Universidad de Costa Rica

Facultad de Derecho

Tesis para optar por el grado de licenciatura en Derecho

"Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz"

Elízabeth Jiménez Mora (B13487)

Mariel Merayo Ramírez (B14146)

San José, Ciudad Universitaria "Rodrigo Facio"

Marzo, 2017

13 de marzo de 2017
FD-333-2017

Dr. Alfredo Chirino Sánchez
Decano
Facultad de Derecho

Estimado señor:

Para los efectos reglamentarios correspondientes, le informo que el Trabajo Final de Graduación (categoría Tesis), de las estudiantes: Elizabeth Jiménez Mora, carné B13487 y Mariel Merayo Ramírez, B14146 denominado: "Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz" fue aprobado por el Comité Asesor, para que sea sometido a su defensa final. Asimismo, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo apruebo en el mismo sentido.

Igualmente, le presento a los (as) miembros (as) del Tribunal Examinador de la presente Tesis, quienes firmaron acuso de la tesis (firma y fecha) de conformidad con el Art. 36 de RTFG que indica: ***"EL O LA ESTUDIANTE DEBERA ENTREGAR A CADA UNO DE LOS (AS) MIEMBROS (AS) DEL TRIBUNAL UN BORRADOR FINAL DE SU TESIS, CON NO MENOS DE 8 DIAS HABILES DE ANTICIPACION A LA FECHA DE PRESENTACION PUBLICA".***

Tribunal Examinador

Informante	*Dr. José Thompson Jiménez*
Presidente	*Dr. Alfredo Chirino Sánchez*
Secretario	*Dr. Gilbert Armijo Sancho*
Miembro	*Dra. Elizabeth Odio Benito*
Miembro	*Dr. Jorge Errandonea*

Por último, le informo que la defensa de la tesis es el ***30 de marzo del 2017,*** *a las 7:00 p.m. en el primer piso de la Facultad.*

Atentamente,

Ricardo Salas Porras
Director

FACULTAD DE DERECHO
ÁREA DE INVESTIGACIÓN

RSP/lcv
Cc: arch. expediente

San José, 10 de marzo de 2017.

Señor
Dr. Ricardo Salas Porras
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Presente

Estimado señor Director:

Al saludarlo, tengo el gusto de informarle, en mi condición de **DIRECTOR** de la tesis de grado denominada "*Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz*", confeccionada por los estudiantes **Elízabeth Jiménez Mora** (carné B13487) y **Mariel Merayo Ramírez** (carné B14146), que he aprobado el trabajo, en virtud de que cumple con los requisitos de forma y de fondo que exige la Universidad de Costa Rica para una investigación de esta naturaleza.

El mencionado proyecto de investigación, deviene trascendental en su formulación, por tratar adecuadamente una temática de indudable actualidad, con probables proyecciones aun mayores en el futuro cercano.

Con la presente carta de aprobación, puede procederse con los trámites pertinentes.

Con mis mejores saludos,

JOSÉ THOMPSON JIMÉNEZ
DIRECTOR

CARTA DE APROBACIÓN DE TESIS – LECTORA

Señor
Dr. Ricardo Salas Porras
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Presente

Estimado señor:

Quien suscribe, **ELIZABETH ODIO BENITO**, actuando en mi condición de **LECTORA** de la tesis de grado denominada "*Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz*", confeccionada por los estudiantes **Elízabeth Jiménez Mora** (carné B13487) y **Mariel Merayo Ramírez** (carné B14146), le comunico que he aprobado el trabajo de forma satisfactoria, en virtud de que cumple con los requisitos de forma y de fondo que exige la Universidad de Costa Rica.

De esta manera, me complace extender la presente carta de aprobación, a fin de que se proceda con la defensa de la tesis en la fecha y hora que se sirva fijar.

San José, 10 de marzo de 2017.

Atentamente,

Dra. ELIZABETH ODIO BENITO
LECTORA

CARTA DE APROBACIÓN DE TESIS – LECTOR

Señor
Dr. Ricardo Salas Porras
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Presente

Estimado señor:

Quien suscribe, **JORGE ERRANDONEA**, actuando en mi condición de **LECTOR** de la tesis de grado denominada "*Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz*", confeccionada por los estudiantes **Elízabeth Jiménez Mora** (carné B13487) y **Mariel Merayo Ramírez** (carné B14146), le comunico que he aprobado el trabajo de forma satisfactoria, en virtud de que cumple con los requisitos de forma y de fondo que exige la Universidad de Costa Rica.

De esta manera, me complace extender la presente carta de aprobación, a fin de que se proceda con la defensa de la tesis en la fecha y hora que se sirva fijar.

San José, 07 de marzo de 2017.

Atentamente,

Dr. JORGE ERRANDONEA
LECTOR

San José, 28 de febrero de 2016

Doctor
Ricardo Salas Porras,
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica.

Quien suscribe, en mi condición de filóloga, he leído y corregido el trabajo final de graduación denominado: "**Los ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz**", elaborado por las estudiantes Elizabeth Jiménez Mora y Mariel Merayo Ramírez, con el fin de optar por el grado académico de licenciatura en Derecho de la Universidad de Costa Rica.

Hago constar que he revisado el trabajo de investigación mencionado en todos los aspectos de redacción (cacofonía, repeticiones, queísmos, dequeísmos, anfibología), así como la ortografía y ofrecerle cadencia al texto y fluidez léxica.

Atentamente,

Grettel Hernández Valdés
Carné 166

GRETTEL HERNÁNDEZ VALDÉS
Filóloga
Carné N° 166
Asociación Costarricense de Filólogos
UNIVERSIDAD DE COSTA RICA

Dedicatoria

Todo lo que tengo y todo lo que soy hasta hoy, no puedo dedicárselo a nadie más que a mi madre, que ha sido mi inspiración y soporte por tantos años. Una mujer absolutamente admirable por su valentía, tenacidad y buena actitud ante la vida, la cual merece todo mi amor y mi respeto. A Leslie Guiselle Mora Cordero, es quien dedico este paso tan importante de mi vida.

Elízabeth Jiménez Mora

Dedicatoria

A mi mamá, a quién le debo todo lo que soy.

Mariel Merayo Ramírez

Agradecimientos

Tengo muchas personas a quienes darles las gracias, pues este camino no habría sido lo mismo sin aquellos que han estado a mi lado. Agradezco a mi papá, a mis hermanos, Stward y Kenneth, a mi abuelita Luz Marina, así como al resto de personas que forman mi familia cercana, ya sea por sangre o por elección, pues son pilares importantes en mi vida, y han sido quienes, siempre con su apoyo incondicional me han impulsado hacia delante y han compartido conmigo los momentos más importantes que han marcado mi camino. Así como a esas personas especiales que recientemente llegaron a mi vida y a mis amigos que han representado un soporte esencial para no caer, aún cuando estaba cansada.

A mi compañera Mariel que sin ella este proceso habría sido insufrible. Con su humor y la alta calidad de su trabajo hizo que mi proceso de tesis fuera mil veces mejor y lleno de historias. Debo agradecerle por apoyar las locuras y por hacer un trabajo en el que podía confiar ciegamente, que nos permitió cumplir con los descabellados límites de fecha que tuvimos.

Quiero agradecerle a don José Thompson, a Jorge Errandonea, a doña Elizabeth Odio, a don Alfredo Chirino y a don Gilbert Armijo por su apoyo y por su guía en este proceso.

Además, quiero aprovechar el espacio para agradecerle a personas que han sido pilares en mi vida académica. Doña Elizabeth Odio, es quien ha sido mi inspiración, y quien con mucha paciencia y cariño se ha tomado el tiempo de ayudarme y escucharme, de impulsarme en los procesos que he tenido que pasar. También tengo a mi “gurú académico” que es Edward Pérez, quien ha tenido una paciencia impresionante y me ha guiado en muchos momentos críticos de mi vida académica, escuchándome y alentándome hasta el final. Él es una de las personas en las que más confío en estos temas, por lo que en todos aquellos momentos donde me he sentido perdida o he ocupado un consejo sincero, en él siempre he encontrado a un profesional que admiro y respeto y en quien realmente confío. Le debo muchísimo y no tengo como devolverle todo lo que me ha ayudado y como me ha inspirado y motivado para creer que ninguna meta es demasiado grande, ayudándome así, a alcanzar cosas y superar límites que parecían lejanos para mí.

Asimismo, tengo personas que definitivamente han marcado mi vida en este aspecto y que no puedo dejar de mencionar, por ejemplo, mis profesores Olivier Remy y Karla Blanco por su apoyo incondicional; a Ana Lucía Ugalde, por haberme enseñado lo que se convertiría en mi pasión, y por haberme abierto puertas esenciales para mí en el campo del Derecho Internacional; Auxiliadora Solano y Agustín Martin, quienes confiaron en mí y han sido mis jefes por ya casi tres años en la Corte Interamericana de Derechos Humanos, y que con cariño me han enseñado muchísimo de lo que sé de Derecho Internacional; Marcela Giraldo, quien es una abogada que mezcla la dulzura y la bondad, con la inteligencia, y me ha apoyado de muchas maneras en el camino; José Jaime Villalobos y Fernanda Jiménez Sauter, por haber sido mis coaches y haber confiado en mí, así como por enseñarme grandes cosas para la vida y el Derecho, pues más que coaches fueron guías e inspiración; don Víctor Rodríguez, por haberme dado una oportunidad que marcó mi vida sin lugar a dudas, como lo fue Naciones Unidas, pues me permitió expandir horizontes, al mostrarme un mundo que solo soñaba y que ahora lucho por volver una realidad; y finalmente pero no menos importantes, a los chicos que conformaron el equipo que compitió conmigo en Holanda en el 2014, así como mis dos equipos Jessup 2016 y 2017, porque han sido parte de experiencias muy importantes para mí y que me dejaron grandes enseñanzas académicas y de vida.

Elízabeth Jiménez Mora

A mi abuela, hermanos y amigos, por su paciencia, apoyo y cariño incondicional.

A mis profesores, *coaches*, y mentores, por su dedicación por la enseñanza y haber inspirado en mí la pasión por el derecho.

A Eli, tan solo estamos comenzando.

Mariel Merayo Ramírez

TABLA DE CONTENIDO

I. Resumen

Justificación

En años recientes, la comunidad internacional ha presenciado el incremento en actividades llevadas a cabo a través del ciberespacio por parte de individuos, empresas, Estados e incluso por grupos no estatales. Ciberataques llevados a cabo en los últimos años en Estonia, Irán, Estados Unidos, entre otros, son claro ejemplo de las consecuencias que puede acarrear un ciberataque debido a la rápida evolución de las tecnologías.

El avance tecnológico supera en tiempo al desarrollo de la creación de las leyes, tanto nacionales como internacionales, que permitan regular la comisión de ilícitos en el ciberespacio. Esto demuestra entonces, la necesidad de encontrar una manera de ofrecer respuesta a esta nueva realidad con los medios que se cuentan y la normativa y los principios ya existentes.

