. ``*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations´´.* Cambridge: Cambridge University Press. 2017. Rule 7.

3.2. Ciberoperaciones y el principio de distinción

Según el artículo 48 del Protocolo Adicional I, el principio de distinción, principio fundamental del DIH, se define como

> ``aquel conforme al cual a fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares''[75].

3.2.1. Bienes que son objetivo militar legítimo de un ciberataque

El artículo 52.2 del Protocolo Adicional I define los objetivos contra los que debería limitarse un ciberataque, como

``aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida''[76].

Como explica el General Auditor Jerónimo Domínguez Bascoy

> ``El principal problema que plantea la aplicación de esta regla a las operaciones en el ciberespacio es que la mayor parte de las ciberinfraestructuras son bienes de doble uso que, según la opinión mayoritaria, constituyen objetivos militares por razón del propósito militar al que sirven''[77].

Esto conlleva que la mayor parte de las ciberinfraestructuras son objetivos militares susceptibles de ser atacados, por lo que el DIH ha tenido que atribuir a estos bienes de doble uso una mayor protección basada también en los principios de proporcionalidad y precaución.

Existe la posibilidad de que las ciberinfraestructuras civiles, a pesar de gozar de protección frente a ciberataques directos, pueden sufrir daños por un ataque dirigido contra una ciberinfraestructura militares, dada la interconexión que caracteriza al ciberespacio; esto exige que las partes del conflicto

---

[75] INTERNATIONAL COMMITTEE OF THE RED CROSS. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, Article 48

[76] INTERNATIONAL COMMITTEE OF THE RED CROSS. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I*), 8 June 1977, *Article 52.2*

[77] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 243.

observen estrictamente la prohibición de usar ciberarmas indiscriminadas por naturaleza, como un malware que se replica sin control y cuyos efectos dañinos no se pueden limitar.

Como hemos dicho con anterioridad, se considerará ataque a toda aquella ciberoperación que destruya o altere aquellos datos que causen a raíz de esa manipulación lesiones, muerte, daños o destrucción, estando prohibido atacar bienes civiles.

El grupo de expertos encargados de redactar el Manual de Tallín 2.0 opinan que, dispensar a los datos civiles el trato de bienes protegidos imposibilitaría llevar a cabo ciberoperaciones tradicionalmente no prohibidas. Un sector minoritario, sin embargo, discordó que no considerar a los datos como un bien protegido permitiría llevar a cabo operaciones altamente disruptivas. De ahí que, de lege ferenda, Michael Schmitt haya postulado como posible solución a este dilema la de reconocer que los datos sobre los que descansan funciones civiles esenciales merecen especial protección conforme al DIH.[78]

3.2.2. Las personas como objetivos en la ciberguerra

Puede darse el caso, de que los ciberataques no tengan como objetivo una infraestructura sino causar lesiones o la muerte a individuos; el ataque directo contra civiles está prohibido, sin embargo, sí pueden ser objetivos de un ciberataque aquellos individuos que ostenten la condición de combatientes.

En cuanto a los miembros de grupos armados organizados, un sector de los expertos que participaron en el Manual de Tallin siguió el criterio de la Guía Interpretativa del CICR (2009) sobre la noción de participación directa en las hostilidades, admiten únicamente que pueden lanzarse ciberataques contra aquellos miembros del grupo que desarrollan una «función continua de combate», como son aquellos que llevan a cabo ciberoperaciones contra las fuerzas enemigas. Otro sector, sin embargo, opina que la mera pertenencia al grupo, independientemente de la función que desempeñen, permite tratar a todos sus miembros como objetivos militares legítimos.

