FACULTAD DE DERECHO

LA APLICACIÓN DEL DERECHO INTERNACIONAL AL CIBERESPACIO EN LAS CIBEROPERACIONES REALIZADAS POR ACTORES NO ESTATALES DESDE EL TERRITORIO DE UN ESTADO

La responsabilidad internacional de los Estados y el principio de diligencia debida

Autor: Juan Ríos García

5º E-5

Derecho Internacional Público

Tutor: Antonio Díaz Narváez

Madrid

Abril 2021

ÍNDICE

LISTADO DE ABREVIATURAS

AG: Asamblea General de Naciones Unidas

CIJ: Corte Internacional de Justicia

GEG: Grupo de Expertos Gubernamental

GIE: Grupo Internacional de Expertos

IP: Internet Protocol

OTAN: Organización del Tratado del Atlántico Norte

TPIY: Tribunal Penal Internacional para la ex-Yugoslavia

INTRODUCCIÓN

En los últimos años Internet se ha convertido en una parte indispensable del funcionamiento de los Estados y de la vida de las personas y, además, se encuentra en un proceso de constante crecimiento y expansión. En este contexto, los Estados se encuentran continuamente enfrentándose a nuevos desafíos para la seguridad de su infraestructura, de su territorio y de sus ciudadanos. Los Estados son extremadamente dependientes del ciberespacio, y cada vez más. Por este motivo, es necesario que esta nueva área sea dotada de un marco jurídico propio en el seno del Derecho Internacional, y que éste se adecúe a su relevancia. El incremento de los ciberataques que, en los últimos tiempos, han afectado a las Administraciones Públicas e infraestructuras críticas de diferentes Estados[1] es justificación más que suficiente para exigir a la comunidad internacional una respuesta contundente y a corto plazo para abordar los desafíos del ciberespacio.

Actualmente, no existe una norma específica a nivel internacional que regule el comportamiento de los Estados y de otras entidades privadas y actores no estatales en el ciberespacio, sino que es necesario aplicar el Derecho Internacional existente ante las diferentes problemáticas que surgen. No obstante, el ciberespacio cuenta con características únicas que provocan que la aplicación de estas normas sea problemática: en primer lugar, el ciberespacio no entiende de fronteras, en la medida que lo único que se encuentra en un territorio determinado es la ciberinfraestructura que se utiliza en el ciberataque y la persona detrás de ella, y, en ocasiones, ni siquiera concurre esta circunstancia. En segundo lugar, el enorme anonimato que proporciona el ciberespacio a los actores que realizan hechos ilícitos. En tercer y último lugar, la accesibilidad universal al mismo (Bergwik, 2020, p. 6).

En consecuencia, el ciberespacio está siendo escenario de un nuevo tipo de guerra relámpago, en la que se producen ciberataques continuamente y desde diferentes tipos de fuentes. Las ciberoperaciones orquestadas por Estados continúan existiendo y pueden ser objeto de sanción bajo la figura jurídica de la responsabilidad internacional si generan un daño grave a otro Estado. Sin embargo, recientemente ha aparecido una nueva cuestión:

[1] Véase el ciberataque ruso a Estonia en 2007 (BBC, 2017) o a la bolsa de Nueva Zelanda en agosto de 2020 (El Confidencial, 2020), entre otros.

actores no estatales que realizan ciberataques a otros Estados desde el territorio de otro Estado, en muchas ocasiones con la complacencia e incluso ayuda de este. Por este motivo, es necesario analizar nuevamente las obligaciones aplicables a los Estados en esta materia y como se pueden abordar estas nuevas amenazas para la seguridad internacional desde la perspectiva del Derecho Internacional. Es inconcebible que un Estado que colabore activamente o que sea permisivo respecto de los ciberataques realizados por actores no estatales desde sus territorios quede impune.

Por este motivo, se analizará en el presente Trabajo de Fin de Grado la aplicación del Derecho Internacional al ciberespacio y en caso de que, efectivamente, pueda aplicarse, se determinará qué procedimiento hay que seguir para aplicarlo correctamente. Además, se examinará la posibilidad de aplicar la figura jurídica de la responsabilidad internacional de los Estados a esta cuestión relativa a los hechos internacionalmente ilícitos orquestados por actores no estatales con el apoyo de los Estados y la aplicabilidad del principio general de diligencia debida en caso de que la primera no resulte aplicable. Para todo ello se utilizarán todos los instrumentos normativos, jurisprudenciales y doctrinales a disposición del autor. Entre ellos, es necesario hacer mención expresa del *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.

El objetivo de este trabajo es aportar nuevas conclusiones a la construcción del Derecho Internacional en relación con el ciberespacio, materia respecto de la cual hay antecedentes bibliográficos significativos, especialmente de carácter académico. Sin embargo, no existen unas reglas u posiciones estatales claras sobre la aplicación del Derecho Internacional al ciberespacio. Por ello, es muy importante continuar aportando nuevas ideas y conclusiones que apoyen la importante labor doctrinal que están realizando muchos autores, pero especialmente el Grupo Internacional de Expertos, autor del Manual de Tallin 2.0.

A estos efectos, se han utilizado fuentes primarias, secundarias y terciarias. No solo se ha realizado un minucioso análisis doctrinal de obras académicas ya existentes y publicadas, sino que, a su vez, se ha estudiado la construcción y antecedentes jurisprudenciales y normativos de cada una de las figuras jurídicas examinadas en el presente trabajo. El objetivo de todo este proceso de investigación, realizada a través del método jurídico, no es otro que estudiar la aplicación de las figuras jurídicas expuestas en

este Trabajo de Fin de Grado al ciberespacio en general y, en particular, al fenómeno de los ciberataques realizados por actores no estatales desde un Estado y cuál es la responsabilidad del Estado territorial por los mismos. Para ello, ha sido necesario analizar los antecedentes jurídicos de estas figuras, cómo han sido tratadas por la jurisprudencia y la consideración que tienen en el ámbito doctrinal. Una vez realizados estos pasos previos, se ha interpretado la información recopilada y se han extraído conclusiones propias que constituyen la aportación de este trabajo a la aplicación del Derecho Internacional al ciberespacio.

1. ANÁLISIS JURÍDICO DE LA APLICACIÓN DEL DERECHO INTERNACIONAL AL CIBERESPACIO Y DE LA FIGURA JURÍDICA DE LA RESPONSABILIDAD INTERNACIONAL DE LOS ESTADOS

1.1. La aplicación del Derecho Internacional al ciberespacio.

1.1.1. La naturaleza jurídica del ciberespacio y la vigencia de los principios fundamentales de Derecho Internacional.

La responsabilidad internacional de los Estados por hechos internacionalmente ilícitos es una de las figuras jurídicas más relevantes del Derecho Internacional. Su reflejo en la Resolución 56/83 la convierte en un logro muy significativo para la comunidad jurídica internacional, en la medida que determina cuando un Estado es responsable por un hecho internacionalmente ilícito y prevé sanciones para ese acto, lo cual afecta directamente a la soberanía de los Estados. Es, además, una vía clave de prevención de hechos ilícitos por parte de los Estados, puesto que, aparte de las sanciones y formas de reparación, el mero hecho de ser declarado responsable por tales actos ya supone un castigo reputacional importante para ese Estado y su política exterior.

Por todos estos motivos, la figura de la responsabilidad internacional sería clave para prevenir los daños causados por las diferentes operaciones existentes en el ciberespacio y para determinar la responsabilidad y consecuencias de aquellas que se realicen con éxito y que sean cometidas por actores no estatales. Sin embargo, antes de entrar a analizar la responsabilidad internacional de los Estados en estos casos, es necesario examinar la posición actual del ciberespacio y la pertinencia de aplicar el Derecho Internacional vigente a esta área, atendiendo a sus particularidades y a la rapidez de su evolución.

En primer lugar, es necesario delimitar que se entiende por ciberespacio. Aunque la definición de esta nueva área puede variar entre autores, la utilizada por Tsagourias recoge los elementos más significativos del mismo. En este sentido, el autor indica que el ciberespacio puede definirse como: "*a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems,*

and embedded processors and controllers" (Tsagourias, 2015, p. 15)[2]. Consecuentemente, se concluye que existen tres capas diferenciadas que componen el ciberespacio: una física, compuesta por los ordenadores, infraestructuras etc.; otra de carácter técnico, fundamentalmente *software* y, por último, una tercera capa relativa al intercambio de datos y a la electrónica.

Como se puede observar, el ciberespacio está compuesto tanto por elementos físicos como tecnológicos, que tienen un carácter más virtual. Ambos son completamente interdependientes entre sí, pero es en la virtualidad donde se producen los hechos internacionalmente ilícitos: en el intercambio de datos a través de Internet gracias a los *softwares* previamente diseñados. Esta comunicación de datos se produce vía internet, que es, al fin y al cabo, un fenómeno reciente y novedoso que presenta importantes desafíos para el Derecho Internacional, en la medida que el ciberespacio no se encuentra estrictamente sometido a límites fronterizos. De hecho, los hechos internacionalmente ilícitos son cometidos por sujetos en un Estado desde su territorio, pero sus efectos alcanzan a uno o varios Estados en sus territorios (Zimmermann, 2014, p. 2-3). Incluso, en muchas ocasiones, los propios ataques se desvían a través de servidores de terceros Estados para asegurar que no sean fácilmente trazables.

Por tanto, la primera cuestión que debe resolverse en relación con la aplicabilidad del Derecho Internacional al ciberespacio es el de su naturaleza jurídica. Podría considerarse como parte de los *global commons* (Bergwik, 2020, p. 7), pero hay que tener en cuenta, como bien señala Segura, que "actualmente la infraestructura de Internet es tanto pública como privada y que las normas que se le aplican son tanto internacionales como nacionales" (Segura, 2017, p. 291-292), por lo que podría considerarse como un *global commons* especial. En cualquier caso, como tal, podría y es deseable que se alcanzase en un futuro próximo un régimen jurídico internacionalizado regulador de los inmensos recursos que ofrece el ciberespacio.

En este sentido, para poder ser considerado como parte de los *global commons*, señala Franzese que debería cumplir cinco requisitos: en primer lugar, debería estar sometido a un tratado internacional que rija su régimen jurídico; en segundo lugar, el tratado debe proveer usos y prohibiciones específicas de ese ámbito; en tercer lugar, debe ser definible;

[2] Traducción propia: "Un dominio mundial en el entorno de la información compuesto por la red interdependiente de infraestructuras tecnológicas de la información y datos residentes, incluidos Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados".

en cuarto lugar, debe haber reclamaciones de soberanía exclusiva por parte de algunos Estados sobre un área determinada del ciberespacio y, por último, un Estado o grupo limitados de Estados no pueden controlar por sí solos el *global commons* (Franzese, 2009, p. 16). Como se puede observar, para que el ciberespacio puedas ser considerado como parte de los *global commons,* como señalan los autores anteriores, es necesario que se cumplan una serie de requisitos, de los que únicamente no concurre la existencia de un Tratado regulador del mismo. En definitiva, sí que podría considerarse al ciberespacio como parte de los *global commons* y, como tal, debería proporcionarse un marco jurídico fuerte y que cuente con un consenso acorde a su naturaleza jurídica.

No obstante, a pesar de esta naturaleza particular del ciberespacio, hay que destacar que tal condición expuesta en el párrafo anterior no excluye la territorialización del Internet. O, en otras palabras, el ejercicio de los Estados del principio de soberanía en el ciberespacio, uno de los principios más importantes en el Derecho Internacional. De hecho, este es el primer tema que se trata en el *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (en adelante, Manual de Tallin 2.0)[3], escrito por un grupo de expertos internaciones que intentan dar mayor claridad y aportar una interpretación del Derecho Internacional al aplicarlo al ciberespacio. Esta obra es muy relevante en el ámbito del ciberespacio, puesto que aporta un marco jurídico (si bien se limita al ámbito doctrinal) aplicable a esta materia y permite, así, cubrir muchos de los vacíos legales que deja el Derecho Internacional al ser interpretado de forma errónea.

Es necesario destacar que esta obra es un instrumento no vinculante que estudia la aplicabilidad del Derecho Internacional al ciberespacio y a los conflictos cibernéticos. Como bien se indica en la introducción del propio Manual, lo que se pretende es realizar un análisis e interpretación de la normativa existente y su aplicabilidad al ámbito del ciberespacio conforme a los términos previstos en la legislación ya establecida a nivel internacional. En cualquier caso, se trata de una obra doctrinal de referencia, indispensable para analizar cualquier tema relacionado con el Derecho Internacional y el ciberespacio, cuyas reglas serán probablemente utilizados en un futuro próximo como guías para desarrollar acuerdos internacionales sobre el Derecho del ciberespacio.

[3] En las citas intertextuales, el Manual de Tallin 2.0 será citado como: (Schmitt, 2017, p.-), en la medida que dicho autor es el editor del Manual.

En consecuencia, su relevancia en este tipo de debates es muy significativa, puesto que aporta las interpretaciones y las claves jurídicas necesarias para dar una respuesta fundamentada a estas cuestiones. En relación con el tema de la soberanía, el Manual recoge, en su Regla 1, que "*The principle of State sovereignty applies in cyberspace*"[4] (Schmitt, 2017, p. 11). En consecuencia, sí que sería aplicable el concepto de soberanía del Derecho Internacional al ciberespacio y, con él, se abre la puerta a la aplicabilidad de otros principios y mecanismos, como el de la responsabilidad internacional. Por ello, resulta conveniente realizar un pequeño resumen sobre los aspectos más importantes del principio de soberanía de los Estados, en la medida que su interpretación para adaptarlo al ciberespacio muestra el camino a seguir en un futuro próximo para crear un marco jurídico internacional adaptado al ciberespacio.

En este sentido, el principio de soberanía ha sido tradicionalmente, y sigue siendo, uno de los principios más importantes del Derecho Internacional. Como bien indica Pastor Ridruejo, a pesar de que la sociedad internacional tras la Segunda Guerra Mundial presente rasgos de sociedad basada en intereses comunes y esté parcialmente organizada a través de instituciones, no puede negarse que "El Estado continúa ostentando una posición clave de protagonismo en las relaciones internacionales y sujeto por excelencia del Derecho Internacional" (Pastor, 2017, p. 299).

En consecuencia, el principio de soberanía sigue siendo elemental en la sociedad internacional actual y debe aplicarse a su vez a las relaciones entre los Estados en el ámbito cibernético. En este sentido, la Corte Permanente de Arbitraje ofreció, en el caso *Island of Palmas* de 1928, una definición del principio de soberanía que sigue muy vigente en el Derecho moderno actual: "*Sovereignty in the relations between States signifies Independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State*"[5] (*Island of Palmas*, 1928, párr. 27-28). En definitiva, el principio de soberanía establece que, dentro del territorio de un Estado, solo ese Estado podrá ejercer las funciones propias del mismo.