Si bien es cierto, en un panorama ideal, la creación de un marco normativo especializado en la materia sería la herramienta idónea para regular estas actividades, la posibilidad de que esto suceda en la realidad es limitada, y a su vez un único marco normativo no sería capaz de regular actividades que se desarrollan con gran dinamismo. Este trabajo pretende demostrar que actualmente el Derecho Internacional cuenta con las bases necesarias para dar respuesta a los Estados por la comisión de ciberataques que constituyan hechos internacionalmente ilícitos en tiempos de paz.

Hipótesis

El Derecho Internacional cuenta con las bases necesarias, en diferentes áreas, para establecer la responsabilidad internacional de un Estado por un ciberataque cometido fuera del contexto de un conflicto armado.

Objetivo general

Analizar los mecanismos existentes en el Derecho Internacional y su aplicación para el establecimiento de la responsabilidad internacional de un Estado como consecuencia de un ciberataque.

Metodología

El presente trabajo de investigación se basa en una metodología descriptiva analítica, la cual se apoya en los siguientes métodos de trabajo: 1) *Análisis doctrinario*, donde se hará un análisis doctrinario para determinar lo que han aportado los autores más

reconocidos en la materia, 2) *Análisis legal*: en razón la falta de regulación a nivel internacional en cuestiones de ciberataques, el análisis legal será realizado de conformidad con las fuentes del Derecho Internacional, 3) *Análisis deductivo*: se utilizará el análisis deductivo para establecer las posibles aplicaciones de las fuentes existentes del Derecho Internacional Público, en la regulación de la responsabilidad internacional de los Estados en relación con los ciberataques.

Conclusiones

- El Derecho Internacional cuenta con las bases necesarias para establecer la responsabilidad internacional de un Estado por un ciberataque cometido fuera del contexto de un conflicto armado.
- La complejidad de los sistemas y los ciberataques vuelven difícil, si no imposible, la atribución directa a un Estado por la comisión del ilícito en contra de un sujeto de Derecho Internacional, pero por medio del análisis de la jurisprudencia de la Corte Internacional de Justicia, se llega a la conclusión de que es posible que la Corte determine, a través de medios indirectos, la responsabilidad internacional de un Estado por situaciones relacionadas al ciberespacio.
- La CIJ puede llegar a determinar que un Estado es responsable por un hecho internacionalmente ilícito, cometido por una empresa privada, semiprivada o transnacional, o bien, por colaborar en la comisión de un ciberataque realizado por un grupo terrorista o insurgente, siempre que se cumplan con los requisitos analizados en capítulo respectivo de la tesis.
- Un ciberataque que comprometa los elementos cibernéticos que se encuentran en el territorio de un país, o bien que intervenga en los asuntos internos del Estado violentan la soberanía del mismo.
- Los Estados deben tomar todas las medidas que resulten razonables, entre los parámetros de los estándares analizados, para evitar la comisión de un ciberataque que violente las obligaciones del Estado con la comunidad internacional, y evitar que su infraestructura cibernética sea utilizada para la ejecución de ciberataques en perjuicio de otros Estados, con el objetivo de cumplir con su deber de debida diligencia.
- Las reglas de eximentes de responsabilidad y reparaciones, son aplicables al ámbito de los ciberataques.

II. Ficha bibliográfica

Jiménez Mora, Elízabeth y Merayo Ramírez, Mariel. *"Los Ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz"* Tesis de Licenciatura en Derecho, Facultad de Derecho. Universidad de Costa Rica. San José, Costa Rica. 2017. xi y 152.

Director: Dr. José Thompson Jiménez.

Palabras claves: Ciberataques, Ciberespacio, Internet, Derecho Internacional Público, Responsabilidad Internacional, Corte Internacional de Justicia, Soberanía, Debida Diligencia, Grupos Insurgentes, Eximentes de Responsabilidad, Reparaciones, Cesación.

III. Introducción

En la actualidad, ciertos paradigmas con los que se regulan las interacciones entre los Estados, se han modificado significativamente e incluso han surgido nuevos, gracias al eminente avance de las tecnologías y el espacio cibernético. Dichos avances forman parte importante de la sociedad, por lo tanto, los Estados, empresas y los particulares se enfrentan a situaciones en foros diferentes a los concebidos en forma tradicional. A pesar de las ventajas y los beneficios que trae el desarrollo tecnológico, este medio está siendo utilizado para perpetuar actos ilegales a nivel nacional e internacional. Por eso, el Derecho ha tenido que acoplarse a dichos cambios para proveer una solución o respuesta a estas situaciones en el ciberespacio a nivel interno, pero lamentablemente en el Derecho Internacional no encontramos una respuesta clara sobre el tópico, ya que no se cuenta con una legislación especializada sobre el tema.

Cuando se piensa en un ciberataque, podría contextualizarse el mismo dentro de un conflicto armado, en donde se utilizan medios tecnológicos para llevar a cabo ataques con un fin militar. Para esto, el Derecho Internacional tiene herramientas que regulan las actuaciones de un Estado en el conflicto y establecen las reglas que las partes deben respetar. Entre estas se tienen los cuatro Convenios de Ginebra y sus dos Protocolos adicionales, que juntos conforman la normativa aplicable en conflictos armados, según el Derecho Internacional Humanitario. Sin embargo, los ciberataques no se limitan a contextos bélicos, sino que se encuentran presentes en distintos escenarios.

A pesar de no existir una definición uniformemente aceptada entre Estados o expertos, para efectos de esta investigación se considerará un ciberataque como aquellos que se aprovechan de las vulnerabilidades del software para tener acceso a él con el fin de destruir, alterar o interrumpir el sistema cibernético o físico asociado. Ahora bien, junto con la definición, para conceptualizar y analizar los ciberataques, resulta necesario considerar

una serie de elementos, entre estos: los actores involucrados, la ubicación, los medios, jurisdicciones y los motivos detrás de la realización de los mismos[1].

Para el presente estudio, también es importante hacer referencia una definición de ciberespacio. Dentro de la estrategia de ciberseguridad del Gobierno Federal de Alemania, se indica que el ciberespacio es el espacio virtual de todos los sistemas en red de tecnologías de la información. El ciberespacio se basa en la red de conexión y transporte universal y accesible al público de Internet, la cual puede ser complementada y ampliada a voluntad por otras redes de datos. Los sistemas informáticos que funcionan en un espacio virtual aislado no forman parte del ciberespacio[2].

En estas instancias, el Derecho Internacional no posee herramientas especializadas para regular ciberataques fuera del contexto de un conflicto armado. Asimismo, la mayoría de los Estados, a nivel nacional y en su relación con otros Estados, hasta el momento, no han podido establecer tratados que resuelvan la totalidad de las controversias en la materia, y lamentablemente, no es realista pensar en una solución a corto o mediano plazo. Por tanto, resulta esencial referirse a las fuentes del Derecho, los Principios Generales y la existente regulación sobre responsabilidad internacional de los Estados, que pueda resultar aplicable para el tratamiento de los ciberataques. El presente trabajo analiza las posibles bases que ofrece el Derecho Internacional en situaciones donde se violentan obligaciones internacionales fuera del contexto de un conflicto bélico.

En este sentido, resulta pertinente hacer mención a la máxima *ubi societas, ibi ius*, la cual era utilizada por los antiguos romanos y significa, que donde hay sociedad hay Derecho[3]. No cabe duda que desde los inicios de la humanidad ha existido la necesidad de un mínimo de reglas de conducta, con el propósito de preservar la especie y la paz en la

[1] Kristin Finklea, y Catherine A. Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement", Congressional Research Service, (enero 2015): 2.
[2] Annegret Bendiek, "Due Dilligence in Cyberspace", *Stiftung Wissenscharft und Politik German Institute for International and Security Affairs,* (2016): 7, consultado el 19 de setiembre 2016, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf.
[3] Jorge Francisco Sáenz Carbonell. *Elementos de la Historia del Derecho.* San José, Costa Rica: ISOLMA, 2009, 24.

convivencia. El Derecho Internacional no es la excepción a la regla, pues existen normas que regulan las relaciones entre los Estados.

Entorno a este aspecto, existe una discusión doctrinaria sobre qué es considerado una fuente en el Derecho Internacional y sobre cuáles son los tipos que existen, ya que es importante recordar que en esta área del Derecho no se cuenta con un ente dedicado exclusivamente a la creación de leyes, como lo hace en el Derecho interno el poder legislativo de cada país. Por su parte, Luis Varela, establece que por "fuentes de derecho internacional" debe entenderse "*no su fundamento, sino los modos por los que sus reglas se forman o manifiestan*"[4]. En este mismo sentido, Edmundo Vargas, establece que este concepto debe entenderse como "*la manifestación externa, la constatación del derecho internacional y no su fundamento o las causas materiales que las han originado*"[5].

Sin embargo, la doctrina establece que este concepto tiene múltiples concepciones: la positivista, la iusnaturalista y la objetivista. Desde la perspectiva positivista, las fuentes del Derecho Internacional son únicamente aquellas que emanan del consentimiento de las partes, es decir, solamente de un acuerdo de voluntades entre los Estados que se obligan. Por su parte, la teoría iusnaturalista considera que son fuentes de Derecho Internacional aquellas que son contempladas como fuentes formales (tratados y costumbre), y los principios generales del Derecho[6]. En cuanto a la corriente objetivista, tal y como explica James Crawford[7], existen dos tipos de fuentes: la formal y la material o creadora. Las fuentes formales se comprenden de aquellos métodos para crear reglas, cuya aplicación es general para quienes rige; y, como fuentes materiales las que proveen prueba de la existencia de reglas que cuando son establecidas, estas son vinculantes para todos y de aplicación general. Estas últimas, son reglas que atraen la atención sobre factores extrajurídicos[8].

[4] Luis A. Varela Quirós. *Las Fuentes del Derecho Internacional.* Bogotá, Colombia: Temis, 1996, 4.
[5] Edmundo Vargas Carrero. *Introducción al derecho internacional.* San José, Costa Rica: Juricentro, 1979, 20.
[6] Luis A. Varela Quirós, *op. cit.,* 5 y 7.
[7] James Crawford. *Brownlie's Principles of Principles of Public International Law*. Oxford, Reino Unido: Oxford University Press, 2012, 20.
[8] Luis A. Varela Quirós, *op. cit.,* 7.

Ahora bien, tal como explica Varela, el texto que muchos autores toman como base para sistematizar la teoría de las fuentes es el XII Convenio de la Haya de 18 de octubre de 1907, en cual en su artículo 7 establece "*[a] falta de un convenio entre las partes, el Tribunal aplicará las normas del Derecho Internacional. Si no existen normas generalmente reconocidas, el Tribunal fallará según los principios de derecho y de la equidad*". Sin embargo, como el mismo autor señala, el interés de este artículo quedó limitado al área doctrinal[9].