3.2.3. La participación directa de personas civiles en las hostilidades

[78] RODRÍGUEZ-VILLASANTE Y PRIETO, J. L.; LÓPEZ SÁNCHEZ, J.; PÉREZ GONZÁLEZ, M. (coords.). ``Acciones hostiles y objetivos militares. Los principios de igualdad, distinción, precaución y proporcionalidad´´, *Derecho Internacional Humanitario*. Valencia: Tirant Lo Blanch, 2017, pp. 353-398

Otro sector que puede ser objetivo de los ciberataques son los individuos que, sin ser combatientes ni pertenecer a un grupo armado organizado, participan directamente en las hostilidades; incluyendo en estas categorías hackers individuales que atacan ciberinfraestructuras militares; a múltiples hackers que, sin actuar colaborativamente, lanzan ciberataques contra unas mismas ciberinfraestructuras, y a aquellas personas que recolectan inteligencia por medios cibernéticos, que identifican vulnerabilidades o que desarrollan exploits que pasan a una de las partes en el conflicto.

Como explica Jerónimo Domínguez Bascoy, para que exista participación directa se requieren tres requisitos[79]:

1.ª Umbral de daño: el acto del participante debe tener efectos adversos sobre las operaciones militares o sobre la capacidad militar de una de las partes en conflicto o causar lesiones, muerte, daños o destrucción de personas y bienes protegidos. También lo sería una operación de denegación de servicio dirigida contra la ciberinfraestructura de una de las partes cuando se afectara negativamente a las operaciones militares de esa parte o a su capacidad militar.

2.ª Causalidad directa: debe haber un vínculo causal directo entre el acto y el daño que pueda resultar de ese acto o de la operación militar coordinada de que dicho acto es parte integrante. La causalidad directa exige que el daño causado sea ocasionado por una sola secuencia causal, lo que dificultaría sobremanera apreciar la concurrencia de este requisito en los casos de ciberataques, cuyos efectos relevantes suelen ser normalmente de segundo o tercer grado.

3.ª Nexo beligerante: el propósito específico del acto debe ser causar directamente el umbral exigido de daño en apoyo de una parte en conflicto y en perjuicio de la otra.

A diferencia de lo que sucede con los combatientes y miembros de grupos armados organizados, quienes participan en las hostilidades individualmente solo pueden ser atacados mientras dura tal participación. Los expertos redactores del Manual de Tallín entienden que la limitación al tiempo que dura la participación directa en las hostilidades deba entenderse referida al período comprendido

[79] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., pp. 245-246.

entre la ciberoperación inicial del individuo y el momento en que decide desistir de seguir llevando a cabo ciberoperaciones.[80]

3.3. Los ciberataques y el principio de proporcionalidad

El principio de proporcionalidad, recogido en los artículos 51.5 y 57.2 del Protocolo Adicional I, recoge la posibilidad de llevar a cabo ciberataques

"cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista".[81]

Esta regla que recoge tal principio requiere que solamente se tengan en cuenta los daños físicos que se prevea va a causar el ciberataque, y no sólo los producidos directamente por el ataque, sino también los que produce indirectamente; por lo que la mera irritación que produzcan las ciberoperaciones no han de ser sopesados en el cálculo de proporcionalidad. Sin embargo, como hemos explicado anteriormente, siguiendo las normas de DIH, la pérdida de funcionalidad se considera como daño, por lo que, cuando se causa esta en una ciberinfraestructura civil, la privación de funcionalidad también deberá estimarse como daño a efectos de la regla de proporcionalidad.

3.4. Los ciberataques y el principio de precaución

El principio de precaución exige dar aviso con la debida antelación y por medios eficaces de cualquier ataque que pueda afectar a la población civil, salvo que las circunstancias lo impidan.

La condición que contiene este principio de dar aviso si las circunstancias no lo impiden se traduce en que, si los avisos suponen alertar al enemigo de forma que le permitiera defenderse efectivamente del ataque, no habría obligación de dar aquellos.

Como apuntan los expertos en la materia, este principio,

---

[80] RODRÍGUEZ-VILLASANTE Y PRIETO, J. L.; LÓPEZ SÁNCHEZ, J.; PÉREZ GONZÁLEZ, M. (coords.). `` Participación directa de las personas civiles en las hostilidades´´. *Derecho Internacional Humanitario*. Valencia: Tirant Lo Blanch, 2017, pp. 779-801.