Por tanto, como bien indica el Manual de Tallin 2.0, la aplicación de este concepto al ciberespacio supone que los Estados ostentarán la soberanía sobre cualquier tipo de

[4] Traducción propia: "El principio de soberanía de los Estados se aplica en el ciberespacio".
[5] Traducción propia: "La Soberanía, en las relaciones entre Estados, significa independencia. La independencia en referencia a una porción del globo es el de derecho a ejercer en ese territorio, con la exclusión de cualquier otro Estado, las funciones del Estado".

ciberestructura localizada en su territorio y sobre toda actividad asociada con esa infraestructura cibernética (Schmitt, 2017, p. 11). Naturalmente, esto también se aplicaría a los individuos que utilicen ese tipo de infraestructuras, puesto que, al fin y al cabo, aunque las operaciones cibernéticas sean de carácter internacional al afectar a territorios de diferentes Estados, siguen estando dirigidas por entidades y/o individuos localizados en el territorio donde se encuentra esa infraestructura cibernética. Es decir, están sometidos a la jurisdicción y a la soberanía de ese Estado (Bergwik, 2020, p. 17). Es más, en ejercicio de su soberanía, los Estados gozarán de control absoluto sobre las operaciones e infraestructuras ciber. Esto significa que podrán disponer de ellas, desconectarlas de internet etc. y, además, que podrán someterlas a restricciones normativas, bien a través de Tratados Internacionales, bien a través de leyes nacionales.

Empero, hay que realizar varias precisiones respecto al principio de soberanía. En primer lugar, hay que tener en cuenta que ningún Estado podrá reclamar la soberanía exclusiva sobre el ciberespacio, al encontrarse la infraestructura necesaria para que funcione bajo la soberanía de otros Estados (Manual de Tallin, 2017, p. 13). En cualquier caso, esto no significa que un Estado no pueda estar ejerciendo jurisdicción estatal en el ciberespacio a través de las bases tradicionales de competencia territorial y personal. Es decir, se puede afirmar que existe una territorialización del ciberespacio sobre aquella actividad que está orientada hacia un territorio determinado y que tiene un efecto local (Segura, 2017, p. 292).

Por tanto, en relación con el ciberespacio, se entiende como territorio a aquel que se encuentra conectado con la parte física del ciberespacio, como, por ejemplo, dónde están situados los dispositivos o dónde está la persona que realiza el ciberataque (Bergwik, 2020, p. 17). Esta delimitación tendrá una importancia muy significativa a la hora de determinar la aplicabilidad de la figura jurídica de la responsabilidad internacional a los actos realizados por actores no estatales desde el territorio de un Estado, puesto que es el principal punto de unión que posibilitaría una hipotética atribución de la responsabilidad al Estado desde el que se realiza el ciberataque.

En cualquier caso, hay que recordar que el Estado no tiene completa disposición sobre los dispositivos, personas e infraestructuras relacionadas con el ciberespacio que se encuentran en su territorio. Como bien indica Pastor Ridruejo, en el plano jurídico, la soberanía no es un poder ilimitado del Estado y, además, el principio de soberanía también implica tanto la igualdad de los Estados como la independencia de estos y la

imposición del deber de no intervención entre ellos. Este autor, cuya postura se considera adecuada a los efectos de este trabajo, señala que basar la obligatoriedad del Derecho Internacional en la propia voluntad de los Estados es incompatible con el objetivo de mantener unas mínimas bases de convivencia en la sociedad concreta, en este caso la internacional (Pastor, 2017, p. 299-301).

Es más, la existencia de normas de *ius cogens*[6] y su asimilación por parte de los Estados, están admitiendo la existencia de límites que prevalecen sobre la voluntad soberana de los Estados, cuya inobservancia puede suponer la nulidad de los acuerdos contrarios a él (Pastor, 2017, p. 300). Estas normas también son aplicables al ámbito del ciberespacio, en la medida que, en última instancia, tiene una base eminentemente internacional y es un nuevo plano en el que los Estados pueden relacionarse entre ellos. En consecuencia, la no aplicación de estos límites al principio de soberanía supondría el libre albedrío de los Estados en el ámbito del ciberespacio, lo cual, como bien se ha señalado, es incompatible con la función y naturaleza del Derecho Internacional de asegurar unas bases mínimas de convivencia en la sociedad internacional.

Es más, como bien señaló la CIJ en el caso de *caso concerniente a las actividades militares y paramilitares en Nicaragua y contra ella: Nicaragua contra Estados Unidos de América*, "*between independent States, respect for territorial sovereignty is an essential foundation of international relations*[7]" (Nicaragua, 1986, párr. 202). En consecuencia, y en la medida que el ciberespacio se ha convertido en un nuevo foro en el que los Estados se relacionan, parece razonable realizar una interpretación extensiva del Derecho Internacional y aplicar sus principios, reglas y fundamentos también al ciberespacio.

El Manual de Tallin parece decantarse por este último razonamiento, en la medida que, al igual que reconoce el principio de soberanía de los Estados en el ciberespacio en su Regla 1, también recoge algunos límites al mismo. Entre ellos, es necesario destacar y analizar los contenidos en las Reglas 4 y 5 del Manual, que son las más relevantes a los efectos del presente trabajo (Schmitt, 2017, p. 17 y 27):

[6] Las normas de *ius cogens* son aquellas caracterizadas por ser de obligado cumplimiento. No admiten acuerdo en contrario de los Estados.

[7] Traducción propia: "Entre Estados independientes, el respeto de la soberanía territorial es un pilar fundamental de las relaciones internacionales".

Rule 4 – Violation of sovereignty

A State must not conduct cyber operations that violate the sovereignty of another State[8].

Rule 5 – Sovereign immunity and inviolability

Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty[9].

Por un lado, el Manual de Tallin, tras interpretar el Derecho Internacional vigente y aplicarlo al ciberespacio, también ha establecido límites a la soberanía de los Estados en relación con los otros Estados. En consecuencia, las ciberoperaciones que impidan o perjudiquen el ejercicio de la soberanía por parte de otros Estados serán constitutivas de una violación de una obligación de Derecho Internacional. Es decir, de un hecho internacionalmente ilícito (Schmitt, 2014, p. 275).

Por otro lado, el Manual de Tallin refleja, en su Regla 5, otro de los principios básicos de Derecho Internacional: el principio de no intervención. Como bien indica Pastor Ridruejo, el principio de no intervención constituye una norma de Derecho Internacional General, en la medida que tiene un importante arraigo consuetudinario en la sociedad internacional (Pastor, 2017, p. 304). Tal es su importancia en las relaciones entre Estados que este principio ha quedado cristalizado en la Resolución 2625 XXV de la Asamblea General de Naciones Unidas, que establece que:

> "Ningún Estado o grupo de Estados tiene derecho a intervenir directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro. Por tanto, no solamente la intervención armada, sino también cualesquiera otras formas de injerencia o de amenaza atentatoria de la personalidad del Estado, o de los elementos políticos, económicos y culturales que lo constituyen, son violaciones del Derecho Internacional".

Posteriormente, la CIJ, en el *caso concerniente a las actividades militares y paramilitares en Nicaragua y contra ella: Nicaragua contra Estados Unidos de América*,

[8] Traducción propia: **"Regla 4 – Violación de la soberanía:** Un Estado no debe realizar ciberoperaciones que vulneren la soberanía de otro Estado."

[9] Traducción propia: "**Regla 5 – Inmunidad e inviolabilidad de la soberanía:** Cualquier interferencia de un Estado en relación con la ciber infraestructura contenida en una plataforma y que goce de inmunidad de la soberanía, sea cual sea la localización en la que se encuentre, constituye una violación de la soberanía".

de 1986, refleja la misma idea que la Asamblea General en la resolución citada, determinando que: "El principio de no intervención supone el derecho de todo Estado soberano de conducir sus asuntos sin injerencia exterior; aunque los ejemplos de violación del principio no sean raros, el Tribunal estima que forma parte del Derecho Internacional Consuetudinario […] La existencia del principio de no intervención se apoya en una práctica importante y bien establecida" (Nicaragua, 1986, p. 106). En definitiva, el principio de no intervención prohíbe a cualquier Estado o grupos de Estados intervenir directa o indirectamente en los asuntos externos o internos de otro Estado (Pastor, 2017, p. 305).

Además, hay que tener en cuenta que, en la actualidad, la mayor parte de los asuntos internos y externos de los Estados están vinculados inevitablemente al ciberespacio a todos los niveles: político, económico, cultural, administrativo… De hecho, el funcionamiento de la mayoría de las infraestructuras críticas (energía, salud, agua) depende directamente del buen funcionamiento de sus sistemas informáticos. En consecuencia, si se aplica el contenido de este principio de Derecho General y la interpretación que de él hace la CIJ, es razonable concluir que también está en vigor en el ámbito cibernético. Es más, es fundamental su aplicación en el ciberespacio, en la medida que los derechos y el bienestar de miles de millones de personas depende del buen funcionamiento del ciberespacio que, a su vez, depende de la buena fe y el mantenimiento de una sociedad internacional funcional en el ámbito cibernético.

El análisis de estos principios fundamentales del Derecho Internacional nos ha permitido concluir que las normas internacionales pueden ser objeto de interpretación y aplicación en el ciberespacio, como bien recoge el Manual de Tallin 2.0. No obstante, y a pesar de que estos principios sean fundamentales para regular el ciberespacio, el Manual señala que estas reglas únicamente se aplican a las relaciones entre Estados, es decir, a aquellas ciberoperaciones que hayan sido realizadas directamente por los Estados o cuya responsabilidad pueda ser atribuida a ellos. Es decir, estas limitaciones al principio de soberanía no se aplicarían a aquellos actos cometidos por actores no estatales que no puedan ser atribuidos al Estado (Schmitt, 2017, p. 17).

Esta particularidad supone la aparición de un vacío legal importante en el Derecho Internacional que, en la actualidad, está siendo aprovechado por los Estados para sortear las limitaciones impuestas por las normas de *ius cogens* y vulnerar, así, la soberanía cibernética de otros Estados a través de actores no estatales. Es una prueba de que las

normas de Derecho Internacional General son útiles y funcionales, y que realmente contribuyen a la construcción y mantenimiento de una sociedad internacional que aspira a la paz, a la prosperidad y a la independencia de los Estados. Por este motivo, los Estados se han visto obligados a recurrir a terceros sujetos y actores para realizar actos cibernéticos constitutivos de hechos internacionalmente ilícitos. No obstante, debido a la complejidad y extensión de esta problemática, la cuestión de la atribución de la responsabilidad internacional de los Estados por los actos cometidos por actores no estatales desde sus territorios será analizada detalladamente en el apartado segundo del presente Trabajo de Fin de Grado.

1.1.2. Análisis sobre la eventual configuración un ordenamiento jurídico propio para el ciberespacio en el marco del Derecho Internacional.

En los apartados anteriores se han analizado diferentes figuras jurídicas relevantes para configurar el marco teórico de este trabajo: el principio de soberanía, el principio de no intervención y la figura de la responsabilidad internacional de los Estados. Todas ellas son clave para determinar la responsabilidad internacional de los Estados por los ciberataques lanzados desde sus territorios por actores no estatales. Sin embargo, realmente son figuras tradicionales de Derecho Internacional que se han intentado adaptar a este nuevo ámbito de relaciones entre los Estados.

Conforme se ha avanzado en el análisis de su aplicación al ámbito del ciberespacio, se han detectado varias cuestiones de relevancia en esta adaptación improvisada, en la medida que el ciberespacio es un área totalmente novedosa que evoluciona velozmente y cuya territorialización es muy compleja. Estas características son totalmente opuestas a la naturaleza del Derecho Internacional, cuyas normas están fundamentadas en la existencia de una *opinio juris* relevante en los Estados, lo cual necesita tiempo. En consecuencia, la efectividad del Derecho Internacional en el ciberespacio, como se pondrá de relevancia en los próximos apartados, es muy limitada y no da respuesta a los riesgos que genera el ciberespacio para la estabilidad de la sociedad internacional.

En consecuencia, cabe plantearse la duda de por qué no existen acuerdos a nivel internacional que regulen el mundo del ciberespacio. Al fin y al cabo, ninguno de los desafíos globales a los que se enfrenta la comunidad internacional en la actualidad puede

ser abordado por un único actor internacional, por muy poderoso que sea (Mačák, 2016, p. 127). Todos los grandes desafíos a los que se está enfrentando la sociedad internacional del siglo XXI, como el terrorismo o el cambio climático, gozan de foros de discusión para llegar a acuerdos que permitan alcanzar soluciones que no perjudiquen en exceso a ninguna parte, pero que permitan poner fin al problema. Sin embargo, en el ámbito del ciberespacio no existe una cooperación internacional significativa que permita establecer reglas comunes a todos los Estados para una correcta convivencia en el ámbito virtual que permita satisfacer y proteger los intereses de los países.

Este vacío existente en la cooperación internacional puede deberse, en parte, a la falta de transparencia y voluntad de los Estados en colaborar en materia de ciberseguridad etc. En consecuencia, no se han podido desarrollar en la comunidad internacional normas consuetudinarias, en la medida que estas se desarrollan a raíz de su práctica total por una mayoría de Estados, seguido de un sentimiento de obligatoriedad legal, es decir, de *opinio juris* (Egan, 2016, p. 171). Una de las principales causas es que, por cuestiones de seguridad e interés nacionales, los Estados no quieren descubrir sus cartas, en la medida que el ciberespacio sigue siendo un ámbito muy novedoso y que ofrece increíbles oportunidades, pero también amenazas. Por ello, los esfuerzos más significativos de estudiar las normas internacionales aplicables al ciberespacio se han realizado por parte de actores no estatales y desde el mundo doctrinal, como los expertos que han redactado los Manuales de Tallin, que se han convertido en las principales obras de referencia a la hora de estudiar cómo se aplica el Derecho Internacional al ciberespacio.

Un buen ejemplo de las dificultades existentes para configurar un cuerpo legal propio que regule las particularidades del ciberespacio es el hecho de que hasta 2013 los representantes de los Estados no acordaran determinar que el Derecho Internacional efectivamente se aplica al ciberespacio (Mačák, 2016, p. 127). Este informe fue realizado por el 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 (en adelante, GEG) en 2013. En él, el GEG aborda varias de las cuestiones que se han tratado en este trabajo, resaltando la importancia y vigencia de las mismas. De hecho, en estos años que han pasado desde la publicación del informe, apenas se han producido nuevos avances desde la esfera gubernamental respecto a la creación de un marco jurídico del ciberespacio.