Ahora bien, en el ámbito práctico, las fuentes reconocidas de estos acuerdos de entendimiento en un ordenamiento jurídico positivo, se encuentran plasmadas en el artículo 38.1 del Estatuto de la Corte Internacional de Justicia, el cual establece que han de entenderse como fuentes del Derecho Internacional:

> a. las convenciones internacionales, sean generales o particulares, que establecen reglas expresamente reconocidas por los Estados litigantes;
>
> b. la costumbre internacional como prueba de una práctica generalmente aceptada como derecho;
>
> c. los principios generales de derecho reconocidos por las naciones civilizadas;
>
> d. las decisiones judiciales y las doctrinas de los publicistas de mayor competencia de las distintas naciones, como medio auxiliar para la determinación de las reglas de derecho, sin perjuicio de lo dispuesto en el Artículo 59.

No obstante, aun cuando este artículo es considerado la normativa más comprensiva en cuanto a enumeración de fuentes se refiere, no agota la totalidad de las fuentes existentes, las cuales, tal como señala Varela, han sido completadas por la CIJ y otros organismos internacionales[10]. Ahora bien, se procederá a realizar un breve análisis sobre cada una de

[9] Íbid.
[10] Íbid.

las fuentes mencionadas y aquellas que han sido desarrolladas por los órganos internacionales, ampliando la lista de los tipos de fuentes.

- *Tratados Internacionales*

Los Tratados Internacionales corresponden a una de las fuentes de obligaciones más importantes en el Derecho Internacional. En ese sentido se puede hacer referencia a dos tipos: los tratados "creadores de leyes" y los tratados bilaterales. Los tratados que crean leyes u obligaciones, poseen una influencia directa en el contenido del Derecho Internacional en general. Por su lado, los bilaterales, pueden evidenciar la existencia de una costumbre[11]. Aunque dogmáticamente no existe distinción entre ambos, se debe tomar especial atención al evaluar los mismos.

En el caso de tratados generadores de obligaciones legales, estos crean normas generales, formuladas como proposiciones legales con el objetivo de regular la conducta de las partes. Ejemplos de este tipo de tratados incluyen las cuatro Convenciones de Ginebra[12] y sus Protocolos[13], la Convención para la Prevención y la Sanción del Delito de Genocidio[14].

Aunque los tratados son de cumplimiento obligatorio para las partes, el número de Estados, la aceptación expresa de las reglas por parte de los Estados y, en algunos casos el

[11] James Crawford. *op. cit.*, 31.

[12] La Convención de Ginebra y sus Protocolos Adicionales son el centro del Derecho Internacional Humanitario, el cual regula la conducta de los conflictos armados y busca limitar sus efectos. Los mismos protegen a personas que no toman parte activa en las hostilidades y aquí ellos que ya no forman parte de estos. https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions.

[13] "El Protocolo de Ginebra de 1925 prohíbe el empleo en la guerra de armas biológicas y químicas. Dicho Protocolo se redactó y firmó en la conferencia para la supervisión del comercio internacional de armas y munición, celebrada en Ginebra del 4 de mayo al 17 de junio de 1925 bajo los auspicios de la Sociedad de Naciones, y entró en vigor el 8 de febrero de 1928". http://www.un.org/es/disarmament/instruments/geneva.shtml.

[14] La Convención sobre el Genocidio fue una de las primeras convenciones de las Naciones Unidas que trató temas humanitarios. Fue adoptada en 1948 en respuesta a las atrocidades cometidas durante la Segunda Guerra Mundial y luego de la resolución de la Asamblea General Res. 180(II) del 21 de diciembre de 1947, mediante la cual las Naciones Unidas reconoció que el *"genocidio es un crimen internacional, el cual implica la responsabilidad nacional e internacional de personas individuales y estados"*. Desde entonces, la Convención ha sido ampliamente aceptada en la comunidad internacional y ratificada por la mayoría de los Estados. https://ihl-databases.icrc.org/ihl/INTRO/357?OpenDocument.

carácter declaratorio de las provisiones de los mismos, produce un efecto generador de obligaciones[15]. Asimismo, Estados no parte de un tratado pueden aceptar las provisiones de un Tratado Internacional por medio de su conducta, lo cual representa una costumbre internacional.

Se establece entonces una estrecha relación entre los tratados y la Costumbre Internacional. Un Estado no parte a un Tratado puede ser afectado en forma indirecta por las normas contenidas en la misma, a menos de que se haya opuesto a la disposición por medio de una "objeción persistente", figura mediante la cual un Estado puede eximirse de la aplicación de una nueva regla de costumbre por persistentemente objetar la norma durante su formación[16].

La eventual consecuencia de no participar en dichos tratados creadores de obligaciones, es la inhabilidad de invocar los medios para solucionar disputas, dado que una disputa solo puede surgir bajo un tratado entre Estados parte del mismo[17]. Sin embargo, aun y cuando un Estado no es parte de un tratado, por vía de una Cláusula Opcional, o incluso por ser el contenido de la obligación, al ser costumbre, un Estado puede verse obligado a su cumplimiento. Esto se ejemplifica en el caso de *Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos de América), (Nicaragua)* donde Estados Unidos alegó una disposición excluyente de jurisdicción de la Corte Internacional de Justicia, debido a que no existía otro Estado afectado parte de la OEA. La Corte indicó que era libre de aplicar la Costumbre Internacional independientemente de la reserva sobre jurisdicción de la Carta de la OEA[18].

Como regla general, los requisitos de duración, consistencia y generalidad de la práctica junto con el *opinio iuris,* posicionan a la costumbre internacional a menudo por detrás de tratados específicos. Empero, a largo plazo, la costumbre internacional puede moldear o incluso modificar el texto de tratados, los cuales no pueden ser modificados de

[15] James Crawford, *op. cit.* 31.
[16] Ídem, 28.
[17] Ídem, 33.
[18] *Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos de América),* Jurisdicción y Admisibilidad, Reportes CIJ, 1984, 92.

modo realista, como es el caso del Artículo 51 de la Carta de las Naciones Unidas sobre la legítima defensa[19].

Dicho artículo reza de la siguiente manera:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales[20].

El derecho de legítima defensa existía en el Derecho Internacional Consuetudinario, el cual fue plasmado en dicho artículo. Sin embargo, este no menciona los elementos de necesidad y proporcionalidad como al analizarlos si lo ha hecho la Corte[21].

Este artículo también es ejemplo de una costumbre internacional; pues contrario a lo indicado en el artículo, la obligación de comunicar al Consejo de Seguridad el ejercicio de dicho derecho, no ha sido considerada como costumbre por el Derecho Internacional[22].

- *Costumbre Internacional*

El artículo 38 se refiere a Costumbre Internacional como evidencia de una práctica generalmente aceptada como derecho. En ese sentido, dos preguntas deben considerarse en

[19] James Crawford, *op. cit.*, 33.
[20] Naciones Unidas, *Carta de las Naciones Unidas*, 1 UNTS XVI (24 de octubre de 1945), Art. 51.
[21] *Legalidad de la Amenaza o Uso de Armas Nucleares,* Opinión Consultiva, Reportes CIJ, 1996, 41. *Nicaragua*, Sentencia, 176.
[22] *Nicaragua*, Sentencia, 200.

la determinación de la existencia de este elemento: ¿hay una práctica generalizada?; ¿es aceptada como derecho internacional? En el caso de *Fisheries* (Reino Unido v. Noruega), ante la Corte Internacional de Justicia (CIJ o Corte), el Juez Read describió costumbre internacional como la generalización de la práctica de los Estados[23].

Las fuentes materiales de la costumbre son varias, entre las cuales se pueden mencionar: correspondencia diplomática, declaraciones de políticas, comunicados de prensa, opinión de asesores legales de gobierno, manuales oficiales en cuestiones legales, decisiones ejecutivas, órdenes a fuerzas militares, legislación, decisiones judiciales nacionales e internacionales, práctica de organismos internacionales y resoluciones en relación con aspectos legales de los órganos de las Naciones Unidas[24]. El valor de dichas fuentes varía y depende de las circunstancias específicas del caso.

Para ser considerada Costumbre Internacional, no debe haber completa uniformidad en la práctica, si no meramente uniformidad sustancial. Una vez determinada la consistencia y generalidad de la práctica, la formación de una regla de costumbre no requiere una duración específica, o su práctica por un largo período. En este sentido se deben considerar dos elementos para determinar la existencia de costumbre: generalidad en la práctica de los Estados y *opinio iuris*.

Respecto al primer elemento de práctica generalizada, la consistencia no es requerida y, usualmente, el problema es distinguir una simple abstención de protesta por un número de Estados, frente a una práctica seguida por otros. El silencio puede demostrar aceptación tácita o simple falta de interés en el tema[25].

En el caso de *opinio iuris,* la CIJ puede inferir la existencia de una práctica general, de consenso doctrinario o de sus propias determinaciones o de otros tribunales[26]. La Corte se ha pronunciado en distintas ocasiones sobre la existencia o no de *opinio iuris,* como lo

[23] *Fisheries* (Reino Unido v. Noruega), Reporte CIJ, 1951. Opinión disidente Juez Read, 116.
[24] James Crawford, *op. cit.*, 24.
[25] Ídem, 25.
[26] Ídem, 26.

ha hecho en los casos de *Nicaragua*, *SS Lotus* (Francia v. Turquía) (*Lotus*), y *Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo) (Diallo)*. Sin embargo, en dichos pronunciamientos la Corte ha tomado diferentes enfoques, los cuales parecen depender del estado de la ley que es el punto de contención principal[27]. El abordaje puede depender en si la práctica está basada principalmente en un tratado o si la ley, en el caso específico, aún se está desarrollando.

- *Principios generales del Derecho Internacional*

A falta de Convenciones Internacionales o la existencia de una regla consolidada de costumbre, los Principios Generales del Derecho Internacional vienen a llenar ese vacío en la normativa. Se entiende así, que los Principios Generales del Derecho son una proposición legal tan fundamental que se pueden encontrar en todos los sistemas de Derecho[28]. Son inferencias lógicas que se pueden encontrar en cualquier sistema legal, tales como el principio de reparar un daño causado, los principios de interpretación de reglas, *res iudicata*, buena fe, *estoppel* y aquiescencia, entre otros.

Los tribunales internacionales no han adoptado un mecanismo para tomar en cuenta la legislación nacional, por el contrario, han empleado y adaptado métodos de razonamiento legal y analogías de derecho comparado para crear un cuerpo coherente de reglas a ser aplicadas en procesos judiciales a nivel internacional[29].

Referirse a Principios Generales del Derecho Internacional, puede a su vez referirse a reglas de Costumbre Internacional o a ciertas proporciones lógicas de razonamiento judicial existentes en el Derecho Internacional[30]. Entre estos principios se puede indicar consentimiento, reciprocidad, igualdad de los Estados, buena fe, integridad territorial, no intervención, y autodeterminación. A su vez, ciertos de estos principios han sido elevados a normas imperativas.