[81] INTERNATIONAL COMMITTEE OF THE RED CROSS. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*. Art 51 and 57

``también sujeto a condiciones de factibilidad, de adoptar precauciones contra los efectos de los ataques exige alejar de la proximidad de objetivos militares a la población civil, las personas civiles y los bienes de carácter civil; evitar situar objetivos militares en el interior o en las proximidades de zonas densamente pobladas, y, en general, tomar las demás precauciones necesarias para proteger contra los peligros resultantes de operaciones militares a la población civil, las personas civiles y los bienes de carácter civil.´´[82]

Esto conllevaría en el ámbito del ciberespacio que los beligerantes hicieran todo lo posible para separar las ciberinfraestructuras civiles de las militares; siendo en la práctica difícilmente factible; por lo que lo máximo que podría exigirse es que se adoptasen las precauciones precisas para asegurar que las ciberinfraestructuras críticas sean protegidas en la medida de lo posible de los efectos de los ciberataques; un ejemplo práctico de ello que nos comentan los expertos es

``almacenando de forma segura los datos esenciales, realizando un back up efectivo o, en fin, garantizando una permanente asistencia técnica que permita reparar las redes o, en su caso, redirigirlas a otros sistemas alternativos a fin de que aquellas continúen manteniendo su funcionalidad´´[83].

[82] RODRÍGUEZ-VILLASANTE Y PRIETO, J. L.; LÓPEZ SÁNCHEZ, J.; PÉREZ GONZÁLEZ, M. (coords.). ``Acciones hostiles y objetivos militares. Los principios de igualdad, distinción, precaución y proporcionalidad´´, *Derecho Internacional Humanitario*. Valencia: Tirant Lo Blanch, 2017, pp. 353-398

[83] DOMÍNGUEZ BASCOY, Jerónimo. "Aplicación del derecho internacional "... op. cit., p. 249.

CONCLUSIONES

La falta de un marco jurídico específico que se encuentre generalizado y aceptado por los Estados provoca la existencia de vacíos legales y aprovechados por otros Estados y actores no estatales para realizar ciberataques que produzcan daños muy graves a otros Estados. Es por ello que la doctrina se ha erigido como principal fuente del Derecho Internacional en el ciberespacio, proporcionando marcos provisionales de interpretación del Derecho Internacional que imponen límites a la actividad de los Estados en este ámbito, y que recoge el Manual de Tallín 2.0.

PRIMERA: Los Estados serán responsables de la ciberestructura e individuos que se encuentren en sus territorios, aunque sus actividades realizadas desde esas mismas fronteras causen daños a otros Estados fuera de ellas. Es decir, cuando un Estado realice un ciberataque a otro Estado será considerado como que ha ejercido el uso de la fuerza, y por tanto, una ciberoperación 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.

Para que pueda considerarse tal ciberoperación como ataque armado, debe provocar un daño de una determinada gravedad, como recoge el artículo 51 CNU, al que aplicaremos por analogía en este ámbito, para que el Estado víctima pueda actuar acogiéndose a su derecho a la legítima defensa.

SEGUNDA: Otro de los inconvenientes que surge para que pueda ejercer la legítima defensa se recoge en que se debe atribuir la responsabilidad del ciberataque a un Estado; esto se complica no sólo por lo fácil que es mantener el anonimato en este nuevo campo de batalla, sino que además, cuando estas ciberoperaciones son llevadas a cabo por actores no Estatales, es de gran dificultad demostrar fehacientemente que estos actores no estatales han actuado y realizado tales ciberataques con la ayuda o consentimiento de un Estado.