En cualquier caso, es necesario destacar varios puntos de este informe, cuyo contenido fue posteriormente aprobado en la GEG de la Asamblea General en 2013. En primer lugar, el informe del GEG resalta que "la cooperación internacional es fundamental para reducir los riesgos y mejorar la seguridad" y que "deben examinarse medidas de cooperación que puedan contribuir a la paz, la estabilidad y a la seguridad internacionales" (GEG, 2013, párr. 2 & 11). En otras palabras, el GEG y la AG resaltan la necesidad de que los sujetos de la comunidad internacional colaboren para la configuración de normas jurídicas que aseguren unas mínimas bases de convivencia en la sociedad internacional (Pastor, 2017, p. 299-301).

Sin embargo, resulta llamativo que el informe no señale la posibilidad de crear nuevas normas jurídicas que se adapten a la particular naturaleza jurídica del ciberespacio y a las dificultades que esta conlleva. La configuración de un marco jurídico adaptado a estos factores solucionaría muchos de los problemas de interpretación y aplicación de normas de Derecho Internacional al ciberespacio, como bien señalan algunos autores (Egan, 2016; Mačák, 2016 & Zhixiong & Mačák, 2017). En este aspecto puede apreciarse una vez más la premisa de que, a pesar de que la comunidad internacional de después de la Segunda Guerra Mundial se halle enormemente institucionalizada por medio de Organizaciones Internacionales, los Estados siguen teniendo el papel principal en ella. En última instancia, son los sujetos estatales los que deciden sobre las Resoluciones, Acuerdos y otras fuentes de Derecho Internacional que regulan su comportamiento en las relaciones con otros Estados.

Por este motivo, el GEG estableció en su Informe de 2013 que "debe llegarse, por ejemplo, a un entendimiento común sobre cómo aplicar el derecho internacional pertinente y las normas, reglas y principios de conducta estatal responsable que se deriven de él" y 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" (GEG, 2013, párr. 11 & 16). Es en este punto, pues, en el que se concluye que las normas de Derecho Internacional deben interpretarse para ser aplicadas al ciberespacio. El proceso para ello es similar al que se ha utilizado en el apartado anterior. Es necesario examinar una figura jurídica tras otra, una a una, y, sobre la base de la jurisprudencia y doctrina internacionales existentes, determinar el

marco jurídico específico de esas figuras que será aplicable a la particular naturaleza del ciberespacio.

Sin embargo, si bien el informe señala que son los propios Estados los que deben liderar la labor de interpretar el Derecho Internacional en su aplicación para el ciberespacio, los actores no estatales provenientes del sector privado y académico son los que están realizando la labor más significativa en este aspecto. El mejor ejemplo de ello, una vez más, es el Manual de Tallin 2.0, que aborda una gran cantidad de cuestiones relativas al Derecho Internacional y el ciberespacio. Esta falta de pronunciamiento oficial por parte de Estados y Organizaciones Internacionales a gran escala supone la existencia de una gran inseguridad jurídica en el ciberespacio y de impunidad de comportamientos que no pueden encuadrarse bajo las reglas internacionales existentes por sus características.

En este sentido, es necesario destacar que ha habido algunos intentos de crear marcos jurídicos concretos para el ciberespacio, el más reciente fueron dos Códigos de Conducta para la Seguridad de la Información, propuesto conjuntamente por China y Rusia a la Asamblea General de Naciones Unidas en 2011 y 2015, sin mucho éxito entre los demás Estados. No obstante, los Estados mantienen una firme reticencia a contribuir al desarrollo de normas consuetudinarias de Derecho Internacional, en la medida que supondría desvelar sus posturas al respecto y el compartir información con otros Estados (Mačák, 2016, p. 130). Las oportunidades que ofrece el Derecho Internacional quedan, una vez más, limitadas por el poder e influencia que tienen los Estados en la comunidad jurídica internacional. De hecho, el informe del GEG de 2015, sobre la misma temática que el de 2013, señala que las normas de comportamiento responsable de los Estados en el ámbito del ciberespacio se regirían por las reglas de la voluntariedad, y no serían legalmente vinculantes (GEG. 2015, párr. 13).

Por último, resulta de interés mencionar algunas ideas que aportan Zhixiong y Mačák en un ensayo conjunto publicado en 2017 que compara las visiones chinas y occidentales respecto al Estado de Derecho en el ciberespacio. En este sentido, señalan algunas circunstancias y factores que debe considerarse como causas clave del no desarrollo de un Derecho Internacional específico aplicable al ciberespacio. Defienden estos académicos que, si bien se ha alcanzado un consenso general en forma de principios generales en relación con el ciberespacio, los Estados siguen difiriendo en aspectos clave del Derecho aplicable a este ámbito. Estas visiones divergentes responden a cuestiones

de ideología, intereses nacionales y diferentes interpretaciones de las normas de Derecho Internacional y de cómo debe ser la gobernanza de Internet. Por ejemplo, mientras que Estados Unidos considera que el marco jurídico internacional es adecuado tal y como está en la actualidad, China defiende que son necesarios nuevas normas para abordar problemas únicos que actualmente carecen de soluciones aplicables (Zhixiong & Mačák. 2017, p. 278-281).

Es relevante, a su vez, la diferencia de ideología que se manifiesta en el ámbito de la gobernanza de Internet, puesto que, actualmente, el ciberespacio se caracteriza por su descentralización y por las dificultades que tienen los Estados de controlar lo que sucede en la Red. En este sentido, la infraestructura que aloja los diferentes componentes técnicos e informáticos del ciberespacio se encuentra distribuida en forma de numerosos proveedores y servidores en diferentes Estados, lo cual supone que el poder de la soberanía estatal se encuentra, teóricamente, muy limitado. No obstante, los Estados han conseguido, poco a poco, introducir sus normas jurídicas en el ciberespacio (el mejor ejemplo de ello es la Unión Europea y el gran esfuerzo de los Estados Miembros en materias como la Protección de Datos). Sin embargo, los Estados occidentales buscan mantener este carácter descentralizado de Internet en buena parte, mientras que China, por otra parte, busca que el Estado tenga un gran poder también en esta área (Zhixiong & Mačák, 2017, p. 285-287).

En definitiva, habrá que esperar unos años para que el ciberespacio pueda contar con un acuerdo u otra norma de Derecho Internacional que permita regular los aspectos más innovadores y problemáticos que en la actualidad el Derecho Internacional clásico aborda de forma insuficiente. Desde la esfera de los sujetos estatales que componen la comunidad internacional no parece existir mucho interés en comenzar a desarrollar esta materia, en la medida que los intereses y la confidencialidad de sus posturas y capacidades son más importantes para los Estados que la regulación internacional del ciberespacio. Además, las diferentes visiones de carácter ideológico y cultural han provocado diferencias aún más marcadas que sobrepasan el tema jurídico y de seguridad.

En última instancia, se trata de una vez más de la lucha entre la cultura democrática de Occidente y el mayor control y autoritarismo de otros Estados, que buscan restringir la esfera individual incluso en el ciberespacio. Desde ninguno de estos extremos se va a ceder respecto al otro, en la medida que eso significaría renunciar en ciertos aspectos a su ideología. Por este motivo, no se considera previsible que existan mayores avances en los

próximos años que aquellos aportados por actores no estatales como el grupo de expertos autores del Manual de Tallin 2.0, que se ha convertido en una obra de referencia clave para abordar este tema.

No obstante, hay que señalar que, históricamente, ha habido situaciones similares con otras materias. Es coherente que las infraestructuras internacionales de gobernanza tarde un tiempo en construirse, en la medida que los Estados buscan obtener un mayor entendimiento del potencial estratégico de estos fenómenos (Franzese, 2009, p. 38). Una vez lo logren, su voluntad y predisposición para someterse a normas legalmente vinculantes será más elevada y, en consecuencia, habrá mayores oportunidades de lograr acuerdos que permitan la regulación del ciberespacio con un amplio consenso. Hasta entonces, serán los actores no estatales los protagonistas de estas primeras fases de adaptación del Derecho Internacional al ciberespacio, como ya ha quedado de manifiesto con las dos versiones del Manual de Tallin. En cualquier caso, a medio plazo, los Estados deberían reclamar su posición clásica como sujetos creadores de normas de Derecho Internacional. A corto plazo, se puede esperar que los Estados participen más activamente en la interpretación de las normas de Derecho Internacional vigentes al ámbito del ciberespacio. Todo esto permitirá, en el largo plazo, la aparición de la *opinio juris* respecto de los principios fundamentales aplicables al ciberespacio (Mačák, p. 138).

1.2. La Responsabilidad Internacional de los Estados en el Derecho Internacional Público: Determinación del régimen jurídico y análisis de la Resolución 56/83, de la Asamblea General, de Responsabilidad del Estado por hechos internacionalmente ilícitos.

Este apartado tiene por objeto delimitar la aplicación del concepto de la Responsabilidad Internacional de los Estados en los ciberataques orquestados por actores no estatales desde sus territorios. Para ello, es necesario analizar detalladamente el concepto de Responsabilidad Internacional en el Derecho Internacional Público, sus orígenes, su aplicación en la jurisprudencia, sus características y su aplicabilidad en el ámbito de la Ciberseguridad. Una vez analizado que, efectivamente, el Derecho Internacional es aplicable al ciberespacio, en este apartado se analizará este concepto desde una perspectiva puramente legal, con la finalidad de construir el marco teórico necesario para la correcta fundamentación y conclusión de este trabajo.

Actualmente, la Responsabilidad Internacional de los Estados es una de las pocas materias reguladas detalladamente en el ámbito internacional, en este caso a través de la Resolución 56/83 de la Asamblea General de Naciones Unidas, de Responsabilidad del Estado por hechos internacionalmente ilícitos de 2001. El marco jurídico que proporciona esta Resolución es fundamental para determinar la aplicabilidad de este concepto en el ámbito de los ciberataques, en la medida que delimita los conceptos, criterios, tipos de incumplimiento de obligaciones, efectos y normas para tener en cuenta en materia de Responsabilidad Internacional.

No obstante, la Resolución 56/83, que será la principal base jurídica de este apartado, es el resultado de un largo proceso, puesto que la aparición de este concepto por primera vez se remonta a 1928. En este año, la Corte Permanente de Justicia Internacional estableció, en el caso *Chorzov*, un principio básico del Derecho Internacional, concluyendo que el incumplimiento de una obligación legal supone la atribución de la responsabilidad de reparar el daño causado (Dimitrovska, 2015, p. 2). Posteriormente, la evolución de la sociedad internacional hacia una comunidad caracterizada por el multilateralismo y la persecución del interés común de la comunidad internacional en su conjunto marcó la evolución del Derecho Internacional Público. De hecho, este factor fue clave en la preparación y posterior aprobación de la Resolución 56/83, puesto que la Responsabilidad Internacional fue elegida como una de las primeras catorce áreas para la codificación por la Comisión de Justicia Internacional (Dimitrovska, 2015, p. 3).

De esta forma, la Responsabilidad Internacional de los Estados se ha configurado como uno de los principios más relevantes del Derecho Internacional. Como tal, refleja sus principios y espíritu, puesto que se fundamenta en la igualdad y soberanía de los Estados en la sociedad internacional (Bergwik, 2020, p. 23). Tiene por objeto limitar la soberanía de los Estados en su política exterior cuando esta tenga por objeto causar un daño a otro Estado (Dimitrovska, 2015, p. 4). En consecuencia, este principio estipula, en su artículo primero, que "Todo hecho internacionalmente ilícito del Estado genera su responsabilidad internacional" (AG Resolución 56/83, Art.1). Como se puede observar, se establece la igualdad entre los Estados, puesto que determina la aparición de la responsabilidad internacional cuando un Estado comete un acto internacionalmente ilícito contra otro Estado, independientemente de su condición.

Además, con el término "hecho internacionalmente ilícito", pretende incluir cualquier tipo de acto ilícito que pueda cometer un Estado, indiferentemente de su

naturaleza o de si es consecuencia de la acción, omisión o fracaso en actuar del Estado (Bergwik, 2020, p. 23). Es decir, atendido a la literalidad de la Resolución, sí cabría la Responsabilidad Internacional de un Estado en el ámbito de los ciberataques. Sin embargo, hay que tener en cuenta que el propio artículo indica que deben ser los Estados los que cometan dichos actos ilícitos. Por tanto, habrá que examinar de forma separada qué relación tiene que haber entre el Estado y un actor no estatal para que el primero sea responsable por los actos ilícitos del último. Es decir, las formas de atribución de un comportamiento susceptible de causar un supuesto de Responsabilidad Internacional conforme a lo previsto en el Capítulo II de la Resolución 56/83.

Otro aspecto relevante de la figura jurídica de la Responsabilidad Internacional es la cuestión de qué puede considerarse como "hecho internacionalmente ilícito". En primer lugar, hay un hecho internacionalmente ilícito del Estado cuando un comportamiento consistente en una acción u omisión es atribuible al Estado según el derecho internacional y constituye una violación de una obligación internacional del Estado (AG Resolución 56/83, art. 2). En segundo lugar, establece el art. 3 que la calificación del hecho como internacionalmente ilícito se rife por el derecho internacional (AG Resolución 56/83, art. 3). Es decir, la calificación del hecho ilícito no se verá afectada por las disposiciones de derecho interno aplicables, si las hubiere, si no por el incumplimiento de una obligación internacional que tuviera el Estado. De esta forma, la Resolución pretende restringir el margen de actuación de los Estados, mantener la naturaleza de esta figura jurídica y dotar de unidad al Derecho Internacional en conceptos tan relevantes como es el de hecho internacionalmente ilícito.

Por tanto, de acuerdo con lo examinado hasta este punto, habrá Responsabilidad Internacional de los Estados cuando se incumpla una obligación internacional mediante la realización de un acto internacionalmente ilícito y se genere un daño a otro Estado. Sin embargo, no cualquier hecho internacionalmente ilícito genera Responsabilidad Internacional. Solo lo harán aquellos actos que constituyan una violación de una obligación cuando el Estado se halle vinculado por dicha obligación en el momento que se produce el hecho (AG Resolución 56/83, art. 13). El ámbito temporal de aplicación es fundamental, puesto que todos los hechos anteriores, por muy ilícitos que sean, no serán objeto de Responsabilidad Internacional si el Estado no se hallaba vinculado a esa obligación. Por último, es necesario destacar que "hay violación de una obligación internacional por un Estado cuando un hecho de ese Estado no está en conformidad con

lo que de él exige esa obligación, sea cual fuere el origen o la naturaleza de esa obligación" (AG Resolución 56/83, art. 12). Por ejemplo, en el ámbito de los ciberataques, si un Estado ha suscrito un acuerdo internacional de no atacar infraestructuras críticas a través de ciberataques y lo hace, ese Estado sería responsable por infringir el contenido de dicho acuerdo, siempre que ya lo hubiera firmado en el momento de realizar el ciberataque.