---

[27] Ídem, 27.
[28] James G., Apple, "General Principles of International Law", *International Judicial Monitor* 2, No. 2 (julio/agosto 2007). Consultado 17 de setiembre de 2016. http://www.judicialmonitor.org/archive_0707/generalprinciples.html.
[29] James Crawford, *op. cit.*, 35.
[30] Ídem, 37.

- *Medios auxiliares*

El artículo 38 inciso 1 punto d, establece como medios auxiliares para la determinación de reglas de derecho, las decisiones judiciales y las doctrinas de los publicistas de mayor competencia de las distintas naciones.

Las decisiones judiciales no son formalmente una fuente de derecho, pero pueden ser consideradas evidencia de la ley. Contrario a la tradición del *common law*, no son calificadas como precedente. A pesar de que la CIJ no sigue una doctrina de precedente, excepto en asuntos sobre procedimiento, la Corte se esfuerza por mantener consistencia. Sin embargo, la Corte tiene potestades incluso de alejarse de sus propias decisiones anteriores[31].

Con referencia a decisiones de otros tribunales internacionales, la Corte no se encuentra obligada a los criterios contenidos en esas decisiones. Sin embargo, el trabajo de tribunales como la Corte Penal Internacional, el Tribunal Criminal para la Antigua Yugoslavia, la Comisión de Reclamos Irán-Estados Unidos y el Tribunal Internacional Militar para el Juicio de los Principales Criminales de Guerra Alemanes, han contribuido sustancialmente en hallazgos significativos sobre cuestiones de Derecho[32], por lo que la Corte ha hecho referencia a estos y a tribunales arbitrales.

En relación con decisiones de la propia Corte, en teoría la CIJ aplica la ley y no la crea, únicamente resuelve disputas tal y como le son presentadas y no modifica la ley en sí misma[33]. A pesar de que las decisiones de la Corte son solo vinculantes para las partes y las opiniones consultivas no son vinculantes para ninguna parte, la historia ininterrumpida de la Corte, consistencia y amplia jurisdicción *ratione materiae*, ha resultado en pronunciamientos en temas de sustancia a los cuales se les ha dado gran peso[34].

[31] James Crawford, *op. cit.*, 39.
[32] Ídem, 40.
[33] Íbid.
[34] James Crawford, *op. cit.*, 41.

Por último, las decisiones de Cortes nacionales también tienen valor. Estas decisiones proveen prueba indirecta de la práctica de los Estados en cuestiones específicas y han sido una fuente importante de material en temas de inmunidad diplomática, inmunidad soberana y crímenes de guerra[35].

Adicionalmente a decisiones judiciales de tribunales nacionales e internacionales, surgen otras fuentes materiales a considerar: conclusiones de conferencias internacionales, resoluciones de la Asamblea General de las Naciones Unidas, el trabajo de expertos y el trabajo de la Comisión de Derecho Internacional (CDI).

En primer lugar, el "acto final" o conclusiones de conferencias internacionales constituyen evidencia del estado de la ley en dicho tema. Incluso, antes de la ratificación necesaria del tratado, el acto puede ser influyente[36].

En segundo lugar, las resoluciones de la Asamblea General de las Naciones Unidas, aunque no son obligatorias para los Estados miembros, muestran evidencia de la opinión de gobiernos en uno de los foros más grandes para la expresión de dichas opiniones. Incluso cuando las resoluciones son enmarcadas como principios generales, pueden indicar la base del desarrollo progresivo de la ley y consolidación de costumbre[37]. Como ejemplo de resoluciones creadoras de obligaciones, cabe mencionar la Declaración sobre la Concesión de la Independencia a los Países y Pueblos Coloniales[38], Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970[39] y la Declaración de los Principios Jurídicos que deben regir las Actividades de los Estados en la Exploración y Utilización del Espacio[40].

[35] Ídem.
[36] Ídem, 42.
[37] Íbid.
[38] Declaración sobre la concesión de la independencia a los países y pueblos coloniales. Aprobada por la resolución 1514 (XV) de la Asamblea General de las Naciones Unidas el 14 de diciembre de 1960.
[39] Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 (XXV)).
[40] Asamblea General, Resolución, RES 2222 (XXI) (1996), Declaración de los Principios Jurídicos que deben regir las Actividades de los Estados en la Exploración y Utilización del Espacio.

En relación con las doctrinas de los publicistas de mayor competencia de las distintas naciones, sus trabajos y las opiniones se utilizan en forma amplia. A pesar de que en apariencia la Corte no utiliza en sus sentencias referencia a la escritura de juristas, esto se debe mayormente al proceso de redacción colectiva de los juzgamientos y la necesidad de evitar el utilizar citaciones. Sin embargo, evidencia de que sí son utilizadas, normalmente se nota en las opiniones separadas en donde el trabajo es más detallado y refleja el método de la Corte[41].

Por su lado, el trabajo de la Comisión de Derecho Internacional, ha sido considerado ampliamente por tribunales y Cortes Internacionales por su trabajo en distintas áreas. Su membresía combina cualidades técnicas y la experiencia del servicio civil; por lo tanto, sus trabajos por lo general reflejan soluciones aceptables a gobiernos, al manifestar una variedad de perspectivas políticas y regionales[42].

Por último, otras deferencias de importancia al momento de las decisiones por la Corte son cuestiones de equidad, consideraciones humanitarias e intereses legítimos[43], las cuales son tomadas en cuenta no como fuente directa de Derecho, pero si como elementos relevantes de atención en la toma de decisiones.

- *Soft Law*

Si bien no existe una definición precisa de lo que se entiende por *soft law*, se ha dicho que el concepto puede variar, según los atributos que se predican del mismo[44]. Dichas normas han recibido diversas denominaciones por la doctrina, tales como: resoluciones, recomendaciones, guías, códigos o estándares de conducta[45]. Ahora bien, existen tres aceptaciones y sus respectivas críticas sobre lo que constituye *soft law*, que se derivan de la práctica de las organizaciones internacionales y la abundante doctrina sobre el tema.

[41] James Crawford, *op. cit*., 43.
[42] Ídem, 44.
[43] Ídem, 44-47.
[44] Pablo Damián Colmegna, "Impacto de las normas de soft law en el Desarrollo del Derecho Internacional de los Derechos Humanos", Revista electrónica del Instituto de Investigaciones "Ambrioso L. Gloja", No. 8 (invierno, 2012): 30, consultado 18 de septiembre de 2016, http://www.derecho.uba.ar/revistagioja/articulos/R0008A006_0004_investigacion.pdf.
[45] Shaw M, *International Law.* Cambridge, Inglaterra: Cambridge University Press, 2008, 118.

Primero, se puede llamar así a normas que se encuentran en proceso de formación y aún no han adquirido la validez jurídica, como es el caso de un tratado internacional suscripto que no cuenta con el número de ratificaciones mínimas para entrar en vigor[46]. No obstante, el autor Barberis, establece que en la doctrina ya existe la diferencia entre las disposiciones que han adquirido validez jurídica y las que no, y esto recibe el nombre de *lex lata* y *lex ferenda*, por lo que señala que no parece justificado llamar así a algo que ya tenía su propio nombre[47].

Segundo, se le llama de esta forma a normas jurídicas de contenido difuso o vago, en la cuales resulta difícil determinar si sus disposiciones han sido o no cumplidas[48]. Sobre esta definición, Barberis establece que viene a constituir dos concepciones distintas, como si hubiesen prescripciones provenientes del *hard law* y otras del *soft law*, cuya obligatoriedad sería más difusa. El autor señala que la obligatoriedad de las conductas son la misma, pues, aunque haya una falta de precisión en la enunciación, la estructura de la norma no se ve afectada, por lo que la diferencia realmente radica en que hay mayor o menor dificultad en comprobar su cumplimiento, no en el grado de obligatoriedad de cada una[49].

Por último, el término se ha empleado para designar normas que se desprenden de resoluciones de la Asamblea General de las Naciones Unidas y de algunas organizaciones regionales, ya sean acuerdos políticos, códigos de conducta, entre otros[50]. La crítica planteada por el autor Barberis en este aspecto, es que la idea se sostener la existencia de normas pertenecientes a un derecho "blando" y que constituirían un orden jurídico intermedio, no aparece como razonable, pues señala, que podría admitirse que esas normas

[46] Julio A. Barberis. *Formación del derecho internacional.* Buenos Aires, Argentina: Editorial Ábaco de Rodolfo Depalma, 1994, 283.
[47] Ídem, 285.
[48] Ídem, 283.
[49] Ídem, 286.
[50] Idem, 284.

pertenezcan a otro orden normativo, que no sería el jurídico, pero señala que no resulta lógico postular un orden jurídico intermedio[51].

Este tipo de fuente se encuentra vinculado especialmente al ámbito del derecho económico internacional, y su origen se remonta al inicio de las relaciones entre Estados desarrollados y subdesarrollados[52], y se ha sugerido la idea de que:

> […] las normas de *soft law*, caracterizadas por carecer de fuerza vinculante para los Estados que las adoptan, presentan ciertas ventajas por sobre los tratados internacionales, los cuales constituyen los acuerdos vinculantes por excelencia. Así es como las normas de *soft law* pueden ser adoptadas y modificadas más rápida y flexiblemente que los tratados, ya que las mismas no requieren ratificación; son más fáciles de negociar ya que implican un menor nivel de compromiso; mitiga los posibles efectos adversos que para el Estado podría tener el dictado de la norma, ya que la misma resulta no vinculante[53].

De igual manera, la categoría de *soft law* puede encontrar vinculación con otras fuentes concebidas en el artículo 38.1 del Estatuto de la CIJ, tales como los tratados internacionales. Un ejemplo de esto es la amplia discusión en la doctrina alrededor de las Resoluciones del Consejo de Seguridad de Naciones Unidas, las cuales no podrían ser consideradas como fuentes autónomas, pues aunque al momento de redactar la Carta de Naciones Unidas en su artículo 25 se dispuso que los Estados se comprometían a aceptar y cumplir las decisiones del Consejo, su fuerza vinculante está necesariamente ligada al tratado que le dio ese valor jurídico; por lo tanto, no se podrían ver como una fuente en sí misma.

---

[51] Ídem, 288.
[52] Ídem, 284.
[53] Pablo Damián Colmegna, "Impacto de las normas de soft law en el Desarrollo del Derecho Internacional de los Derechos Humanos", Revista electrónica del Instituto de Investigaciones "Ambrioso L. Gloja", No. 8 (invierno, 2012): 32, consultado 18 de septiembre de 2016, http://www.derecho.uba.ar/revistagioja/articulos/R0008A006_0004_investigacion.pdf.

De esta manera se concluye que por *soft law* ha de entenderse esas fuentes del Derecho que no pueden ser claramente distinguidas dentro del artículo 38.1 del Estatuto de la CIJ.