La responsabilidad internacional de los Estados en cuanto a los ciberataques ha sido gran parte del estudio de este Trabajo Fin de Grado, y como hemos explicado en él, a pesar de existir textos legales que lo regulan como es la Resolución 56/83, aplicable también al ámbito del ciberespacio, la jurisprudencia de la Corte Internacional de Justicia en relación con los actores no estatales genera un vacío legal que deviene en la impunidad de los Estados que se aprovechan de estos actores para cometer actos internacionalmente ilícitos, y en cuanto a esta problemática, a pesar de existir dos

teorías que intentaban solucionarla, la doctrina mayoritaria optó por elegir la teoría del control general, acuñada por el Tribunal Penal para la Antigua Yugoslavia, que establecía que la responsabilidad del Estado también abarcaba todas las acciones de coordinación, financiación, preparación… siendo necesaria la aplicación de otra figura a la responsabilidad de los Estados por los ciberataques lanzados por actores no estatales desde sus territorios: el principio general de diligencia debida.

TERCERA: El principio de diligencia debida conlleva la obligación por parte de los Estados de no permitir que su territorio e infraestructuras sean utilizados para la realización de ciberataques a otros Estados; para cumplimentar dicha obligación, el Estado deberá adoptar las medidas que fueran necesarias para evitar que se produzca dicho daño. El principio de diligencia debida, sin embargo, únicamente se impondrá al Estado cuando este tuviera o debiera tener conocimiento del desarrollo de dicha actividad por parte de un actor no estatal y que dicha ciberoperación llevada a cabo por estos actores fuera susceptible de causar un daño grave en otro Estado, considerándolo como ataque armado. Esto no conlleva una obligación de prevención en el marco de la diligencia debida, ya que no se considera razonable que un Estado deba destinar gran cantidad de recursos a prevenir ciberataques hipotéticos.

Una vez se hayan cumplimentado los dos requisitos anteriores de que el ciberataque alcance el nivel de ataque armado, y que haya sido posible atribuir una ciberoperación ofensiva a un Estado, el Estado víctima podrá activar la legítima defensa del artículo 51 CNU, pudiendo emplear tato medidas cibernéticas como cinéticas, pero siempre con el respeto a los principios de proporcionalidad, necesidad e inmediatez. Lo mismo se establece para el caso de ejercer la legítima defensa colectiva, los Estados que auxilien al Estado agredido deberán respetar los límites que este imponga.

CUARTA: El Estado víctima de un ciberataque no solo posee la legítima defensa como medio de respuesta, sino que podrá acudir a las contramedidas que regula el 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, 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.

QUINTA: Es por todo lo formulado en esta conclusión, que me parece necesario que la comunidad internacional busque con urgencia, debido a la rápida expansión del ciberespacio como campo de combate, la elaboración de una normativa específica para tal ámbito que se adecue a sus

particulares características, que con la aplicación por analogía del ya existente Derecho Internacional conllevan una problemática pues no son cubiertas adecuadamente. A pesar de esto, es claro, que siendo racionales, es difícil que se lleguen a acuerdos de elaboración de este marco jurídico por parte de los diferentes Estados, pues estos también velan por su propia soberanía y poder, y el que ciertos aspectos no estén regulados les beneficia a la hora de realizar ciberoperaciones buscando sus propios intereses, por lo que desde mi punto de vista, la comunidad internacional procederá a la elaboración de normas específicas en este ámbito cuando se hayan aprovechado o agotado todas las oportunidades estratégicas que ofrece el ciberespacio.

BIBLIOGRAFÍA

- BANKS, W., *Cyber Attribution and State Responsibility. International Law Studies*, vol. 97, Nº 1, 2021.

- 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.
- CASANOVAS, O.; RODRIGO, A.J. Compendio de derecho Internacional Público. Madrid: Tecnos, 2017. 1ºed.
- COCCHINI, A. ``Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados: Non-State Actors' Cyberattacks and States' "Cyber-due diligence."´´ *Revista UNISCI / UNISCI Journal,* 55.