El quebrantamiento de cualquier obligación a la que se halle sujeta el Estado y que suponga que ese Estado es sujeto de Responsabilidad Internacional tiene como consecuencia la necesidad de reparar el daño causado (Dimitrovska, 2015, p. 8). En este sentido, las consecuencias legales del Estado por el hecho internacionalmente ilícito cometido no le eximen de cumplir con la obligación legal originaria de Responsabilidad Internacional. Así lo establece el art. 29 de la Resolución 56/83 de la AG, que establece que "Las consecuencias jurídicas del hecho internacionalmente ilícito con arreglo a lo dispuesto en esta parte no afectan la continuidad del deber del Estado responsable de cumplir la obligación violada".

Las consecuencias legales de infringir una obligación vinculante comprenden, por un lado, la obligación de poner fin al hecho ilícito y de ofrecer garantías de no repetición (AG Resolución 56/83, art. 30). Por otro lado, se impone la obligación del Estado de reparar íntegramente el perjuicio, tanto material como moral, causado por el hecho internacionalmente ilícito (AG Resolución 56/83, art. 31). Esta reparación deberá, en la medida de lo posible, anular todas las consecuencias del acto internacionalmente ilícito cometido y restituir la situación que hubiera existido si no se hubiera realizado el acto, conforme a la definición aportada por la Corte Permanente de Justicia Internacional en el caso *Chorzow*. Sin embargo, esta premisa es extremadamente idealista, puesto que no es posible, en la mayoría de las ocasiones, restituir la situación anterior al daño causado. De hecho, incluso se puede afirmar que no conviene al Estado atacante utilizar la restitución como forma de reparación, en la medida que el hecho internacionalmente ilícito se ha cometido con un objetivo específico de los intereses nacionales de ese país.

Debido a esta situación, la Resolución 56/83 prevé varias formas de reparación en sus artículos 35 al 37 con el objetivo de que un Estado no salga indemne de la comisión de un hecho internacionalmente ilícito: restitución, compensación y satisfacción. En torno a esta cuestión es necesario destacar varios elementos. En primer lugar, es preferible que la reparación se realice a través de la regla de la restitución en la medida de lo posible. En

segundo lugar, se permite la combinación de varias de estas formas, con el objeto de intentar reparar el daño causado en la medida de lo posible (AG Resolución 56/83, art. 34). En tercer y último lugar, las reparaciones no tienen carácter retributivo, ya que, aunque pueden variar cualitativamente, su único objeto es reparar exclusivamente el daño causado (Dimitrovska, 2015, p. 9).

La forma más frecuente de reparación en el Derecho Internacional es la de la indemnización regulada en el art. 36 de la Resolución 56/83. En él, se establece que el Estado responsable de un hecho internacionalmente ilícito está obligado a indemnizar el daño causado (y por el lucro cesante) por ese hecho en la medida en que dicho daño no sea reparado por la restitución (AG Resolución 56/83, art. 36). Como se puede observar, y si se atiende a lo establecido en la Resolución, la indemnización es una forma de reparación puramente subsidiaria de la restitución, y únicamente se aplicará cuando la restitución no sea materialmente imposible (circunstancia que suele ocurrir en el ámbito del ciberespacio debido a la naturaleza del ataque) y no entrañe una carga totalmente desproporcionada con relación al beneficio que derivaría de la restitución en vez de la indemnización (AG Resolución 56/83, art. 35).

No obstante, hay ocasiones en las que el daño causado por un hecho internacionalmente ilícito no puede repararse por la restitución o la indemnización. Estos supuestos suelen responder a los hechos ilícitos que causan daños morales o un sentimiento específico de injusticia. Para estos supuestos, se prevé que la reparación pueda realizarse a través de la satisfacción. Este medio incluye la realización de diferentes actos, como, por ejemplo, el reconocimiento público de la comisión del hecho, disculpas formales, compromiso de que no volverá a repetirse… (Dimitrovska, 2015, p. 9). En cualquier caso, se establece una limitación importante a esta forma de reparación con el objeto de favorecer su aplicación.

El art. 37.3 de la Resolución 56/83 prevé que "La satisfacción no será desproporcionada con relación al perjuicio y no podrá adoptar una forma humillante para el Estado responsable" (AG Resolución 56/83, art. 37). Por esta vía se busca conseguir que realmente exista una reparación total del daño causado por el hecho internacionalmente ilícito. Al mismo tiempo, se intenta favorecer la reconciliación de los Estados en conflicto, con el objeto de evitar en una escalada de tensión o de rencor que suponga ulteriores incumplimientos del Derecho Internacional. En cualquier caso, la opción más viable y conveniente es la combinación de las tres vías de reparación, de

forma que todo daño, tanto material como moral, que pudiera haberse causado quede cubierto por la reparación realizada por un Estado en el marco de su Responsabilidad Internacional por la comisión de hechos internacionalmente ilícitos.

Como se puede observar, la cuestión de determinar el tipo de reparación a aplicar no es sencilla y depende de numerosos factores. En el ámbito de los ciberataques es aún más complejo, tanto por las dificultades en determinar la atribución de la Responsabilidad por los mismos, como en cuantificar los daños causados. En este sentido, un ciberataque puede tener efectos negativos prolongados en el tiempo o que no sean descubiertos hasta que pasan meses e incluso años. En una época en la que cada vez son más frecuentes este tipo de ataques, ya no solo contra individuos, sino también contra infraestructuras críticas, la existencia de un marco regulador claro es imprescindible. Es inaceptable que los Estados responsables no reparen el daño causado a las infraestructuras críticas de otros Estados por cuestiones jurídicas, como sería la de la atribución, que será analizada detenidamente en el apartado 1.3.

No obstante, cabe plantearse la cuestión de si la Resolución 56/83 es realmente eficaz y las normas contenidas en ella son respetadas y aplicadas por los Estados. Hay que recordar que esta Resolución forma parte del Derecho Internacional Público y, como tal, representa el acuerdo al que han llegado a los Estados para establecer unas reglas generales aplicables a las relaciones entre ellos (Schmitt, 2014, p. 272). La creación y evolución de estas normas internacionales dependen, fundamentalmente, del contexto internacional que exista en cada momento. En este sentido, estas reglas de Derecho Internacional Público aparecerán, serán modificadas y se extinguirán conforme evolucione la historia y los intereses de cada época específica. Si bien hay diferentes sujetos que influyen en esta evolución normativa, como, por ejemplo, las ONG u otros sujetos de Derecho Público no estatales; en última instancia siempre son los Estados los que deciden sobre la vigencia de esas reglas.

En definitiva, el proceso de creación y evolución de las normas de Derecho Internacional Público está dirigido por los Estados. Esta afirmación quedó reflejada en el caso *Lotus* de 1927, en el que la Corte Permanente de Justicia Internacional estableció el siguiente precepto que ha quedado para la posterioridad:

> *"International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in*

conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims[10] (*Lotus*, 1927, p. 18)*"*.

En consecuencia, el proceso de creación de una norma de Derecho Internacional puede resumirse en los siguientes pasos: en primer lugar, aparece una situación que exige una respuesta a nivel internacional. En segundo lugar, los Estados, dependiendo de sus intereses nacionales, acuerdan o no la creación de marcos jurídicos materiales o costumbres que regulen las relaciones entre ellos en un determinado ámbito. En tercer lugar, prestan su consentimiento para someterse a esas normas, bien a través de los tratados o bien participando en prácticas provenientes de la *opinio juris* y que acaban convirtiéndose en derecho internacional consuetudinario cuando se extiende entre un gran número de Estados (Schmitt, 2014, p. 272).

Estos mismos principios aplicables al Derecho Internacional están muy vigentes en el ámbito del ciberespacio. Actualmente, esta área se encuentra en una época muy convulsa y cambiante debido a la evolución constante de la tecnología existente y la aparición de nuevas tecnologías que exigen una constante revisión y actualización de las normas jurídicas, tanto a nivel internacional como nacional. No obstante, hay que ser optimistas respecto al futuro de la regulación en el Derecho Internacional Público de los ciberataques y similares, debido a los intereses estatales en juego. Como bien se ha mencionado el párrafo anterior, la aparición y asimilación de nuevas normas internacionales dependen de los intereses de los Estados, en este caso, en el ciberespacio. La gran dependencia actual en las tecnologías y en Internet para la prestación de servicios fundamentales para el Estado, como es el suministro eléctrico o el funcionamiento de hospitales etc., provoca que sea previsible un esfuerzo por parte de los Estados a nivel internacional para crear un marco jurídico que ayude a proteger estas infraestructuras críticas (Schmitt, 2014, p. 273).

En cualquier caso, la eficacia de estas normas está en entredicho, puesto que, en última instancia, son los propios Estados los que deciden si atenerse o no a las consecuencias de sus actos internacionalmente ilícitos. Además, conforme se vayan

[10] Traducción propia: "El Derecho Internacional rige las relaciones entre Estados independientes. Las reglas legalmente vinculantes entre Estados, por tanto, emanan de su propia y libre voluntad, como bien se expresa en los acuerdos internacionales o en las costumbres aceptadas como principios del derecho y establecidas con el objeto de regular las relaciones entre estas comunidades independientes o con el objetivo de lograr la consecución de objetivos comunes".

regulando y restringiendo las diferentes opciones existentes de actuar en el ciberespacio, serán los propios Estados los que busquen nuevas vías de aprovecharse de las oportunidades que ofrece este campo. Un ejemplo de ello es la figura de los ciberataques realizados por actores no estatales, una vía que China y Rusia utilizan muy frecuentemente para perpetrar ciberataques contra otros países sin utilizar órganos ni mecanismos estatales. La dificultad para trazar el origen de los ciberataques y vincularlos con las autoridades de esos Estados provoca que no puedan atribuírseles estos ataques y que, en consecuencia, las normas de Derecho Internacional aplicables pierdan su eficacia.

2. LA ATRIBUCIÓN DE LA RESPONSABILIDAD INTERNACIONAL DE LOS CIBERATAQUES: LA NECESIDAD DE UN NUEVO MECANISMO JURÍDICO.

El artículo 2 de la Resolución 56/83 de la Asamblea General de Naciones Unidas, de Responsabilidad del Estado por hechos internacionalmente ilícitos de 2001 prevé que un hecho internacionalmente ilícito de un Estado genera su responsabilidad internacional cuando hay un comportamiento consistente en una acción u omisión que es atribuible al Estado según el Derecho Internacional. 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. Es, además, una cuestión delicada en el Derecho Internacional, pero especialmente en el ámbito del ciberespacio, debido a las dificultades de trazabilidad de los ciberataques, que será estudiado en los párrafos siguientes.

Sin embargo, antes de profundizar en el problema de la atribución de la Responsabilidad en el ámbito 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 commentaries*, en el cual los miembros de la Comisión de Derecho Internacional analizan el contenido de los artículos de la resolución 56/83 de la AG. La cuestión que aborda este comentario es muy relevante a efectos del presente Trabajo de Fin de Grado, 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"[11] (*Draft articles on Responsibility of States for Internationally Wrongful Acts, witch commentaries*, 2001, comentario 2º).

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, puesto que bastaría una mera 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 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[12]. En definitiva, 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 u autoridades del Estado y los actores no estatales.

Este elemento supone la aparición de una doble problemática: por un lado, las dificultades de la atribución de la Responsabilidad por las acciones cometidas 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. No obstante, antes de analizar qué respuesta es más adecuada a cada uno de estos supuestos, hay que abordar el problema común a ambos: las dificultades de atribución en el ciberespacio.

La cuestión de la atribución de la responsabilidad internacional es un problema complejo de por sí, puesto que supone el análisis de numerosos factores y la utilización

[11] Traducción propia: "En teoría, el comportamiento de todos los seres humanos, corporaciones y colectivos vinculados al Estado a través de la nacionalidad, residencia habitual o incorporación podría ser atribuido al Estado, tengan o no una conexión con el Gobierno".

[12] "*In international law, such an approach is avoided, both with a view to limiting responsibility to conduct which engages the State as an organization, and also so as to recognize the autonomy of persons acting on their own account and not at the instigation of a public authority. Thus, the general rule is that the only conduct attributed to the State at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e. as agents of the State*" (*Draft articles on Responsibility of States for Internationally Wrongful Acts, witch commentaries*, 2001, comentario 2º).

Traducción propia: "En Derecho Internacional, tal aproximación se evita con el objeto de limitar la responsabilidad a conductas que implican al Estado como organización, así como para reconocer la autonomía de la persona actuando por cuenta propia y sin la instigación de una autoridad pública. Por ello, la regla general es que únicamente la conducta atribuida al Estado en el ámbito internacional solo se producirá si se ha producido por parte de órganos del gobierno u otros sujetos que han actuado bajo su dirección, instigación o control de esos órganos".

de los diferentes medios de prueba que se puedan conseguir para aplicar el Derecho Internacional. Sin embargo, en el ámbito del ciberespacio es un problema que se agudiza en gran medida y que, actualmente, es un foco de discusión doctrinal en el ámbito de la ciberseguridad.

En cualquier caso, antes de proceder a realizar un análisis de las dificultades y riesgos que entraña el intentar atribuir un ciberataque a un actor y/o individuo concreto y vincular dicha actuación con un Estado, es necesario concretar los conceptos de atribución que se van a utilizar en este apartado. En primer lugar, hay que recordar que, 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" (Cocchini, 2021, p. 77). En definitiva, la capacidad de imputar la conducta realizada por una entidad o individuo al Estado. Sin embargo, como bien indica esta autora, 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.

2.1. Las dificultades técnicas de atribución de los ciberataques a actores concretos.

El principal problema al que hay que hacer frente en este ámbito en relación con la atribución técnica es el de la trazabilidad y el anonimato. En este sentido, es la propia estructura tecnológica de la red lo que provoca que sea tan complejo atribuir un ciberataque a una persona o entidad determinada (Tran, 2018, p. 386). 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.