- *Actos Jurídicos Unilaterales*

El autor Varela utiliza la definición de actos unilaterales dada por Manuel Díez de Velásco, la cual establece que es "*una manifestación de voluntad de un solo sujeto de Derecho Internacional, cuya validez no depende prima facie de otros actos jurídicos y que tiende a producir efectos –creación de deberes y obligaciones– para el sujeto que la emite y para terceros en determinadas circunstancias*"[54], por lo que es un acto que se basta a sí mismo para producir efectos obligatorios[55].

Ahora bien, hay ciertos elementos que caracterizan un acto jurídico unilateral creador de obligaciones jurídicas. En este sentido, Julio Barberis establece que los elementos necesarios son[56]:

a) Manifestación de voluntad de uno o varios sujetos de Derecho Internacional con capacidades suficientes

Barberis explica, que no es necesario que el autor del acto sea un Estado, ya que puede tratarse de otro sujeto internacional, siempre que sea capaz de asumir las consecuencias de la manifestación de voluntad que realizó. Ahora bien, para considerar que la declaración es realizada por un Estado, surge un requisito extra establecido por el principio 4 de los Principios rectores de las declaraciones unilaterales de los Estados, el cual establece:

[54] Luis A. Varela Quirós, *op. cit.*, 106.
[55] Ídem, 107; Comisión de Derecho Internacional, Principios rectores de las declaraciones unilaterales de los Estados, 2006, principio 1; y *Caso de Pruebas Nucleares (Nueva Zelandia v. Francia)*. Juzgamiento, Reportes CIJ, 1974, párr. 46.
[56] Julio A. Barberis, *op. cit*., 1994,131.

> Una declaración unilateral obliga internacionalmente al Estado sólo si emana de una autoridad que tenga competencia a estos efectos. En virtud de sus funciones, los jefes de Estado, jefes de gobierno y ministros de relaciones exteriores son competentes para formular tales declaraciones. Otras personas que representan al Estado en esferas determinadas podrán ser autorizadas para obligar a éste, mediante sus declaraciones, en las materias que correspondan a su esfera de competencia.

Por lo que podemos concluir que, el sujeto que realice la declaración debe ser capaz de asumir las consecuencias de las mismas a nivel internacional, y que es requerido que sea una autoridad competente la que realice una manifestación de voluntad, para poder obligar a un Estado por medio de la figura de un acto jurídico unilateral.

b) Manifestación de voluntad no vinculada con ningún acto convencional

La manifestación de un sujeto de Derecho Internacional, no requiere el consentimiento de ninguna otra parte, ni una actitud complementaria de otro sujeto, para que genere una obligación para sí mismo; característica que distingue a los tratados de los actos jurídicos unilaterales[57]. La CIJ estableció que las declaraciones unilaterales, si se dan públicamente, y con la intención de obligarse, aunque no se hagan en el contexto de negociaciones internacionales, son vinculantes[58]. En cuanto a las formalidades, la CIJ hace énfasis en que los sujetos de Derecho Internacional, son libres de elegir la forma que les parezca[59], siempre que la intención resulte claramente de ella[60].

c) Manifestación de voluntad tendiente a establecer una regla de derecho en el orden jurídico internacional

El autor Barberis, establece que es necesario referirse al contenido de la manifestación de voluntad, pues el autor habla de que el acto jurídico unilateral debe

[57] Íbid, 133.
[58] *Caso de Pruebas Nucleares, párr. 46.*
[59] *Templo de Preah Vihear (Camboya v. Tailandia)*. Excepciones Preliminares, Reportes CIJ, 1961, 31.
[60] Íbid, 32.

establecer una disposición en ámbito normativo[61]. En este sentido, la CIJ estableció que los Estados tomarán nota de las declaraciones unilaterales públicas de otros Estados y se basarán en su eficacia[62] y tendrán derecho a exigir que se respete la obligación creada[63]. Por su parte, el relator especial Roberto Ago, establece que esta norma general ha sido ampliamente respaldada por la práctica de los Estados[64].

d) Manifestación de voluntad regida por el derecho de gentes

Barberis explica que es importante analizar si la declaración de voluntad realizada se halla regida por el Derecho Internacional o por el Derecho interno del Estado que la realizó, pues establece que los Estados tienen derecho a efectuar actos jurídicos unilaterales que no estén sujetos al Derecho Internacional, siempre que no sean contrarios a normas de *jus cogens*, pues ningún sujeto puede valerse de la posibilidad de salirse del ámbito del Derecho Internacional para transgredir normas jurídicas imperativas[65].

Partes de un conflicto internacional ante la Corte Internacional de Justicia

La CIJ ha establecido que un sujeto de Derecho Internacional es una entidad que posee derechos y obligaciones en el plano internacional, así como la capacidad de proteger sus derechos cuando inicia un proceso ante una Corte de esta naturaleza[66]. Asimismo, Crawford indica que además de lo mencionado, debe tener la posibilidad de ser objeto de esas denuncias, poder realizar tratados o arreglos válidos a nivel internacional y poseer inmunidades y privilegios a nivel nacional[67]. Según todo lo anterior, se hará referencia a las partes que pueden formar parte de un conflicto internacional.

---

[61] Julio A. Barberis, *op. cit*., 136.
[62] *Caso de Pruebas Nucleares, párr. 53.*
[63] Ídem, párr. 49.
[64] Roberto Ago. Addendum al Octavo Informe sobre la Responsabilidad del Estado. UN Doc. A/CN.4/318/Add.5 a 7, 29 de febrero, 10 y 19 de junio de 1980. Nueva York: Comisión de Derecho Internacional, 1980, tomo II, primera parte.
[65] Julio A. Barberis, *op. cit.*, 139-140.
[66] *Reparaciones por daños sufridos al servicio de Naciones Unidas*, Opinión Consultiva, Reporte CIJ,1949, 178-180.
[67] James Crawford, *op. cit.* 117.

- *Estados*

Como señala Thomas Hobbes en el reconocido libro *El Leviatán*, los hombres *"que naturalmente aman la libertad y el dominio sobre los demás"* buscan resguardar aquello que él describe como *"el cuidado de su propia conservación y, por añadidura, el logro de una vida armónica; es decir, el deseo de abandonar [l]a miserable condición de guerra […que] es consecuencia necesaria de las pasiones naturales de los hombres, cuando no existe poder visible que los tenga a raya y los sujete, por temor al castigo"*[68]; por medio de la creación de la figura que hoy se conoce como Estado.

La manera de organización social de la que habla Hobbes, ha venido cambiando a lo largo de la historia. Como explica el autor Mario de la Cueva y de la Rosa, el *"Estado nace bajo la forma de gobierno de la monarquía, particularmente la monarquía absoluta, aquella en la que todo el poder corresponde al monarca"*[69], y como un claro ejemplo de esto, se aprecia la definición que proviene de la figura el autor Thomas Hobbes, el cual lo define como *"una persona de cuyos actos una gran multitud, por pactos mutuos, realizados entre sí, ha sido instituida (sic) por cada uno como autor, al objeto de que pueda utilizar la fortaleza y medios de todos, como lo juzgue oportuno, para asegurar la paz y la defensa común"*[70].

Sin embargo, como ya se indicó, el concepto de esta figura se ha venido transformando, hasta llegar al concepto de Estado como sujeto de Derecho Internacional, cuya definición se encuentra contemplada en el artículo 1 de la Convención sobre Deberes y Derechos de los Estados[71], el cual establece:

> **ARTÍCULO 1**
>
> El Estado como persona de Derecho Internacional debe reunir los siguientes requisitos:

[68] Thomas Hobbes, *El Leviatán. O la materia, forma y poder de una república eclesiástica y civil.* México: Fondo de Cultura Económica, 2010, 137.
[69] Marco de la Cueva y de la Rosa, *Teoría General del Estado. Apuntes de las clases impartidas por ilustres juristas del siglo XX.* México: Suprema Corte de Justicia de la Nación, 2014, 22.
[70] Thomas Hobbes, *op. cit.* 141.
[71] Convención sobre Derechos y Deberes de los Estados. Aprobada en la séptima Conferencia de la Organización de Estados Americanos en Montevideo en diciembre de 1933.

I. Población permanente.

II. Territorio determinado.

III. Gobierno.

IV. Capacidad de entrar en relaciones con los demás Estados.

Por población permanente, ha de entenderse una comunidad estable, pues sin las bases físicas y humanas para dialogar de una comunidad organizada, no se puede hablar de Estado. El segundo elemento corresponde al territorio, este es un elemento primario; pues no se puede pensar en una comunidad política estable sin un territorio en donde los habitantes pertenecientes a un Estado puedan desarrollar sus actividades. Por otra parte, se tiene el requisito de poseer un gobierno, el cual corresponde a tener organismos que centralicen tanto el poder legislativo como el administrativo. Sin embargo, como indica Crawford, para ser considerado un Estado a nivel internacional no siempre se ha requerido la estabilidad política de la sociedad en cuestión y ejemplo de ello son Ruanda y Burundi, los cuales fueron admitidos en Naciones Unidas en 1962, cuando aún su estructura de gobierno no estaba bien consolidada[72].

Finalmente, se observa la capacidad de entrar en relaciones con los demás Estados, lo cual también podría ser visto como independencia de otro gobierno. En este punto, aparece un requerimiento importante, como lo es el reconocimiento por parte de otros Estados. Un Estado para ser considerado como tal tiene que tener la capacidad de tener derechos, poderes, privilegios e inmunidades respecto de otros Estados, así como establecer tratados o arreglos con los mismos. No obstante, no se ha definido un número mínimo de reconocimientos para poder ser considerado como tal a nivel internacional.

Existe la posibilidad de que un Estado, que cumpla con todos los requisitos antes mencionados, sea sujeto parte de un conflicto internacional debido a las acciones de personas *sui generis* y agentes no tradicionales. No obstante, es esencial recordar, que es el Estado quien sigue siendo responsable y por ende sujeto ante la CIJ. En este sentido, el

[72] James Crawford, *op. cit.* 129.

tema de responsabilidad internacional de un Estado por actos de terceros será analizado con mayor profundidad en el capítulo I del presente trabajo.

- *Organizaciones Internacionales*

Según el artículo 2(a) sobre el Poyecto de Artículos referentes a la Responsabilidad Internacional de las Organizaciones Internacionales, dado por la Asamblea General en resolución de 30 de mayo de 2011, una organización internacional ha de entenderse como:

> […] una organización instituida por un tratado u otro instrumento regido por el Derecho Internacional y dotada de personalidad jurídica internacional propia. Además de los Estados, las organizaciones internacionales pueden contar entre sus miembros con otras entidades[73].