- DIEZ DE VELASCO, M. *Instituciones de Derecho Internacional Público*. Madrid, Tecnos, 2009.
- DOMÍNGUEZ BASCOY, Jerónimo.``Aplicación del derecho internacional a las operaciones en el ciberespacio´´. *Manual de Derecho Internacional Humanitario aplicable a la guerra aérea.* Madrid: Ministerio de Defensa, 2021, 1º ed.
- GUTIÉRREZ ESPADA, C. *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*, Cizur Menor, Thomson-Reuters Aranzadi, 2020.
- HAUBLER, U. *Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO*. International Cyber Security Legal & Policy Proceedings, 2010.
- INTERNATIONAL GROUP OF EXPERTS. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. ISBN 978-1316630372
- ÑO LUCO, R. ``La guerra aérea y el derecho internacional humanitario´´, *Derecho internacional humanitario y temas de áreas vinculadas. Lecciones y Ensayos*. 2003, nº 78, pp. 201-237
- PATRICK, C. ``Debugging the Tallin Manual 2.0's Application of the Due Diligence Principle to Cyber Operations´´. *Washington International Law Journal, 28(2*).

- RIPOLL CARULLA, S. ``*Protección del espacio aéreo y nueva política de Defensa Nacional´´*. Revista Española de Derecho Militar. 2006, n.º 88.
- RODRÍGUEZ-VILLASANTE Y PRIETO, J. L.; LÓPEZ SÁNCHEZ, J.; PÉREZ GONZÁLEZ, M. (coords.). ``Acciones hostiles y objetivos militares. Los principios de igualdad, distinción, precaución y proporcionalidad´´, *Derecho Internacional Humanitario*. Valencia: Tirant Lo Blanch, 2017.

- RODRÍGUEZ-VILLASANTE Y PRIETO, J. L.; LÓPEZ SÁNCHEZ, J.; PÉREZ GONZÁLEZ, M. (coords.). `` Participación directa de las personas civiles en las hostilidades´´. *Derecho Internacional Humanitario*. Valencia: Tirant Lo Blanch, 2017.
- ROSCINI, M. World Wide Warfare. *Ius ad Bellum and the Use of Cyber Force*. Max Planck Yearbook of United Nations Law, Vol. 14, 2010.
- ROSCINI, Marco, *Cyber Operations and the Use of Force in International Law*. Oxford, 2014.
- SCHMITT, M. N. (Ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013

TEXTOS NORMATIVOS Y JURISPRUDENCIA

- COMISIÓN DE DERECHO INTERNACIONAL NACIONES UNIDAS. (2001). *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*. PREHII.
- CORTE INTERNACIONAL DE JUSTICIA. (1996). *Legalidad de la amenaza o uso de armas nucleares*. https://www.icj-cij.org/case/95/advisory-opinions. (Consulta: abril 2024)
- CORTE INTERNACIONAL DE JUSTICIA. *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua* (Nicaragua contra los Estados Unidos de América). 1984.
- CORTE INTERNACIONAL DE JUSTICIA. *Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América*). Fallo de 27 de junio de 1986. https://www.dipublico.org/cij/doc/79.pdf. (Consulta: abril 2024).
- *Draft articles on Responsibility of States for Internationally Wrongful Acts, witch commentaries*, 2001, comentario 2º.
- ESPAÑA. MINISTERIO DE DEFENSA. (2013). *Orden Ministerial 10/2013, de 19 de febrero por la que se crea el Mando Conjunto de Ciberdefensa.* BOE.
- ESPAÑA. MINISTERIO DE DEFENSA. (2013). *Orden pci/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [BOE n. º 103, 30/iv/2019]*. (Consulta: marzo 2024)
- EUROPEAN COMMISSION. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001. (Consulta: marzo 2024)