Tran explica muy bien todo este proceso de carácter más técnico que tiene tanta influencia sobre la atribución de un ciberataque (Tran, 2018, p. 387-389). En este sentido, señala que todo ello es posible gracias a las facilidades que proporciona la tecnología actual de ocultar o falsificar los identificadores de los dispositivos. A este respecto, a la

hora de usar Internet, el dispositivo utilizado tiene que encontrar una vía de comunicación con el servidor que aloja el contenido específico, y este servidor, una vez recibida la solicitud, envía los datos de vuelta al dispositivo. Esto se realiza a través de los *Internet Protocol* (en adelante, IP), que son direcciones virtuales que se asignan a los dispositivos por el proveedor de telecomunicaciones correspondientes. A través de estas direcciones 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 ocultadas (Chircop, 2018, p. 646-647). En este sentido, 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.

Es más, incluso si se pudiera identificar a la persona concreta que ha realizado el ciberataque, la atribución del mismo, como bien se analizará en el próximo apartado, 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 (Payne & Finlay, 2017, p. 561). Y, aunque la Resolución 56/83 aborde correctamente este ámbito, la presencia de actores no estatales tan activos y sofisticados como los que se encuentran en el ciberespacio provocan que dichos artículos sobre la Responsabilidad Internacional de los Estados queden obsoletos. Es más, esos actores disfrutan de un nivel de inmunidad significativo frente a las consecuencias de los ciberataques que cometido (Chircop, 2018, p. 646-647).

En definitiva, como se puede observar, las dificultades de atribución de carácter técnico no pueden evitarse con carácter general, puesto que eso supondría rediseñar completamente la estructura de la Red (Payne & Finlay, 2017, p. 560). Esta posible vía de solucionar el problema, aparte de los costes que lleva aparejados, supondría despojar a Internet de algunas de sus principales características: velocidad, eficiencia y confianza. Es más, aunque se lograra identificar en todos los casos a los dispositivos desde los cuales se han lanzado los ciberataques, esto no supondría resolver de forma automática el problema de la atribución. Hay que tener en cuenta que se identificaría el dispositivo atacante, pero no la persona que ha diseñado, ordenado o lanzado efectivamente el ataque.

Siempre existirá el riesgo de que un dispositivo haya sido utilizado por un atacante distinto al de su propietario a través de un robo físico o incluso pirateando ese dispositivo.

2.2. Las dificultades jurídicas de atribución de los ciberataques a actores concretos.

Si a pesar de todas las dificultades técnicas descritas en el apartado anterior un Estado lograra identificar de forma clara y fiable al dispositivo y al individuo que provocó el ciberataque, aún tendría que superar las dificultades jurídicas de atribución para lograr que ese Estado se hiciera responsable internacionalmente por los daños causados por ese ciberataque, especialmente si el sujeto identificado fuera un actor no estatal. La falta de una normativa internacional clara respecto a los criterios jurídicos de atribución ha causado que la construcción de esta figura se realice a través de la jurisprudencia del CIJ, que es bastante constante y clara al respecto.

En este sentido, como bien indica Cocchini, la sentencia más relevante de la Corte Internacional de Justicia a este respecto es la del caso de las *Actividades militares y paramilitares en Nicaragua y contra Nicaragua* (1986), en el que la CIJ se pronuncia respecto al problema de la atribución de la responsabilidad internacional de los Estados por su implicación con actores no estatales (Cocchini, 2021, p. 78). En ella, el CIJ 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" (Nicaragua, 1986, párrafo 115). En definitiva, conforme al criterio de la CIJ, únicamente habría responsabilidad internacional del Estado si se prueba que tenía control efectivo de las operaciones, lo cual supone que se excluyen del ámbito de la responsabilidad actividades tales como la financiación, organización equipamiento y planificación de las acciones armadas de un actor no estatal.

Esta línea jurisprudencial mantenida por el CIJ no parece muy lógica, puesto que niega la responsabilidad internacional del Estado por acciones realizadas por actores no estatales sobre las cuales no disponía de control efectivo. Sin embargo, hay que tener en cuenta que, sin esas actividades de carácter "secundario" realizadas por los Estados, como son las de financiación, planificación o suministro, los actores no estatales no habrían podido, en muchas ocasiones, perpetrar tales acciones. En consecuencia, existe una falta

de atención a la naturaleza de la figura jurídica de la responsabilidad de los Estados por parte del CIJ. La polémica de esta doctrina se pudo apreciar posteriormente en el caso *Tadic*, del Tribunal Penal Internacional para la ex-Yugoslavia (TPIY), que intentó flexibilizar el criterio de control efectivo por uno más orientado al control general. En este sentido, establece el tribunal que:

> *The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group. Acts performed by the group or members thereof may be regarded as acts of de facto State organs regardless of any specific instruction by the controlling State concerning the commission of each of those acts* (*Tadic*, 1999, párr. 137)[13].

Es decir, concluye el Tribunal que el principio que debe seguir la atribución de la responsabilidad internacional debe ser la del control general, en el cual se incluyen todas las acciones de coordinación, financiación, preparación etc. que desechó en primera instancia la CIJ. Este criterio parece mucho más acertado en atención a la naturaleza jurídica de la figura de la responsabilidad internacional de los Estados, que no es otra que penalizar los hechos internacionalmente ilícitos cometidos por las entidades o individuos que conforman la entidad jurídica del Estado. Sin embargo, la CIJ ha mantenido el criterio del control efectivo en sentencias posteriores como el caso de las *Actividades armadas en el territorio del Congo*, de 2004, o la del caso de la *Aplicación de la Convención para la prevención y la represión del crimen de genocidio* de 2007, descartando la doctrina marcada por el TPIY.

En definitiva, según la jurisprudencia de la CIJ, no se podría atribuir, casi en ningún caso, la responsabilidad internacional a un Estado por los ciberataques lanzados por actores no estatales desde sus territorios, en la medida que únicamente habrían de escudarse en que no existía un control efectivo o instrucciones por parte del Estado. Este

[13] Traducción propia: "El control exigido por el Derecho Internacional puede considerarse que existe cuando un Estado (o, en el contexto de un conflicto armado, la Parte del conflicto) tiene un papel en organizar, coordinar o planificar las acciones militares de un grupo militar, además de financiar, entrenar y equipar o proporcionar apoyo operacional a ese grupo. Los actos realizados por ese grupo pueden ser, por tanto, considerado como actos de órganos estatales de facto, indiferentemente de que exista ninguna instrucción específica por el Estado que ostenta el control en relación con la comisión de cada uno de eso actos".

factor indica que el mecanismo de la responsabilidad internacional ha quedado obsoleto ante la evolución de la tecnología y de las vías que tienen los Estados de realizar actos internacionalmente ilícitos a través de actores no estatales, sin necesidad de tener un control efectivo sobre ellos. Un Estado podría proporcionar el *Software* y los medios necesarios a una organización para que realizara un ciberataque masivo a las infraestructuras críticas de otro país dando total libertad a ese actor para hacer lo que considere oportuno una vez proporcionados los medios. Según esta doctrina, el Estado no sería responsable por ese ciberataque, a pesar de que existe una participación activa del mismo.

Hay que recordar que en el contexto actual es muy frecuente que existan diferentes niveles de cooperación o vinculación entre los Estados y los actores no estatales que desarrollan este tipo de actuaciones ilícitas. En última instancia, se trata de una cuestión de interés nacional, que en muchas ocasiones coincide con la visión que sujetos nacionales de esos Estados tienen respecto a un determinado tema (Chircop, 2018, p. 646-647). En consecuencia, es necesario que dentro de la figura de la Responsabilidad Internacional por hechos internacionalmente ilícitos exista un espectro que diferencie entre los diferentes niveles de vinculación del Estado y los perpetradores del ataque.

Esta problemática es a la que intentaba responder la doctrina de la CIJ en las sentencias anteriormente analizadas. Esta jurisprudencia excluiría a los primeros estadios de actuaciones estatales, basados en una actuación más pasiva, y se centraría en sancionar y restituir el daño causado por las que hayan tenido una participación más activa del Estado. El criterio de control efectivo no incluiría, en primer lugar, las actuaciones ignoradas por el Estado, en las que las autoridades nacionales conocen que se va a producir el ataque, pero, no solo no intervienen para detenerlo, sino que incluso lo apoyan por cuestiones relacionadas con el interés nacional. En segundo lugar, tampoco abarcaría aquellos ataques fomentados desde el propio Estado y cometidos por actores no estatales. En tercer y último lugar, el Estado tampoco sería responsable por aquellos ciberataques cometidos por terceros, pero que han contado con un apoyo y/o coordinación activa por parte del Estado (Healey, 2012, p. 3).

Como se puede observar, con esa política de control efectivo señalada por la CIJ la mayoría de los ciberataques actuales quedarían impunes en términos de responsabilidad. No obstante, como bien indican autores como Cocchini o Pastor Ridruejo, la práctica y doctrina internacionales tras los atentados del 11 de septiembre

han mostrado una tendencia opuesta a la señalada por la jurisprudencia de la CIJ, en la medida que ha quedado más que demostrado que un actor no estatal puede realizar acciones tan letales como las de un Estado sin necesidad de contar con las instrucciones o el control efectivo del Estado territorial (Cocchini, 2021, p. 80). Por ejemplo, en el caso de los movimientos insurreccionales, el Estado no sería responsable por los hechos internacionalmente ilícitos que realicen esos sujetos, "a no ser que, eventualmente, los órganos del Estado hayan dejado de cumplir las obligaciones de vigilancia, prevención o represión que les incumben" (Pastor, 2017, p. 593).

Desde la esfera jurídica internacional se enfrentan los sujetos de Derecho Internacional Público a una disyuntiva: respetar la soberanía de los Estados o atender a la naturaleza de la norma. La situación es similar a la que tuvo que enfrentarse la CIJ en el asunto de *Actividades militares y paramilitares en Nicaragua y contra Nicaragua* (1986). Sin embargo, hay una clara evolución de criterio de los sujetos internacionales, en la medida que es necesario adaptar el Derecho Internacional a las nuevas amenazas y a un contexto internacional que se encuentra en constante cambio.

El objetivo de esta evolución no es otro que evitar que haya Estados que "burlen" el mecanismo de la Responsabilidad Internacional argumentando que no ostentaban el control efectivo sobre los atacantes o que no tenían conocimiento de sus actividades. Resulta inevitable, pues, la creación de nuevas figuras jurídicas que insten a las autoridades y órganos del Estado a prevenir estas actuaciones y actuar contra ellas de forma contundente y sancionar las negligencias que se hayan producido. Esa nueva figura jurídica atributiva de responsabilidad no es otra que la diligencia debida, a través de la cual se puede considerar responsable al Estado territorial por no haber querido o podido atajar una amenaza, en este caso, cibernética (Chircop, 2018, p. 644-645); en línea con el criterio utilizado respecto de los movimientos insurreccionales y que bien destaca Pastor Ridruejo.

La figura jurídica de la diligencia debida será la clave jurídico-teórica del presente Trabajo de Fin de Grado, puesto que es el mecanismo más adecuado y pertinente para determinar la responsabilidad internacional de los Estados en los ciberataques lanzados desde sus territorios por los actores no estatales. En este sentido, es necesario contar con una figura jurídica que permita atribuir la responsabilidad en un ambiente como el ciberespacio donde los hechos internacionalmente ilícitos suelen ser cometidos por actores no estatales, que, en algunos casos, pueden contar con un mayor o menor apoyo

del Estado del que forman parte. Además, para abordar esta problemática también serán claves las reglas contenidas en el *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, desarrollado por el grupo de experto de la OTAN. A través de estas dos figuras se intentará responder a la problemática de la atribución de la responsabilidad internacional en esta área y se tratará la posible configuración de estas reglas como un marco jurídico adecuado para responder a los desafíos legales producidos por la evolución tecnológica.

2.3. Análisis de la Responsabilidad Internacional de los Estados en los actos realizados por actores no estatales desde la perspectiva del Manual de Tallin 2.0.

Como bien se ha explicado en el apartado 1.1. del presente 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. En esta obra lo que se pretende es realizar 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. En consecuencia, este manual no tiene carácter vinculante, si bien proporciona conceptos, ideas e interpretaciones que pueden resultar claves para el correcto desarrollo, ya no solo de este trabajo, sino también de la evolución de la normativa internacional en relación con los desafíos creados por los ciberataques y el constante desarrollo del ciberespacio. Por ello, es pertinente y necesario dedicar un apartado en exclusiva a resumir y analizar la regla nº 17 del Manual, que aborda directamente la atribución de las ciberoperaciones realizadas por actores no estatales.

En este sentido, la Regla 17 del Manual de Tallin 2.0. 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; or

(b) the State acknowledges and adopts the operations as its own[14] (Schmitt, 2017, p. 94).

En relación con esta regla, concluye el Manual de Tallin 2.0. que, conforme a los artículos sobre la Responsabilidad de los Estados (Resolución 56/83), las ciberoperaciones realizadas por actores no estatales (tanto a nivel individual como grupal), no pueden atribuirse a los Estados. Esta regla general tiene, sin embargo, dos excepciones: cuando actúen bajo las instrucciones[15] 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 (Egan, 2017, p. 177).

Esta regla recoge, pues, la interpretación de la CIJ sobre el criterio de control efectivo respecto de la responsabilidad internacional de los Estados por hechos internacionalmente ilícitos cometidos por actores no estatales. De hecho, señala el Manual, con referencia a los Comentarios de la Resolución 56/83, 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" (Schmitt, 2017, p. 95). En definitiva, para que un Estado pueda ser considerado responsable por las actuaciones de un actor no estatal, sería necesario que tenga la capacidad tanto de generar el daño a través de los ciberataques como de ordenar su cese, conforme a la jurisprudencia de la CIJ en el caso *Nicaragua* ya explicado en el apartado anterior.

Es necesario recordar, antes de continuar el análisis del contenido del Manual de Tallin 2.0 respecto a la atribución de la responsabilidad internacional por hechos ilícitos cometidos por actores no estatales, que el Manual simplemente pretende proporcionar unas reglas generales creadas sobre la base de la legislación, jurisprudencia y doctrina internacionales existentes hasta la fecha. En consecuencia, puede concluirse que lo reflejado en él simplemente muestra la situación actual en el Derecho Internacional en

[14] Traducción propia de la regla:

"Regla 17 – La atribución de las ciberoperaciones realizadas por actores no estatales

Las ciberoperaciones realizadas por un actor no estatal será atribuible a un Estado cuando:

(a) se realice siguiendo sus instrucciones o bajo su dirección o control; o

(b) el Estado reconozca y adopte las operaciones como propias".

[15] Con "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.

relación con el ciberespacio y como responde a las diferentes situaciones que en él pueden darse.