Asimismo, la CIJ en la *Opinión Consultiva de Reparaciones por daños sufridos al Servicio de Naciones Unidas*, afirmó:

> *[…] the Organization was intended to exercise and enjoy, and is in fact exercising and enjoying, functions and rights which can only be explained on the basis of the possession of a large measure of international personality and the capacity to operate upon an international plane. It is at present the supreme type of international organization, and it could not carry out the intentions of its founders if it was devoid of international personality. It must be acknowledged that its Members, by entrusting certain functions to it, with the attendant duties and responsibilities, have clothed it with the competence required to enable those functions to be effectively discharged.*
>
> *Accordingly, the Court has come to the conclusion that the Organization is an international person. That is not the same thing as saying that it is a state, which it certainly is not, or that its legal personality and rights and*

[73] Asamblea General, Resolución A/CN.4/L.778 30 de mayo de 2011, *Responsabilidad de las organizaciones internacionales.*

duties are the same as those of a state. Still less is it the same thing as saying that it is a "super-state" whatever the expression may mean […] What it does mean is that it is a subject of international law and capable of possessing international rights and duties, and that it has capacity to maintain its rights by bringing international claims[74].

En virtud de lo anterior, cabe concluir que las organizaciones internacionales poseen capacidad para ser consideradas como parte de un conflicto internacional, pues poseen personalidad internacional con capacidad de adquirir obligaciones y derechos en este campo, así como de gozar de inmunidades.

- *Grupos Beligerantes*

Los Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (AREHII), establecen en su artículo 10 inciso 2, la posibilidad de que un movimiento insurreccional sea sujeto de Derecho Internacional por volverse un nuevo Estado dentro de un Estado preexistente. Lo que nos deja como consecuencia, que un grupo beligerante o un movimiento insurreccional, no pueden ser sujetos de Derecho Internacional, pues al darles carácter de Estado, entran dentro de la categoría antes analizada. Este tema se estudia con mayor detalle dentro del capítulo I del presente trabajo.

[74]Reparaciones por daños sufridos al servicio de Naciones Unidas, 179. "*La Organización tenía la intención de ejercer y disfrutar, y de hecho es ejercer y disfrutar, funciones y derechos que sólo pueden explicarse sobre la base de la posesión de una gran medida de la personalidad internacional y la capacidad de operar en un plano internacional. Es en la actualidad el tipo supremo de la organización internacional, y que no podía llevar a cabo las intenciones de sus fundadores si era carente de personalidad internacional. Hay que reconocer que sus miembros, al encomendar ciertas funciones a ella, con los deberes y las responsabilidades correspondientes, han revestido con la competencia necesaria para que estas funciones a desarrollar con eficacia. En consecuencia, el Tribunal ha llegado a la conclusión de que la Organización es una persona internacional. Eso no es lo mismo que decir que es un estado, que ciertamente no es, ni que su personalidad jurídica y los derechos y deberes son los mismos que los de un estado. Menos aún es que lo mismo que decir que es un "súper-estado" cualquiera que sea la expresión puede significar [...] Lo que sí significa es que se trata de un sujeto de derecho internacional y capaz de ser titular de derechos y obligaciones internacionales, y que tiene capacidad de mantener sus derechos interponiendo reclamaciones internacionales".* Traducción hecha por las autoras.

Protección Diplomática

La protección diplomática corresponde a:

> […] la acción que un Estado lleva a cabo, frente a otro Estado o una Organización Internacional, reclamando la debida aplicación del Derecho Internacional, bien en relación con un hecho ilícito del que han sido víctimas sus nacionales e imputable a las autoridades del Estado o la Organización frente a la cual se reclama, bien para asegurar el respeto de sus propios derechos. [75]

Asimismo, la CIJ y la Corte Permanente de Justicia Internacional (CPJI) se han referido a la figura en múltiples ocasiones. En el Caso de Concesiones Palestinas de Mavrommatis la CPJI estableció que un Estado en realidad está haciendo valer sus propios derechos, al garantizar el respeto de las reglas de Derecho Internacional en favor de sus nacionales[76].

En el caso de los hermanos *LaGrand (Alemania v. Estados Unidos)*, mediante sentencia del 27 de junio de 2001, la CIJ estableció que un Estado puede tomar bajo sus auspicios el caso de uno de sus nacionales e instituir procedimientos judiciales en representación de estos[77].

En el caso *Avena y otros Nacionales Mexicanos (México v. Estados Unidos de América) (Avena)* [78], la CIJ estableció que observaría inicialmente que los derechos individuales de los mexicanos conforme al inciso 1 (b) del Artículo 36 de la Convención de Viena son derechos que deben hacerse valer, en primer lugar dentro del régimen jurídico local de los Estados Unidos y solo una vez concluido ese proceso y agotados los recursos

[75] Julio D. González Campos; Luis I. Sánchez Rodríguez; Paz Andrés Sáenz de Santamaría, "Curso de Derecho Internacional Público", Segunda Edición Revisada, Editorial Civitas, (Madrid 2002): 385.
[76] Concesiones Palestinas de Mavrommatis (Grecia v. Gran Bretaña), Sentencia, CPJI Rep Series A No 2, 12.
[77] *LaGrand (Alemania v. Estados Unidos)*, Reportes 2001, p.466, para. 42.
[78] *Avena y otros Nacionales Mexicanos (México v. Estados Unidos de América), Sentencia, Reportes CIJ 2004, p. 12*, para. 40.

que otorga el derecho interno, México tendría derecho de defender las demandas individuales de sus nacionales mediante el procedimiento de protección diplomática.

En razón de lo anterior, cabe concluir que la protección diplomática es una posibilidad que tienen los Estados para proteger a sus ciudadanos frente otros Estados. No obstante, la misma Corte ha establecido que deben agotarse los recursos internos previo a que un Estado pueda tomar como suya una violación a los derechos de uno de sus ciudadanos. Por lo tanto, un ciudadano podría ser la razón por la cual se inicie un proceso internacional, aunque resulta esencial aclarar que esto no implica que un civil pueda ser parte en un proceso ante la Corte Internacional de Justicia.

Jurisdicción y Admisibilidad ante la Corte Internacional de Justicia

Cuando existen conflictos entre Estados, surge una serie de posibilidades para la resolución pacífica de los mismos. Un ejemplo de estos medios es la existencia de la Corte Internacional de Justicia, la cual fue establecida en 1945 por la Carta de la ONU y comenzó su labor en 1946. Es el órgano judicial principal de las Naciones Unidas y una entidad central para la solución pacífica de controversias jurídicas entre Estados. Funciona de conformidad con su Estatuto, el cual forma una parte integral de la Carta de la ONU.

La CIJ vino a sustituir a la Corte Permanente de Justicia Internacional, establecida por el Acuerdo de la Liga de Naciones y estuvo operativa entre 1922 y 1940. Finalmente, se disolvió en 1946. La sede de la Corte se encuentra en La Haya (Países Bajos)[79].

No obstante, para que la Corte pueda conocer de un caso se requiere que los Estados involucrados acepten su jurisdicción, ya sea, a) firmando un acuerdo especial; b) convirtiéndose en Parte de un Tratado que estipula la resolución de controversias de la Corte, o, c) presentando una declaración unilateral (también llamadas declaraciones de "cláusulas opcionales") donde se reconozca la jurisdicción de la Corte. Puede también ser

[79] Confederación Suiza, Manual sobre la aceptación de la jurisdicción de la Corte Internacional de Justicia: Modelo de cláusulas y formulaciones tipo, (2014):6, consultado el 23 de febrero de 2017, https://www.eda.admin.ch/dam/eda/es/documents/publications/Voelkerrecht/handbook-jurisdiction-international-court_es.

expresado luego de que la Corte haya asumido competencia (*forum prorogatum*). En este orden de ideas es importante tener presente que:

1. El acceso a la Corte es otorgado a todos los Estados que son Parte del Estatuto de la Corte, según lo establece el artículo 35.1 del mismo instrumento.
2. Todos los miembros de las Naciones Unidas automáticamente son Parte del Estatuto de la Corte según lo establece el artículo 93.2 de la Carta de la ONU.
3. Sujeto a ciertas condiciones, un Estado que no es miembro de las Naciones Unidas también puede ser Parte del Estatuto de la Corte según lo establece el artículo 93.2 de la Carta de la ONU.
4. A modo de excepción, la Corte puede también estar abierta a Estados que no sean Parte de su Estatuto, según como se encuentra contemplado en el artículo 35.2 del Estatuto de la Corte; y siguiendo las condiciones que determinó el Consejo de Seguridad para aquellos Estados que no sean Partes del Estatuto, en su Resolución 9 de 15 de octubre de 1946[80].
5. Según el artículo 36.2 del Estatuto de la Corte, los Estados pueden, en cualquier momento, declarar que reconocen como obligatorio *ipso facto* y sin convenio especial respecto a cualquier otro Estado que acepte la misma obligación, la jurisdicción de la Corte, en todas las controversias jurídicas en relación con (a) la interpretación de un tratado, (b) a cualquier cuestión de Derecho Internacional, (c) a la existencia de cualquier hecho que, si fuere establecido, podría constituir un incumplimiento de una obligación internacional, (d) a la naturaleza o extensión de la reparación que ha de hacerse por el quebrantamiento de una obligación internacional[81].

[80] Consejo de Seguridad. Resolución número 9, La Corte Internacional de Justicia. 15 de octubre de 1946, disponible en: http://www.un.org/es/sc/documents/resolutions/1946.shtml
[81] Confederación Suiza, Manual sobre la aceptación de la jurisdicción de la Corte Internacional de Justicia: Modelo de cláusulas y formulaciones tipo, (2014):10.

Justificación del tema

En años recientes, la comunidad internacional ha visto de manera cada vez más frecuente, por parte de Estados, individuos o grupos no estatales, actividades por medio del ciberespacio.

En el 2007 Estonia fue blanco de una serie de ciberataques que afectaron de manera importante la economía del país. El primer ataque tuvo lugar el 27 de abril de 2007, cuando se infiltró el sitio web del Primer Ministro del Estado. Posteriormente periódicos, medios televisivos, escuelas y hasta bancos fueron afectados por los ciberataques[82], lo cual dejó importantes pérdidas para el Estado.

Al siguiente año, el 20 de julio de 2008, meses antes de que iniciara el bombardeo entre Georgia y Rusia que originó la Guerra de Osetia del Sur, inició una serie de ciberataques que dieron como consecuencia el impedimento de la distribución de servicios en Georgia[83].