- INFORME DEL GRUPO DE EXPERTOS GUBERNAMENTALES sobre los *Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en el Contexto de la Seguridad Internacional*, 2015. https://undocs.org/es/A/70/174. (Consulta: marzo 2024)
- INTERNATIONAL COMMITTEE OF THE RED CROSS. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
- INTERNATIONAL COMMITTEE OF THE RED CROSS. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II).*
- INTERNATIONAL COURT OF JUSTICE. ``Pulp Mills on the River Uruguay (Argentina v. Uruguay)´´. ICJ Reports 2010, Pulp Mills on the River Uruguay (Argentina v. Uruguay) (icj-cij.org). (Consulta: abril 2024)
- NACIONES UNIDAS. (1948). *Carta de las Naciones Unidas. Y estatuto de la Corte Internacional de Justicia.Artículo 2.4*. Naciones Unidas, Departamento de Información Pública. (Consulta: marzo 2024)
- NACIONES UNIDAS. (1948). *Carta de las Naciones Unidas. Y estatuto de la Corte Internacional de Justicia. Artículo 51*. Naciones Unidas, Departamento de Información Pública. (Consulta: marzo 2024).
- NACIONES UNIDAS. *Convención de las Naciones Unidas sobre el Derecho del Mar.*(1982). https://www.un.org/Depts/los/convention_agreements/texts/unclos/convemar_es.pdf. (Consulta: mayo 2024)
- NACIONES UNIDAS. CORTE INTERNACIONAL DE JUSTICIA. *Funcionamiento de la Corte.* https://www.un.org/es/icj/how.shtml. (Consulta: mayo 2024)
- NACIONES UNIDAS. *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones*, comentario Nº1 al artículo 22. (Consulta: mayo 2024)
- NACIONES UNIDAS. *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.* (Consulta: mayo 2024)
- NACIONES UNIDAS. *Resolución 56/83 de la Asamblea General de las Naciones Unidas*. A/RES/56/83, de 28 de enero de 2002. https://www.dipublico.org/4076/responsabilidad-del-estado-porhechos-internacionalmente-ilicitos-ag5683/. (Consulta: marzo de 2024)

- OTAN. *Análisis y Recomendaciones del Grupo de Expertos Sobre un Nuevo concepto Estratégico para la OTAN,* 17 de mayo de 2010. https://www.nato.int/cps/en/natohq/topics_85961.htm. (Consulta: abril 2024)
- 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*.
- Relations, U. S. C. S. C. o. F. (1949). *North Atlantic Treaty: Documents Relating to the North Atlantic Treaty*.Artículo 5.
- *Texto del proyecto de artículos sobre la responsabilidad de las organizaciones internacionales* (2011) - Derecho InternacionalPúblico.dipublico.org.https://www.dipublico.org/8237/texto-del-proyecto-de-articulos-sobre-la-responsabilidad-de-las-organizaciones-internacionales-2011. (Consulta: marzo 2024)
- *Tratado de Funcionamiento de la Unión Europea.* (1992). *Artículo 222.* Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002. (Consulta: marzo 2024)
- *Tratado de la Unión Europea. (1992). Artículo 42.7.* Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002. (Consulta: marzo 2024)

WEBGRAFÍA

- HOLLIS, D. *Derecho Internacional y operaciones cibernéticas del Estado: Mejora de la transparencia*. Rio de Janeiro: Organización de los Estados Americanos. 2020. https://www. oas. org/en/sla/iajc/docs/CJI_doc_603-20_rev1. pdf. (Consulta: abril de 2024)
- OCHOA-RUIZ. N; SALAMANCA-AGUADO. E, *Exploring the Limits of International Law relating to the Use of Force in Self-defence;* European Journal of International Law, Volume 16, Issue 3, June 2005, https://doi.org/10.1093/ejil/chi128. (Consulta: mayo de 2024)
- PIERNAS, J. ``El principio de diligencia debida en Derecho internacional y su aplicación al contexto cibernético´´. *Anuales de Derecho*, *41*(1), 2024, https://doi.org/10.6018/analesderecho.594441. (Consulta: mayo de 2024).