El Manual concluye que, conforme a la situación normativa y doctrinal actual, el apoyo general por parte del Estado a un actor no estatal o a las ciberoperaciones cometidas por este es insuficiente para atribuir la responsabilidad al Estado. De hecho, ejemplifica esta afirmación señalando que la provisión de un *malware* por parte del Estado no sería generadora de responsabilidad estatal si no concurre el criterio de control efectivo. Aunque no sea un hecho generador de responsabilidad internacional, 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 externos de otro Estado". En definitiva, puede afirmarse 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.

Tras analizar como aborda la problemática el Manual de Tallin 2.0, principal obra de referencia en la actualidad para analizar cómo se aplica el Derecho Internacional al fenómeno del ciberespacio, no se puede más que concluir que la figura jurídica de la responsabilidad internacional está obsoleta. No obstante, es necesario precisar que no es un problema de la figura *per se*. Al contrario, el problema se deriva de una interpretación restrictiva, en exceso, de la normativa internacional existente. El criterio de la CIJ pudo ser adecuado para juzgar el caso de Nicaragua y probablemente lo siga siendo para juzgar actos más convencionales.

Sin embargo, 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. Por ello, como ya se ha mencionado en el apartado anterior, es necesaria la aplicación de una nueva figura para abordar todos aquellos actos internacionalmente ilícitos en el ciberespacio y que no quedan comprendidos dentro de la figura de la responsabilidad internacional. Esta figura no es otra que la diligencia debida, que ya tiene una larga trayectoria en otros ámbitos del Derecho Internacional y que se erige como principal alternativa hasta que se alcance un acuerdo a nivel internacional sobre el ciberespacio.

3. EL PRINCIPIO DE DILIGENCIA DEBIDA Y SU APLICACIÓN EN EL CIBERESPACIO

El análisis realizado de la aplicación del Derecho Internacional vigente al ciberespacio y a sus particularidades ha mostrado las dificultades existentes para crear un marco jurídico estable que sea aceptado por la amplia mayoría de la comunidad internacional y proporcione respuestas a los desafíos que presenta este nuevo ámbito de las relaciones internacionales. Como bien indica Schmitt, la comunidad internacional se encuentra en un dilema normativo. Por un lado, si los Estados adoptan de forma oficial interpretaciones del Derecho Internacional que restrinjan las ciberoperaciones, limitarán su propia libertad y capacidades en el ciberespacio. Por otro lado, es necesario determinar un marco jurídico mínimo que establezca límites a la libertad de los Estados en el ciberespacio y permita, así, proteger la infraestructura básica de los Estados (Schmitt, 2015, p. 69).

Observamos, en este aspecto, lo argumentado en el apartado 1.1 del presente trabajo, en el que se indicaba que las infraestructuras internacionales de gobernanza tardan un tiempo en construirse, en la medida que los Estados buscan obtener un mayor entendimiento del potencial estratégico de estos fenómenos (Franzese, 2009, p. 38). En consecuencia, y como es lógico, los Estados han optado por mantener una postura pasiva frente a los desafíos legales que genera el ciberespacio. Por ello, ha sido el discurso académico el que ha construido en estos últimos años la aplicación concreta del Derecho Internacional al ciberespacio. El mejor ejemplo de ello son los Manuales de Tallin escritos por el Grupo Internacional de Expertos, que han proporcionado una interpretación clara y específica de cómo se aplica el Derecho Internacional a este ámbito, convirtiéndose en obra de referencia para todo autor que entre a analizar el fondo de esta cuestión.

En este último apartado del presente Trabajo de Fin de Grado se analizará la pertinencia de aplicar el principio de diligencia debida a la problemática de la responsabilidad internacional de los Estados por los ciberataques lanzados por actores no estatales desde sus territorios como alternativa a la figura de la responsabilidad internacional. De esta forma, se pretende aportar nuevos argumentos que apoyen y justifiquen la necesidad de aplicar firmemente los principios existentes en el Derecho Internacional al ciberespacio, ya no solo como medio para proteger la ciberinfraestructura de los Estados, sino también como una necesidad de las sociedades democráticas para

proteger el sistema liberal ante los cada vez más frecuentes intentos de manipular las elecciones o de paralizar infraestructuras básicas por parte de determinados Estados.

3.1. El principio de diligencia debida en el Derecho Internacional.

El principio de diligencia debida se erige como la mejor alternativa a la limitada figura de la responsabilidad internacional, que únicamente es aplicable al ámbito de los ciberataques en supuestos muy tasados. Recordemos, como se analizó en el apartado 2.2, que, en el caso sobre las *Actividades militares y paramilitares en Nicaragua y contra Nicaragua* (1986), el CIJ 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" (CIJ, 1986, párrafo 115).

Esto supondría 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. El propio Manual de Tallin 2.0 acoge esta interpretación, alegando que "*as a general rule, the cyber operations of private persons or groups are not attributable to States*"[16], admitiendo como excepciones los supuestos de control efectivos planteados por la CIJ (Manual de Tallin, 2017, p. 95).

En consecuencia, aunque la responsabilidad internacional de los Estados sea una figura más contundente como medio para prevenir y sancionar los hechos internacionalmente ilícitos cometidos por un Estado o en/desde su territorio, no resulta aplicable al supuesto de hecho que trata el presente trabajo. En contraste, el principio de diligencia debida tiene una larga trayectoria en el Derecho Internacional y su construcción jurisprudencial da cabida a la responsabilidad de los Estados por los actos cometidos por actores no estatales desde sus territorios. Por todo ello, es el principio de Derecho Internacional que mejor puede abordar esta cuestión hasta que los Estados acuerden un marco jurídico específico que sea aplicable al ciberespacio o se consolide una *opinio juris* en una dirección determinada.

[16] Traducción propia: "Como regla general, las ciberoperaciones realizadas por personas o grupos privados no son atribuibles a los Estados".

La construcción jurisprudencial del principio de diligencia debida y su aceptación por los Estados se remonta a 1872, fecha en la que Estados Unidos y Reino Unido se sometieron al arbitraje del Tribunal previsto en el marco del Tratado de Washington de 1871, por una supuesta violación de la neutralidad inglesa durante la guerra civil estadounidense conocida como las "*Alabama Claims*" (Patrick, 2019, p. 586). En este sentido, se establecía en el Tratado 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"* (*Alabama Claims*, 1871, p. 127)[17].

Como se puede observar en el caso expuesto en el apartado anterior, la cuestión de la diligencia debida se remonta al siglo XIX. En el caso *Tellini*, de 1923, la Sociedad de Naciones creó un comité para investigar el asesinato de algunos miembros de una comisión internacional, concluyendo que un Estado podría ser responsable por los hechos ilícitos cometidos en su territorio si no adoptara todas las medidas razonables para prevenirlo y perseguir a los responsables (Cocchini, 2021, p. 13).

Sin embargo, no será hasta el *Trail smelter case (United States, Canada)*, de 1941, cuando el principio de diligencia debida empezará a cobrar una mayor relevancia en el Derecho Internacional. En este caso, se estableció que Canadá debía utilizar medidas de protección y prevención para reducir la contaminación en el valle del río Columbia, causado por plantas de fundición en territorio canadiense (Stockburger, 2018, p. 249). Estableció a este respecto el tribunal de arbitraje que:

> *Under the principles of international law, […] no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence*[18] (*Trail Smelter*, 1941, p. 62).

[17] Traducción propia: "Los medios legales insuficientes no pueden justificar el fracaso de la diligencia debida".

[18] Traducción propia: "Bajo los principios del Derecho Internacional, ningún Estado tiene el derecho a usar o permitir el uso de su territorio de forma tal que los humos causen daño en el territorio o al territorio de

En relación con el caso *Trail Smelter* es necesario destacar, a su vez, que con estas palabras el Tribunal aceptó la existencia de un estándar de diligencia debida con el objeto de evitar daños transfronterizos, lo cual fue casi una novedad en Derecho Internacional (Bergwik, 2020, p. 32). De hecho, 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[19].

Esto supone que, aunque ya existían algunos precedentes anteriores de este principio, la primera vez que se estableció tan claramente en el Derecho Internacional contemporáneo se utilizó como base el Derecho nacional de un Estado. Y, a pesar de ello, este principio ha sido aceptado por la *opinio juris* de la comunidad internacional sin mayores inconvenientes. Es una prueba más de que la voluntad de los Estados sigue siendo fundamental a la hora de crear Derecho Internacional en la actualidad y que, en muchas ocasiones, la mejor forma de construir nuevas normas o costumbres internacionales es aprovechando los intereses nacionales y preocupaciones de los Estados.

Finalmente, en 1949 la Corte Internacional de Justicia, en el caso del Canal de Corfú, proporcionó el concepto del principio de diligencia debida que será utilizado en este trabajo. En este caso, se juzgó si Albania era responsable de los daños causados a dos destructores británicos que chocaron con minas en aguas albanesas sin que mediara información alguna por parte del Estado territorial. Estableció la CIJ que es "*every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"*[20] (*Corfú Channel*, 1949, p. 22). Además, en esta misma sentencia la CIJ reconoce que el principio de diligencia debida es uno de los principios generales más reconocidos del Derecho Internacional.

En definitiva, sobre la base de la jurisprudencia estudiada en los párrafos anteriores, puede definirse el principio de diligencia debida como aquella obligación de los Estados de controlar la actividad que sucede en sus territorios con la finalidad de proteger los derechos de los demás Estados que pudieran verse comprometidos por ellas. Además, los

otro o a las propiedades de las personas que allí se encuentren, cuando el caso tenga consecuencias graves y el daño quede probado de forma clara y convincente".

[19] Véase, por ejemplo, la página 17 de la resolución, donde se hace referencia al caso *Story Parchment Company v. Paterson Parchment Paper Company* (1931), del Tribunal Supremo de Estados Unidos.

[20] Traducción propia: "Es la obligación de todo Estado no permitir adrede que su territorio sea usado para actos contrarios a los derechos de otros Estados".

casos citados muestran la gran flexibilidad del principio de diligencia debida, que ha sido aplicado a numerosos ámbitos: actividades de corsarios, medioambiente, negligencia estatal… Es decir, se trata de un principio general del Derecho Internacional cuyo contenido se ha adaptado a las materias específicas en las que ha tenido que ser aplicado (Manual de Tallin, 2017, p. 31). En consecuencia, no solo es el principio de diligencia debida aplicable al ciberespacio como parte del Derecho Internacional, sino que es la figura adecuada para sustituir a la de la responsabilidad internacional y mantener, así, un cierto orden en el ciberespacio.

Además, desde 2010 el principio de diligencia debida abarca el principio de prevención, como bien recogió la CIJ en el caso *Pulp Mills*. Además de reconocer el principio de diligencia debida como reflexivo de la costumbre internacional, determinó que dentro de este mismo principio existe uno de prevención que también es una regla consuetudinaria de Derecho Internacional (Stockburger, 2018, p. 250 & *Pulp Mills*, 2010, párr. 101). A este respecto, prevé la CIJ que "*a State is thus obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State. This Court has established that this obligation "is now part of the corpus of international law relating to the environment.*[21]" (*Pulp Mills*, 2010, párr. 101).

De esta forma la CIJ proporciona una solución a los daños que no se pueden prever y que pueden ser de una entidad considerable, estableciendo la obligación de prevenir actividades que puedan causar un daño significativo al medioambiente. Este mismo principio podría aplicarse en el ámbito del ciberespacio, con el objetivo de evitar que las ciberoperaciones realizadas por actores no estatales puedan causar un daño desproporcionado a los demás Estados. Sin embargo, en el siguiente apartado se analizará con más detalle las razones por las que no es lógico aplicar el principio de prevención en el ciberespacio, en la medida que supondría una carga excesiva a nivel de responsabilidad para los Estados.

Como bien ha quedado en las diferentes citas de la jurisprudencia internacional sobre este tema, las interpretaciones y formas de aplicarlo por los diferentes tribunales

[21] Traducción propia: "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".

internacionales son muy flexibles. No obstante, hay dos elementos principales que todas ellas tienen en común. Por un lado, 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. Por otro lado, 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 (Patrick, 2019, p. 583-584).

Es decir, las obligaciones a las que se encuentra sometido un Estado como consecuencia de la aplicación del principio de diligencia debida están muy condicionadas por el contexto y por la interpretación que de él hagan los organismos internacionales (Patrick, 2019, p. 584). Este aspecto es de una gran relevancia, puesto que puede permitir, a corto plazo, que la aplicación de este principio en el ciberespacio sea más fácilmente aceptada por los Estados. La imposición de obligaciones y sanciones demasiado estrictas supondría un mayor rechazo a la debida diligencia, en la medida que hay Estados más vulnerables que otros a sufrir ciberataques y a no ser capaces de responder de forma efectiva a aquellos realizados o que pasan por sus territorios. Por este motivo es tan importante que este principio sea flexible y se interprete conforme a las capacidades técnicas y materiales de cada Estado (Schmitt, 2015, p. 75). En caso contrario, únicamente se estará perjudicando la construcción de una *opinio juris* respecto de los pormenores de la aplicación del principio de diligencia debida al ciberespacio.

En definitiva, al igual que ha sucedido en los ámbitos más convencionales del Derecho Internacional, para que el principio de diligencia debida pase a ocupar un papel relevante en el ciberespacio es necesario que cuente con un apoyo uniforme en la comunidad internacional por parte de la costumbre de los Estados y su *opinio juris*. Empero, ya existen precedentes en relación con la aceptación del principio de diligencia debida respecto de los hechos internacionalmente ilícitos cometidos por actores no estatales. En los últimos años, se ha podido percibir como la comunidad internacional a buscado modificar el espectro de los actores no estatales y la responsabilidad de los Estados debido al terrorismo. Por otro lado, los Estados han apoyado este estándar de atribución a través de la diligencia debida como medio para abordar las amenazas características del ciberespacio (Chircop, 2018, p. 662). En el próximo apartado, se analizará la aplicación del principio de diligencia debida al ciberespacio y las posibles

respuestas que aporta a los hechos cometidos por actores no estatales con la complacencia de los Estados en cuyos territorios se encuentran.

3.2. El Manual de Tallin 2.0 y la aplicación de diligencia debida al ciberespacio.

El Manual de Tallin 2.0 recoge, en su regla 6, el principio de diligencia debida como principio general aplicable al ciberespacio. Como se podrá observar a continuación, el GIE utiliza las diferentes definiciones y delimitaciones del concepto proporcionadas por la jurisprudencia y analizadas en los párrafos anteriores para determinar la aplicación del principio a los ciberataques:

> ***Rule 6- Due diligence (general principle)***
>
> *A State must exercise due diligence in not allowing its territory or territory or cyber infrastructure under its governmental control to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States*[22] (Schmitt, 2017, p. 30).