Tiempo después, en el 2010, se conoció lo que fue llamado Stuxnet, un "gusano" informático y primer virus diseñado para atacar estaciones de energía, plantas de agua y otras unidades industriales[84]. Este virus infectó la base nuclear de Irán así como a más de 30.000 direcciones IP (*Internet Protocol* por sus siglas en inglés) en el mismo país, lo cual se consideró como el lanzamiento de una "guerra electrónica", según señaló Mahmoud Liayi del Ministerio de Industria de Irán[85]. Stuxnet lo crearon los Estados Unidos e Israel,

[82] Steven Lee Mayers, "Cyberattack on Estonia stirs fear of 'virtual war'", *New York Times*, 18 de mayo de 2007, Europa, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html.
[83] John Markoff, "Before the gunfire, Cyberattacks", New York Times, 12 de agosto de 2008, Tecnología, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
[84] BBC Mundo, "Alertan sobre virus que puede apagar fábricas", *BBC Mundo*, 24 de septiembre de 2010, sección Tecnología, versión en línea, consultado el 10 de junio de 2016, http://www.bbc.com/mundo/ciencia_tecnologia/2010/09/100924_1043_virus_gusano_malware_stuxnet_iran_dc.shtml.
[85] BBC Mundo, "Virus infecta planta nuclear iraní", *BBC Mundo*, 26 de septiembre de 2010, sección Internacional, versión en línea, consultado el 10 de julio de 2016, http://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw.shtml.

según señalaron los medios y esto fue solamente el inicio de posteriores ataques más poderosos, como el lanzamiento de la ciberarma denominada *Flame*[86].

Posteriormente, en noviembre de 2014 la compañía americana Sony Pictures, sufrió un ciberataque cuya dimensión nunca antes había sido vista contra una empresa americana, el cual emitió Corea del Norte. Montañas de documentos fueron robadas, los centros de datos internos borrados y el 75 por ciento de los servidores destruidos[87].

Todos los casos mencionados resultan claros ejemplos de todas las consecuencias que podría acarrear un ciberataque y de la rápida evolución de las tecnologías. Asimismo, evidencian una necesidad y una nueva realidad a la cual debe dar respuesta el Derecho Internacional. Los hechos expuestos generaron tensiones entre Estados e incluso, como lo es el caso de aquellos que se llevaron a cabo en el 2008 en Georgia, fueron el preludio de un enfrentamiento armado.

El avance tecnológico supera en tiempo al desarrollo de la creación de las leyes, tanto nacionales como internacionales, las cuales permitan regular esta situación. Esto deja como resultado la necesidad de encontrar una manera de ofrecer respuesta a esta nueva realidad con los medios que se cuentan y la normativa y los principios ya existentes. Si bien es cierto, en un panorama ideal, la creación de un marco normativo especializado en la materia sería una opción, este trabajo pretende demostrar que actualmente se cuenta con los medios necesarios para dar respuesta a los ciberataques en tiempos de paz.

[86] David E. Sanger, "Obama order sped up wave of cyberattacks against Iran", *New York Times*, Middle East, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[87] Michael Cieply y Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm", *New York Times*, Media, 30 de diciembre de 2014, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html, y Michael Schmitt, "International Law and Cyber Attacks: Sony v. North Korea", *Just Security*, (17 de diciembre de 2014, 9:29 a.m.), consultado el 10 de julio de 2016, https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

El anonimato y la difícil atribución de los ciberataques son los mayores retos que enfrenta la persecución de la comisión de los mismos[88]. La tecnología actual y las distintas formas de burlar la identificación de la fuente de un ataque por el ciberespacio, resulta que identificar el servidor real desde donde se origina el ciberataque sea sumamente complejo y, en ocasiones, hasta imposible. Esto sin mencionar la dificultad aún mayor que presenta el identificar los autores responsables.

Es en virtud de lo anterior que debe considerarse la atribución directa e indirecta de los ciberataques y el uso de la prueba indiciaria en la materia, así como otras opciones que impidan dejar en la impunidad las consecuencias de un ataque de esta naturaleza, como lo es la falta de debida diligencia de un Estado.

Todas estas opciones mencionadas, así como la aplicación del marco jurídico internacional ya existente, serán desarrolladas a lo largo de la tesis, para así intentar dar respuesta a la necesidad inminente de plantear medios jurídicos que ofrezcan una solución a esta nueva realidad.

El desarrollo planteado y efectuar el respectivo análisis, es importante para intentar descubrir los medios jurídicos que permitan establecer la prohibición del ciberespacio como un arma, o al menos, limitar el uso del mismo como tal, para así mitigar los daños que puedan causar; o en su defecto, para otorgar seguridad jurídica en la materia a los Estados, sin importar el nivel de desarrollo tecnológico y las posibilidades que tengan los diferentes países de defenderse por otros medios distintos a los legales.

El exponer las diferentes opciones jurídicas que permitan llevar a un Estado ante la Corte Internacional de Justicia por la comisión de un ciberataque contra otro Estado, puede prevenir conflictos de mayor envergadura e incluso la comisión de los mismos; pues al lograr exponer los medios que impidan la impunidad de un ataque de esta naturaleza, los Estados estarían prevenidos sobre lo que significaría el llevar a cabo este tipo de intrusiones.

[88] Duncan B. Hollis, "An e-SOS for Cyberspace", *Harvard International Law Journal*, No. 2, Vol. 52, (Verano, 2011): 378.

Más aún cuando los Estados estén conscientes de las consecuencias que pueden derivar de dichas actividades e incluso así no cumplan con lo establecido por el ordenamiento jurídico internacional, se da una oportunidad a otros Estados de presentar reclamos a la Corte Internacional de Justicia y encontrar debida reparación por los daños causados.

Hipótesis

El Derecho Internacional cuenta con las bases necesarias, en diferentes áreas, para establecer la responsabilidad internacional de un Estado por un ciberataque cometido fuera del contexto de un conflicto armado.

Objetivos

Objetivo general

Analizar los mecanismos existentes en el Derecho Internacional y su aplicación para el establecimiento de la responsabilidad internacional de un Estado como consecuencia de un ciberataque.

Objetivos específicos

1. Establecer un panorama general sobre las reglas que rigen la responsabilidad internacional de los Estados ante la Corte Internacional de Justicia.
2. Analizar la aplicación de los antecedentes jurisprudenciales de la Corte Internacional de Justicia en temas de responsabilidad internacional de un Estado.
3. Exponer el desarrollo doctrinario sobre la regulación de ciberataques en Derecho Internacional.
4. Determinar la aplicación de la normativa internacional existente en la determinación de la responsabilidad de un Estado por ciberataques en tiempos de paz.

IV. Marco teórico

Los conceptos de la responsabilidad internacional han sido desarrollados en el trabajo de la CID, en los Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (AREHII) y su consecuente desarrollo en la jurisprudencia de la CIJ y otros tribunales internacionales.

En el Capítulo I sobre "Principios Generales" de los AREHII, el Artículo 1 indica que *"todo hecho internacionalmente ilícito del Estado genera su responsabilidad internacional"*[89].

Asimismo el Artículo 2 "Elementos del hecho internacionalmente ilícito del Estado" indica que: *"Hay hecho internacionalmente ilícito del Estado cuando un comportamiento consistente en una acción u omisión: a) Es atribuible al Estado según el Derecho Internacional; y, b) Constituye una violación de una obligación internacional del Estado"*[90].

Mediante laudos y sentencias en distintas instancias en el Derecho Internacional, los conceptos de la responsabilidad de los Estados por el incumplimiento de una obligación internacional y su correspondiente derecho a la reparación, han sido desarrollados y aplicados a casos de disputas entre Estados, de tal forma que así se convierten en costumbre internacional.

En el Laudo Arbitral en el *Caso de Reclamos Británicos en la Zona Española de Marruecos*, el Juez Huber indicó: *"responsibility is the necessary corollary of a right. All rights of an international character involve international responsibility. If the obligation in question is not met, responsibility entails the duty to make reparations"*[91].

---

[89] AREHII, Art.1.
[90] AREHII, Art. 2.
[91] James Crawford, *Brownlie's Principles*, 541. *"La responsabilidad es el corolario necesario de un derecho. Todos los derechos de carácter internacional involucran la responsabilidad internacional. Si la obligación en cuestión no es satisfecha, la responsabilidad implica el deber de reparación",* traducción realizada por las autoras.

En el Caso de *Fábrica de Chórzow (Alemania vs. Polonia), (Competencia)*, la Corte Permanente de Justicia Internacional indicó:

> *It is a principle of international law that the breach of an engagement involves an obligation to make reparation in an adequate form. Reparation therefore is the indispensable complement of a failure to apply a convention and there is no necessity for this to be stated in the convention itself*[92].

Lo anterior nuevamente se indicó con énfasis en la resolución sobre Indemnización de *Fábrica en Chorzów*, donde se señaló:

> *[…] it is a principle of international law, and even a general conception of law, that any breach of an engagement involves an obligation to make reparation. […] the Court has already said that reparation is the indispensable complement of a failure to apply a convention, and there is no necessity for this to be stated in the convention itself.*[93]

Asimismo, en el caso del *Canal de Corfu (Reino Unido v. Albania) (Corfu)* la CIJ indicó que dicha responsabilidad, la cual se le atribuyó a Albania, se derivó de su falta de avisar sobre el peligro existente, lo cual lo hace responsable de las minas localizadas en sus aguas territoriales aún y cuando no las había colocado[94].

En el caso de *Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro) (Genocidio),* la Corte consideró si las violaciones a la "Convención para la Prevención y la Sanción del Delito de Genocidio" derivan consecuencias particulares al estado en violación: *"The Court observes that the obligation in question in this case, arising from the terms of*

---

[92] CPJI, *Fábrica en Chorzów,* Ser A No *9,* 21. "*Es un principio del Derecho Internacional que un incumplimiento de un deber involucra una obligación para hacer reparaciones de una manera adecuada. Reparación es entonces el complemento indispensable de la falta de aplicación de una convención y no hay necesidad de que esto esté indicado en el propio convenio".* Traducción realizada por las autoras.

[93] CPJI, *Fábrica en Chorzów,* Ser A No 17, 29 *"[…] es un principio de Derecho Internacional, e incluso un concepto general de derecho, que cualquier incumplimiento de un deber involucra la obligación de hacer reparaciones […] la Corte ya ha dicho que las reparaciones son el complemento indispensable de la falta de aplicación de una convención, y no hay necesidad de que esté indicado en el propio convenio".* Traducción realizada por las autoras.

[94] *Corfu,* 4 y 23.

the Convention, and the responsibilities of States that would arise from breach of such obligations, are obligations and responsibilities under international law. They are not of a criminal nature"[95].

Dichos pronunciamientos demuestran que no hay una dicotomía contrato/delito y, mucho menos, entre delitos y crímenes internacionales de los Estados. Por el contrario, surge un único e indiferenciado concepto de responsabilidad, cuyo elemento principal es el incumplimiento de una obligación del Estado por una persona o entidad cuya conducta sea, en esas circunstancias, atribuible a un Estado, sin perjuicio de cualquier responsabilidad que pueda derivar de un delito internacional atribuible a un individuo.

El artículo 12 de los AREHII establece que: *"Hay violación de una obligación internacional por un Estado cuando un hecho de ese Estado no está en conformidad con lo que le exige esa obligación, sea cual fuere el origen o a la naturaleza de esa obligación"*[96].