En la redacción de este principio, el GIE se ha fundamentado en el largo recorrido de este principio en el Derecho Internacional, en la medida que han recogido numerosos elementos señalados por los Tribunales internacionales en sus resoluciones. Por ejemplo, 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. Por otro lado, señala el Manual, a su vez, que el daño al otro Estado tiene que ser severo. Señala el propio Manual que el GIE aprovecha el hecho de que este principio haya sido utilizado en tantas materias específicas por la jurisprudencia para aplicarlo al ámbito del ciberespacio hasta que se cree una normativa específica que resuelva los vacíos legales y problemáticas de este ámbito (Schmitt, 2017, p. 31).

[22] Traducción propia:

> **"Regla 6 – Diligencia debida (principio general)**
>
> 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".

Es más, indica la propia regla entre paréntesis que se trata de un principio general. En este sentido, se señala, tanto por el Manual como por la propia doctrina, que el principio de diligencia debida aplicable a las ciberoperaciones debe ser considerado como *lex lata*, es decir, derecho vigente (Schmitt, 2017, p. 31; Patrick, 2019, p. 592 & Cocchini, 2021, p. 84). En consecuencia, al tratarse de un principio general del Derecho Internacional, también será aplicable al ciberespacio hasta que exista una excepción legal que excluya tal aplicación. No obstante, el Grupo de Expertos Gubernamentales (GEG) recomendaba en sus informes a los Estados aplicar el principio de debida diligencia, sin establecer la obligación legal de respetar tal principio de Derecho Internacional (GEG, 2013, párr. 23 & GEG, 2015, párr. 13c y 28e). Estos informes abren la puerta a un debate doctrinal sobre la obligatoriedad del principio de diligencia debida al ciberespacio, en la medida que puede considerarse que reflejan esa postura equidistante de los Estados en esta materia con el objeto de no desaprovechar las oportunidades estratégicas que ofrece el ciberespacio (Franzese, 2009, p. 38). Sin embargo, en esos mismos informes el GEG establecía que los principios de derecho internacional derivados del principio de soberanía son legalmente vinculantes para los Estados en el ciberespacio (GEG, 2013, párr. 20 & GEG, 2015, párr. 27).

La existencia de dudas sobre si el principio de diligencia debida es legalmente vinculante en el ámbito del ciberespacio o no es muy relevante a los efectos del presente Trabajo de Fin de Grado, en la medida que el GIE autores del Manual de Tallin han determinado, sobre la base de la jurisprudencia internacional existente, la aplicabilidad del principio de diligencia debida a los hechos realizados por actores no estatales. En este sentido, el Manual recoge que esta regla n.º 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 (Schmitt, 2017, p. 32).

Es más, no solo sería aplicable el principio de diligencia debida a las ciberoperaciones cometidas por actores no estatales desde el territorio de un Estado que causen un perjuicio importante a otro Estado, sino que se plantea la posibilidad de que los Estados de tránsito también tengan la obligación de aplicarlo. Se conoce como un Estado de tránsito 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. Por ejemplo, un grupo terrorista lanza desde el Estado A (atacante) un ciberataque al Estado B (víctima), para lo cual utiliza un virus que ha infectado x equipos en un Estado C (tránsito).

En un principio, sí que podría afirmarse la aplicabilidad del principio de diligencia debida a los terceros Estados que actúen como Estados de tránsito de las ciberoperaciones, en la medida que, en virtud del principio de soberanía, los Estados ostentan el control sobre la ciberinfraestructura y las actividades localizadas en su territorio. En consecuencia, parece pertinente determinar la obligación de los Estados de adoptar todas las medidas que sean necesarias para poner fin a una situación en la que un actor no estatal utiliza su territorio y su ciberinfraestructura para realizar ciberoperaciones que puedan generar un daño grave a otro Estado (Schmitt, 2015, p. 72), aunque no se encuentre físicamente presente en el territorio del Estado de tránsito. Aunque hay que admitir que, desde el punto de vista de este trabajo, aplicar del principio de diligencia debida también a los Estados en tránsito solucionaría muchos de los vacíos legales existentes actualmente en el Derecho Internacional en relación con el ciberespacio, hay que analizar con precaución las consecuencias de ello.

En este sentido, existe un problema similar al del principio de prevención en relación con el de diligencia debida explicado en el apartado anterior, y es el de las capacidades de los Estados. No parece coherente exigir la aplicación de este principio a los países sin las capacidades técnicas y materiales suficientes para evitar la realización de dichas actividades, puesto que generaría un rechazo importante al principio de diligencia debida y dificultaría su cristalización en la *opinio juris* de los Estados (Schmitt, 2015, p. 75). En cualquier caso, es muy complicado que un Estado de tránsito sea declarado responsable de quebrantar su obligación de diligencia debida por un ciberataque para el que se ha usado su ciberinfraestructura, en la medida que es muy difícil probar que este Estado tenía conocimiento de que dichas acciones se estaban produciendo (Bergwik, 2020, p. 46 & Schmitt, 2017, p. 34). Además, podría argumentarse no existe una obligación real sobre la obligación de estos Estados de actuar en caso de que un ciberataque sea lanzado desde estos territorios en virtud del principio de diligencia debida (Bannelier-Christakis, 2014, p. 6).

Empero a todo lo expuesto, sí se considera en este trabajo que el Estado de tránsito en cuestión tiene la obligación de poner todos los medios necesarios para detener la ciberoperación que se esté realizando desde su territorio. Naturalmente, esta obligación

solo existiría si concurrieran dos circunstancias cumulativas: en primer lugar, si tuviera conocimiento de que dicho ciberataque se está produciendo y, en segundo lugar, que tengan las capacidades técnicas, materiales y humanas para detenerlo. En definitiva, la problemática se encontraría en el mismo aspecto que la responsabilidad internacional: la atribución.

Resulta pertinente, llegados a este punto, retornar al caso de la CIJ sobre el *Corfú Channel*, de 1949. Determinó la Corte sobre el tema que atañe a este trabajo que no es razonable que un Estado sea declarado responsable por una situación de la cual no era consciente (*Corfú Channel*, 1949, p. 18). En consecuencia, si cualquier Estado no tuviera conocimiento de que se está produciendo un ataque desde sus territorios por parte de actores no estatales, no incurriría en una violación del principio de diligencia debida.

Sin embargo, el Manual de Tallin 2.0 complementa esta regla jurisprudencial con el término denominado *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 (Schmitt, 2017, p. 43). Este elemento también es acogido por la jurisprudencia de la CIJ en el propio caso del *Corfú Channel*, en el que estableció claramente que Albania "*ought to or should have known"* (*Corfú Channel*, 1949, p. 18). Por tanto, podría concluirse que el Estado deberá poner todos los medios de los que disponga para tener conocimiento de cualquier actividad de naturaleza ilícita que pueda producirse dentro de su territorio o jurisdicción, en la medida que sus capacidades se lo permitan (Bergwik, 2020, p. 46).

Como se puede observar, el cumplimiento del principio de diligencia debida en los Estados es muy complejo y depende de varios factores, como el conocimiento efectivo o constructivo o las capacidades del Estado para actuar frente a una determinada ciberoperación que se está realizando desde o a través de su territorio. En este sentido, el Manual de Tallin delimita cuándo se está cumpliendo con esta obligación en su regla 7:

Rule 7 – Compliance with the due diligence principle

The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right

of, and produce serious adverse consequences for, other States[23] (Schmitt, 2017, p. 43).

En definitiva, se entenderá que un Estado ha incumplido el principio general de diligencia debida cuando 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. Por tanto, el principio de diligencia debida se quebranta por omisión, no por acción. Es la inacción ante una determinada amenaza de la que se tiene conocimiento la que supone la violación de este principio y la aparición de responsabilidad por parte del Estado (Schmitt, 2017, p. 43). Complementa a la responsabilidad internacional del Estado, figura jurídica fundamentada principalmente en la acción estatal y en el control efectivo de los actores no estatales u otros sujetos privados, como se ha estudiado en el apartado 1.2 del presente trabajo.

Por último, es necesario abordar una cuestión muy relevante en relación con el principio de diligencia debida y el principio de precaución. Si bien podría parecer razonable, como ya se ha explicado en el apartado anterior, la imposición de la obligación a los Estados de prevenir las ciberoperaciones realizadas en sus territorios, el Manual de Tallin rechaza tal posibilidad. Establece, en este sentido, que "*given the difficulty of mounting comprehensive and effective defences against all possible cyber threats, it would be unreasonable to assert that an obligation of prevention exists in the cyber context* [24]*"* (Schmitt, 2017, p. 45). La falta de razonabilidad respecto de esta obligación es clave a la hora de determinar su no concurrencia en el ámbito del ciberespacio. Además, no es solo una discusión doctrinal, sino que existe jurisprudencia internacional de diferentes órganos que argumentan sobre la base de esa "razonabilidad" de la obligación de prevención.

En el ámbito del Derecho Internacional, la resolución más relevante aparece en el caso *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro*, de la Corte Internacional de Justicia, donde se estableció que "*a State does not incur responsibility simply because*

[23] Traducción propia:

"Regla 7 – El cumplimiento del principio de diligencia debida

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".

[24] Traducción propia: "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".

the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide[25]" (*Genocide*, 2007, párr. 430). Como se puede observar, la CIJ ha establecido un criterio flexible, a través del cual busca no imponer una obligación excesiva a los Estados en materias que, en muchas ocasiones, escapan de sus capacidades.

En la misma línea se ha pronunciado la jurisprudencia del Tribunal Europeo de Derechos Humanos en varias sentencias[26]. La más interesante para este trabajo es la sentencia del caso *Kiliç v. Turkey*, en la cual se determinó que Turquía era responsable por no proteger el derecho a la vida de un periodista que fue finalmente asesinado después de numerosas amenazas de muerte. En este sentido, el TEDH estableció que las autoridades fallaron al actuar, a pesar de que existían una gran cantidad de medidas preventivas disponibles que hubieran permitido minimizar el riesgo de que dicho asesinato se hubiera producido y no hubiera supuesto una inversión de recursos que no fuera razonable (*Kiliç v. Turkey*, párr. 76).

Estas mismas reglas son aplicables al ámbito del ciberespacio, en la medida que no resulta razonable exigir a los Estados el desarrollo y preparación de personal e infraestructuras destinadas única y exclusivamente a prevenir ciberoperaciones. Además, existe otra cuestión de fondo puramente jurídico, puesto que, en virtud del criterio del GIE, el conocimiento efectivo o constructivo es requisito indispensable para que se produjera la violación de la diligencia debida (Cocchini, 2021, p. 86). En este sentido, sería contradictorio expandir este requisito a las operaciones cibernéticas en las que aún no se pueda determinar su realización, puesto que un Estado no puede conocer los ciberataques que aún no han sido planificados. Recoge el manual que "*extending this Rule to a general duty of prevention would accordingly render the knowledge requirement – which all the Experts agreed was necessary for the breach of the obligation - moot*[27]*".*

[25] Traducción propia: "Un Estado no incurre en responsabilidad simplemente porque el resultado deseado no se ha conseguido; la responsabilidad sí aparece cuando el Estado haya fallado manifiestamente al adoptar toda medida necesaria dentro de su capacidad para prevenir el genocidio, y que efectivamente podría haber contribuido a prevenirlo".
[26] Véase *Lopez Ostra v. Spain* y *Ärtze fur das Leben v. Austria*.
[27] Traducción propia: "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".

En definitiva, si se tienen en consideración las reglas y comentarios provistos en el Manual de Tallin y en la jurisprudencia y doctrina existentes hasta la fecha, podemos concluir que el principio de diligencia debida es aplicable al ciberespacio. Sin embargo, 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. Gracias a los límites marcados por la jurisprudencia y la doctrina que han sido descritos a los párrafos anteriores, el principio de diligencia debida puede convertirse en un principio general asumible por los Estados que pase a formar parte de su *opinio juris*. No impone obligaciones que no sean razonables para los Estados, conforme a sus capacidades, lo cual permitirá su consolidación en el seno del Derecho Internacional aplicable al ciberespacio para abordar el problema de los ataques lanzados por actores no estatales desde los territorios de Estados soberanos.

Además, este principio cuenta con una ventaja importante respecto de figura responsabilidad internacional de los Estados, y es que no se trata de una figura novedosa, sino que tiene un largo recorrido jurisprudencial y aceptación previa por parte de los Estados en el Derecho Internacional. En consecuencia, se encuentra bien definido y delimitado a nivel conceptual y jurídico por parte de numerosas sentencias de tribunales internacionales, por lo que se elimina el factor de la incertidumbre como posible obstáculo para su aceptación por parte de los Estados. Todas estas circunstancias facilitan la aplicación del principio de diligencia debida en el ciberespacio como el instrumento más adecuado que existe actualmente en el Derecho Internacional para cubrir el vacío legal dejado por la responsabilidad internacional y permitir así la convivencia en la comunidad internacional en el ciberespacio.

No obstante, a pesar de que mantener un principio de diligencia debida es necesario en la actualidad y en un futuro próximo hasta que se haya estabilizado la situación normativa y tecnológica y los Estados empiecen a participar de forma activa en el proceso de positivización del ciberespacio, no hay que detenerse a la hora de aportar nuevos instrumentos y doctrina que permitan perfilar estos aspectos del Derecho Internacional. El principio es muy general y su aplicación se encuentra muy limitada, en la medida que las dificultades de atribución técnicas aplicables a la atribución de la responsabilidad internacional también son aplicables a la diligencia debida. Por ello, es necesario continuar trabajando, delimitando y criticando los conceptos y límites existentes, de

forma que realmente se produzca un impacto real en la sociedad internacional que permita la prevención efectiva de ciberoperaciones que pongan en riesgo, ya no solo la soberanía y derechos de los Estados, sino también los sistemas democráticos y la infraestructura de la que dependen las vidas de tantas personas.

4. CONCLUSIONES

La aplicación del Derecho Internacional Público en el ciberespacio es una cuestión de la más inmediata actualidad y relevancia. La falta de un marco jurídico determinado que esté claramente aceptado por los Estados provoca la existencia de vacíos legales y situaciones de desamparo que son aprovechadas con fines ilícitos por otros Estados y actores no estatales. Además, se trata de un ámbito normativo en el que la participación de los Estados es muy limitada, en la medida que ninguno de ellos quiere dejar de aprovechar el potencial estratégico del ciberespacio.

En consecuencia, 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. Con las conclusiones que se enumerarán a continuación, el presente Trabajo de Fin de Grado pretende aportar nuevas conclusiones, críticas y premisas a una de las cuestiones más delicadas de este ámbito: las ciberoperaciones realizadas por actores no estatales desde territorios de Estados y la responsabilidad de estos últimos en los daños que puedan producir a otros Estados. Por todo lo expuesto, las conclusiones de este trabajo, sobre la base de toda la jurisprudencia, doctrina y demás literatura analizada en los apartados anteriores, son las siguientes:

PRIMERA: El ciberespacio, al igual que el espacio o el Ártico, podrá considerarse como un elemento de *global commons* una vez haya un marco normativo determinado que lo regule. No existe una territorialización completa del ciberespacio, pero tampoco existe una descentralización absoluta. 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. Esta naturaleza jurídica especial, así como las particularidades y desafíos propios del ciberespacio, son los causantes de que resulte recomendable la creación de un marco jurídico propio de este ámbito que aborde la problemática que genera la existencia del mismo.

SEGUNDA: El esfuerzo normativo de los Estados respecto del ciberespacio se ha centrado únicamente en aspectos de preocupación general, como la ciberdelincuencia o la piratería, que no afectan a los intereses nacionales de los diferentes países. En este

sentido, no se puede esperar en un futuro inmediato que se lleguen a acuerdos internacionales sobre este ámbito en la comunidad internacional, en la medida que los intereses y valores de los Estados suponen un punto clave de desencuentro a la hora de llegar a un acuerdo. Podría incluso afirmarse que la elaboración de un marco jurídico internacional que regule el ciberespacio será una pugna de poder e influencia de valores e ideologías, que enfrentará a democracia y autoritarismo a la hora de determinar las reglas por las que se regirá el Internet. Por otro lado, tampoco puede esperarse una mayor colaboración y transparencia de los Estados en esta materia hasta que no se hayan aprovechado o agotado todas las oportunidades estratégicas que ofrece el ciberespacio.

TERCERA: Los principios generales del Derecho Internacional son plenamente aplicables al ámbito del ciberespacio. En última instancia, la Red es una dimensión más en el que los Estados desarrollan sus Relaciones Internacionales. No obstante, será necesario analizar y adaptar la aplicación de cada uno de estos principios al ciberespacio en función a la jurisprudencia y doctrina existentes, como se ha realizado en este trabajo con el principio de soberanía. Además, es la propia vigencia del principio de soberanía en el ciberespacio lo que permite justificar el límite que establece que los Estados no pueden desarrollar actividades cibernéticas que afecten a los derechos o territorios de otros Estados, causando un daño grave.

CUARTA: A corto plazo, se puede esperar que los Estados participen más activamente en la interpretación de las normas de Derecho Internacional vigentes en el ciberespacio. Todo esto permitirá, en el largo plazo, la aparición de la *opinio juris* respecto de los principios fundamentales aplicables al ciberespacio. De esta forma, se creará un marco jurídico claro que aborde las relaciones internacionales de los Estados en el ciberespacio teniendo en cuenta sus particularidades y riesgos.

QUINTA: La figura de la responsabilidad internacional de los Estados es uno de los grandes logros del Derecho Internacional, en la medida que hay un texto legal aprobado por la Asamblea General de Naciones Unidas a través de la Resolución 56/83 que regula su régimen jurídico. Aunque es plenamente aplicable al ciberespacio, como el resto de las figuras jurídicas del Derecho Internacional, 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. La doctrina del control efectivo de estos actores por parte de los Estados causa que muchas conductas igualmente graves, como la financiación o la

asistencia, no sean generadoras de responsabilidad internacional de los Estados. En este sentido, se considera más adecuada la doctrina 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 etc. que desechó en posteriormente la CIJ. En consecuencia, es 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.

SEXTA: El principio de diligencia debida tiene una larga trayectoria jurisprudencial, y su régimen jurídico y conceptual ha sido claramente definido y delimitado por diferentes tribunales de arbitraje y por la CIJ. En este sentido, aunque la responsabilidad internacional de los Estados sea una figura más contundente como medio para prevenir y castigar los hechos internacionalmente ilícitos cometidos por un Estado o en/desde su territorio, no resulta aplicable a los ciberataques realizados por actores no estatales sobre los que el Estado no tiene un control efectivo. En contraste, el principio de diligencia debida tiene una larga trayectoria en el Derecho Internacional y su construcción jurisprudencial da cabida a la responsabilidad de los Estados por los actos cometidos por actores no estatales desde sus territorios. Este elemento favorecerá, en el medio plazo, la consolidación de una *opinio juris* de la comunidad internacional respecto a la aplicación de la diligencia debida en el ciberespacio.

SÉPTIMA: El principio de diligencia debida supone la obligación de los Estados de no permitir que su territorio y/o la ciberinfraestructura que en él se encuentra y esté bajo control gubernamental sean utilizados para la realización de ciberoperaciones que afecten los derechos de otros Estados y produzcan consecuencias adversas graves a estos. En consecuencia, el Estado deberá adoptar las medidas que fueran necesarias para evitar que se produzca dicho daño. El contenido de este principio es similar al de la responsabilidad internacional, aunque sus consecuencias no son tan contundentes. No obstante, el principio de diligencia debida, en su aplicación al ciberespacio, tendrá varios límites: en primer lugar, la obligación únicamente se impondrá al Estado cuando este tuviera o debiera tener conocimiento del desarrollo de dicha actividad por parte de un actor no estatal. En segundo lugar, dicha actividad ilícita deberá ser susceptible de generar un daño grave a los derechos o ciberinfraestructura de otro Estado. En tercer lugar, no existe obligación de prevención en el marco de la diligencia debida, en la medida que no se considera razonable que un Estado deba destinar tal cantidad de recursos a prevenir

ciberataques hipotéticos, conforme a los criterios de razonabilidad marcados por la jurisprudencia. En cuarto y último lugar, la flexibilidad del principio de diligencia debida permite que pueda juzgarse el caso concreto, adaptándose a sus circunstancias y a las capacidades técnicas y materiales de cada Estado, lo que será favorable en el largo plazo para la consolidación de una *opinio juris* respecto a la aplicación de esta figura en el ciberespacio.

OCTAVA: En definitiva, el principio general de diligencia debida es la figura perfecta ante la imposibilidad de utilizar la figura de la responsabilidad internacional para sancionar los comportamientos ilícitos de aquellos Estados que colaboran con actores no estatales para realizar ciberataques contra otros países sin ostentar el control efectivo. Su gran flexibilidad y recorrido en el Derecho Internacional permitirá una aceptación mayor por parte de los Estados para su aplicación en el ciberespacio, en la medida que no restringen en gran medida su capacidad de actuación y tampoco les obliga a pronunciarse sobre su postura respecto al ciberespacio, de forma que pueden seguir explotando las oportunidades estratégicas que ofrece. En cualquier caso, es necesario seguir trabajando desde el punto de vista doctrinal y académico por la clarificación y constitución de un ordenamiento jurídico claro para el ciberespacio, puesto que será uno de los campos clave a todos los niveles en este siglo XXI. El Manual de Tallin 2.0 es el ejemplo perfecto de la regulación internacional a la que debe aspirar el ciberespacio, pero para ello es necesario que los Estados participen más activamente de este proceso.

BIBLIOGRAFÍA

1. Normativa y documentos oficiales.

Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, International Law Commission, 2001, Yearbook of the ILC vol. II/2 2001. Consultado el 07/03/2021 en: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

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, 2013. UN Doc. A/68/98. Consultado el 5 de abril de 2021 en: https://undocs.org/es/A/68/98

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. UN Doc. A/70/174. Consultado el 5 de abril de 2021 en: https://undocs.org/es/A/70/174

Resolución 2.625 (XXV): Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas, 1970, Asamblea General de Naciones Unidas. Consultado el 3 de abril de 2021 en: https://www.dipublico.org/doc/A-RES-2625(XXV).pdf

Responsabilidad del Estado por hechos internacionalmente ilícitos, 2001, Asamblea General de Naciones Unidas. Consultado el 07/03/2021 en https://undocs.org/pdf?symbol=es/A/RES/56/83

2. Jurisprudencia.

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. Consultado el 25 de marzo de 2021 en: https://www.dipublico.org/cij/doc/79.pdf

Cour Européenne des Droits de L´Homme, Deuxième Section. Affaire Halime Kiliç c. Turquie. 28 juin 2016. Consultado el 21 de abril de 2021 en: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-164689%22]}

International Court of Justice. Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). Judgment of 26 February 2007. Consultado el 12 de abril de 2021 en: https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

International Court of Justice. The Corfu Channel Case. Judgment of April 9th, 1949. Consultado el 11 de abril de 2021 en: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

International Criminal Tribunal for the Former Yugoslavia. Prosecutor v. Dusko Tadic. Judgement of 15th july, 1999. Consultado el 27 de marzo de 2021 en: https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf/

Permanent Court of Arbitration. Island of Palmas case (Netherlands, USA). Award of April, 1928. Consultado el 2 de abril de 2021 en: https://legal.un.org/riaa/cases/vol_II/829-871.pdf

Permanent Court of International Justice. Case Concerning the Factory At Chorzów. Judgment No. 8, July 26th, 1927. Consultado el 10 de marzo de 2021 en: https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_09/28_Usine_de_Chorzow_Competence_Arret.pdf

Permanent Court of International Justice: The Case of the S.S. “Lotus”. Judgement No. 9, September 7th, 1927. Consultado en marzo de 2021 en: https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf

Reports of International Arbitral Awards: Alabama claims of the United States of America against Great Britain. Award rendered on 14 September 1872. Consultado el 10 de abril de 2021 en: https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf

Reports of International Arbitral Awards: Trail smelter case (United States, Canada). Award rendered on 16 april 1938 and 11 March 1941. Consultado el 10 de abril de 2021 en:https://www.informea.org/sites/default/files/court-decisions/Trail%20Smelter%20Case.pdf

3. Obras doctrinales.

Bannelier-Christakis, K. (2014). Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations? *Baltic Yearbook of International Law*, 14. Consultado el 10 de abril de 2021 en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2550913

Bergwik, M. (2020). *Due Diligence in Cyberspace. An Assessment of Rule 6 in the Tallinn Manual 2.0* (Master's Thesis). Department of Law, Uppsala University, Uppsala, Suecia.

Chircop, L. (2018). A Due Diligence Standard of Attribution in Cyberspace. *International & Comparative Law Quarterly*, 67(3), 643-668. https://doi.org/10.1017/S0020589318000015

Cocchini, A. (2021). 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, 69–98.

Dimitrovska, M. (2020). The Concept of International Responsibility of State in the International Public Law System. *Journal of Liberty and International Affairs*, 1(2).

Egan, B. J. (2017). International Law and Stability in Cyberspace. *Berkeley Journal of International Law*, 35(1), 169-180.

Eichensehr, K. (2020). The Lawy and Politics of Cyberattack Attribution. *U.C.L.A. Law Review*, 67, 520-598.

Franzese, P. (2009). Sovereignty in Cyberspace: Can it Exist? *Air Force Law Review*, 64. Consultado el 5 de abril de 2021 en: https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

Healey, J. (2012). Beyond Attribution: Seeking National Responsibility for Cyber Attacks. *Atlantic Council*. Consultado el 28 de marzo de 2021 en: https://www.files.ethz.ch/isn/142271/022212_ACUS_NatlResponsibilityCyber.pdf

Heffes, E. & Frenkel, B. (2018). The International Responsibility of Non-State Armed Groups: In Search of the Applicable Rules. *Goettingen Journal of International Law* 8(1), 39-72. https://doi.org/10.3249/1868-1581-8-1-heffesfrenkel

Mačák, K. (2016). Is the International Law of Cyber Security in Crisis? *2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia*, pp. 127-139, doi: 10.1109/CYCON.2016.7529431

Maftei, J. (2015). Reflections on the International Responsibility of States for Wrongful Acts. *Acta Universitatis-Danibius: Relationes Internationales* 8(1), 37-55.

Pastor, J. (2017). *Curso de Derecho Internacional Público y Organizaciones Internacionales.* Madrid: Tecnos.

Patrick, C. (2019). Debugging the Tallin Manual 2.0's Application of the Due Diligence Principle to Cyber Operations. *Washington International Law Journal,* 28(2), 581-604.

Payne, C. & Lorraine, F. (2017). Addressing Obstacle to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *The George Washington International Lawy Review*, 49. Consultado el 1 de abril de 2021 en: https://www.eu-space.eu/images/2018/document/Articles/Addresing-obstacles-to-cyber-attribution-a-model-based-on-state-response-to-cyber-attack.pdf

Segura, A. (2017). Ciberseguridad y Derecho Internacional. *Revista Española de Derecho Internacional*, 69(2), 291-299. http://dx.doi.org/10.17103/redi.69.2.2017.2.02

Schmitt, M. (2015). In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 125, p. 68-80. Consultado el 10 de abril de 2021 en: http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

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

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review*, 269. Consultado el 15 de marzo de 2021 en: https://law.stanford.edu/publications/law-cyber-warfare-quo-vadis/

Stockburger, P. (2018). From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize The Due Diligence Principle In Cyberspace. *2018 10th International Conference on Cyber Conflict (CyCon)*, 245–262. https://doi.org/10.23919/CYCON.2018.8405020

Sturma, P. (2016) State Succession in Respect of International Responsibility. *George Washington International Law Review* 48 (3), 653-678.

Tran, D. (2018). The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *The Yale Journal of Law & Technology*, 20, 376-441. Consultado el 22 de marzo de 2021 en: https://yjolt.org/sites/default/files/20_yale_j._l._tech._376.pdf

Zhixiong, H. & Mačák, K. (2017). Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. *Chinese Journal of International Law*, 16(2), p. 271-310. https://doi.org/10.1093/chinesejil/jmx011

Zimmermann, A. (2014). International Law and "Cyber Space". *European Society of International Law*, 3(1). Consultado el 1 de abril de 2021 en: https://esil-sedi.eu/post_name-144/

4. Recursos de internet.

E.P. (2020, 28 de agosto). Un ciberataque interrumpe por cuarto día consecutivo la bolsa de N. Zelanda. *El Confidencial*. Obtenido el 15 de abril de 2021 de https://www.elconfidencial.com/mercados/2020-08-28/un-ciberataque-interrumpe-por-cuarto-dia-consecutivo-la-bolsa-de-n-zelanda_2727867/

McGuiness, D. (2017, 6 de mayo). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó un país. *BBC*. Obtenido el 15 de abril de 2021 de: https://www.bbc.com/mundo/noticias-39800133