A pesar de que el artículo 2, indica que la violación por un Estado de una obligación internacional genera su responsabilidad, el mismo no revela qué se debe comprender por una violación a una obligación. El artículo 12 viene entonces a definir, en los términos más generales posibles, qué constituye un incumplimiento. A pesar de que en el mismo Capítulo III de los AREHII, se indican otras condiciones a ser consideradas para establecer dicho incumplimiento. El determinar si hubo o no una violación a una obligación, dependerá de los precisos términos de esa obligación, su interpretación y aplicación, tomando en cuenta su objeto y propósito y los hechos del caso.

La disconformidad entre la conducta requerida por el Derecho Internacional y los hechos del caso, se ha reflejado de diferentes formas en la jurisprudencia de la CIJ, al usar expresiones tales como *"incompatibilidad con la obligación"*[97], *"actos contrarios a"*[98],

[95] Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro), Reportes CIJ 2007, 43, para. 115 y 170. *"La Corte observa que la obligación en cuestión en el presente caso, derivado de los términos de la Convención, y la responsabilidad de los Estados que se derive de un incumplimiento, son obligaciones bajo el Derecho Internacional. No son de naturaleza penal",* traducción realizada por las autoras.
[96] AREHII, art. 12.
[97] *Agentes Diplomático y Consulares Estadounidenses en Teherán (Estados Unidos v. Irán),* Sentencia, Reportes CIJ, 1980, p. 3, para. 56.
[98] *Nicaragua,* Juzgamiento, para. 115.

"inconsistentes con"[99] una regla determinada, o *"incumplimiento de sus obligaciones contractuales"*[100].

La expresión *"no conforme con lo que es requerido de él por la obligación"* es la más apropiada para indicar que constituye la esencia de una violación de una obligación internacional por un Estado. Permite la posibilidad de que dicha violación exista, incluso cuando la actuación de un Estado es solo en parte contraria a la obligación internacional. El Estado puede verse obligado a actuar de cierta manera y, en otros casos, la obligación determina un mínimo de estándares bajo los cuales los Estados deben actuar. Dicha conducta puede incluir un acto o una omisión o incluso una combinación de ambos. La frase *"no de conformidad con"* es lo suficientemente flexible para cubrir las diferentes formas en las cuales una obligación puede expresarse, al igual que las muchas formas en que se puede quebrantar.

En el caso de *Agentes Diplomático y Consulares Estadounidenses en Teherán (Estados Unidos v. Irán)*, la CIJ estableció su trabajo de la siguiente manera: *"First, it must determine how far, legally, the acts in question may be regarded as imputable to the Iranian State. Secondly, it must consider their compatibility or incompatibility with the obligations of Iran under treaties in force or under any other rules of international law that may be applicable"*[101].

Por todo lo anterior, los dos elementos a los cuales se refiere el artículo 2 de AREHII, reflejan posiciones constantes a lo largo de la jurisprudencia. A continuación, se efectuará una breve referencia a ambos elementos y su importancia en la determinación de responsabilidad a un Estado.

El primer elemento, con referencia a la atribución del Estado, se constituye con base en la acción u omisión de uno o más agentes y órganos del Estado. Debe existir una

[99] Ídem, para. 186
[100] *Gabcikovo*, para. 57.
[101] *Agentes Diplomático y Consulares Estadounidenses en Teherán (Estados Unidos v. Irán)*, Sentencia, Reportes CIJ, 1980, p. 3, para. 56. *"Primero, debe determinar qué tan lejos, legalmente, los actos en cuestión pueden ser considerados como imputables al Estado de Irán. Segundo, debe considerar su compatibilidad o incompatibilidad con las obligaciones de Irán bajo tratados vigentes o bajo cualquier otra relación de Derecho Internacional que pueda ser aplicable al caso",* traducción realizada por las autoras.

relación causal entre las actuaciones del Estado y el daño causado. En este sentido, no es un requisito indispensable que un agente del Estado sea directamente quien lleve a cabo el acto ilegal. En el caso de *Corfu* la CIJ determinó que Albania era responsable por las consecuencias de las minas colocadas en sus aguas territoriales, en vista del conocimiento de las autoridades y su falta de advertencia de la presencia de las minas.

Según la obligación, la falta de asegurar el cumplimiento de la misma puede atribuírsele a un Estado, aun cuando la conducta provenga de un ente privado. Tal es el caso entre la Organización Mundial de Comercio ("OMC"), en el caso de las lecheras. En este caso, el Órgano de Apelaciones de la OMC observó que:

> *[...] irrespective of the role of private parties [...] the obligations [...] remain obligations imposed on Canada [...] The question is no whether one or more individual milk producers, efficient or not, are selling CEM at a price above or below their individual costs of production. The issue is whether Canada, on a national basis, has respected its WTO obligations*[102].

Las reglas de atribución varían según el caso y no se limita entonces únicamente a agentes del Estado como lo determina el artículo 4 de AREHII[103], sino que se han desarrollado y aplicado teorías de atribución con respecto a fuerzas armadas, gobiernos federales frente al gobierno central, el poder legislativo y judicial dentro de un Estado, actos *ultra vires*, revoluciones e insurrecciones, e incluso, en casos de responsabilidad conjunta o complicidad.

El segundo elemento se refiere a la violación de una obligación internacional. En dichas violaciones autores han determinado diferentes teorías al respecto. Crawford, al citar a Oppenheim, determina una diferencia entre una obligación originaria y una indirecta.[104]

---

[102] *Canadá – Measures Affecting the Importation of Milk and the Exportation of Dairy Products,* WTO Doc WT/DS103/AB/RW2, 20 de diciembre de 2002, para. 95 y 96. *"[...] independientemente del papel de las entidades privadas [...] la obligación [...] impuesta a Canadá [...] La pregunta no es si uno o más productores individuales de leche, eficientes o no, están vendiendo leche para la importación comercial (CEM por sus siglas en inglés 'commercial export milk"), a un precio por encima o por debajo de su costo individual de producción. La cuestión es si Canadá a nivel nacional, ha respetado sus obligaciones en la OMC",* traducción realizada por las autoras.

[103] AREHII, art. 4.

[104] James Crawford, *op. cit.* 556.

La responsabilidad objetiva recae en la doctrina del acto voluntario, en el cual se puede establecer una relación causal. La práctica de los Estados y la jurisprudencia de la CIJ y tribunales arbitrales han seguido la teoría de responsabilidad objetiva como un principio general, el cual puede ser modificado o excluido según sea el caso[105].

A pesar de que la responsabilidad objetiva puede llegar a considerarse un principio general, excepciones a dicha responsabilidad se ven ejemplificadas en el caso de *Canal de Corfu*. La CIJ discurrió si, por medio de prueba indirecta, evidencia al conocimiento de Albania de la existencia de las minas en sus aguas territoriales independientemente de su participación. La CIJ concluyó que la colocación de las minas no hubiera podido ocurrir sin el conocimiento del Gobierno de Albania e hizo referencia específica a la obligación de los Estados a no permitir en forma consciente el uso de su territorio para ser utilizado en actos contrarios a los derechos de otros Estados[106].

El motivo y la intención con frecuencia son elementos utilizados en la determinación de una conducta. El principio de responsabilidad objetiva indica que la intención de causar un daño como circunstancia para establecer responsabilidad es irrelevante, a pesar de que puede ser considerado en establecer la violación a la obligación. [107] Por tanto, no se hace referencia a la responsabilidad objetiva o subjetiva, simplemente hay "responsabilidad"[108].

Las disputas entre Estados tienen la particularidad de que resisten la aplicación de las reglas generales. Mucho depende de la asignación de la carga de la prueba, la regulación de la prueba, aquiescencia, "estoppel", los términos del *Compromis* entre los Estados y el contenido de las reglas sustantivas o tratados aplicables.

De igual forma se han establecido reglas por reparaciones como consecuencia de actos que no sean ilegales en el sentido de estar prohibidas en forma expresa. Responsabilidad por actos no prohibidos en el Derecho Internacional ha adquirido

[105] Ídem, 556.
[106] *Corfu*, 18 y 22.
[107] James Crawford, *op. cit.* 559.
[108] Crawford, James. *State Responsibility: The General Part*. New York, Estados Unidos: Cambridge University Press, 2013, 61.

relevancia en el campo del derecho ambiental internacional, cuando actividades económicas legales producen contaminación y otras consecuencias que transcienden las fronteras de un Estado. En *Trail Smelter,* un fundidor ubicado en Canadá, estaba produciendo aire contaminado el cual afectaba a los Estados Unidos de América. El Tribunal Arbitral concluyó en Derecho Internacional que Canadá era responsable por el daño, independientemente de la ilegalidad de la actividad misma. Por analogías de leyes domésticas, el Tribunal indicó lo siguiente:

> *[…] that, under the principles of international law, as well as of the law of the United States, 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.*[109]

En estos casos, se puede hacer referencia a la obligación de debida diligencia. El hecho que una actividad por sí misma no esté prohibida en el Derecho Internacional, no excluye que el daño causado por falta de criterio o mala gestión en llevar a cabo una actividad implique responsabilidad.[110]

A pesar de que Cortes y Tribunales internacionales han venido desarrollando teorías y principios y, por tanto, construyen costumbre internacional, las tecnologías y las nuevas herramientas disponibles han presentado una discusión en temas de responsabilidad internacional en temas de ciberataques.

El único desarrollo en este tema, se ha dado a nivel doctrinal entre autores reconocidos y expertos en Derecho Internacional, tecnologías de la información y ciberataques.

---

[109] Recopilación de Laudos Arbitrales. *Caso Trail smelter* (Estados Unidos v. Canadá). 16 de Abril de 1938 y el 11 de marzo de 1941. VOLUME III pp. 1905-1982, 1965. "*que, bajo los principios del Derecho Internacional, al igual que bajo las leyes de los Estados Unidos, ningún estado tiene el derecho de usar o permitir el uso de su territorio de manera en que cause daño por sus humos dentro o hacia el territorio de otro o sus propiedades o personas, cuando el caso es de serias consecuencias y el daño es claramente establecido con prueba convincente"*, traducción realizada por las autoras.
[110] James Crawford, *op. cit.* 561.

En consecuencia, la presente investigación pretende determinar la aplicación de las actuales herramientas en el Derecho Internacional en ciberataques fuera del contexto de un conflicto armado. La falta de regulación y el rápido desarrollo de las tecnologías, al igual que la cada vez más común utilización de herramientas tecnológicas en las interacciones entre Estados, requiere de un abordaje comprensivo de las posibilidades que existen para regular este tema y la no regulación, o falta de codificación, no permita que se lleven a cabo actos contrarios al Derecho Internacional.

V. Marco metodológico

El presente trabajo de investigación se basa en una metodología descriptiva analítica, la cual se apoya en los siguientes métodos de trabajo:

A. Análisis doctrinario

Primeramente, se hará un análisis doctrinario para determinar lo que han aportado los autores más reconocidos en la materia. Lo anterior con el fin de tener un panorama claro de qué es el Derecho Internacional público y la responsabilidad internacional de los Estados. Las fuentes que se utilizarán para este análisis serán libros, revistas, artículos, así como material de apoyo de fuentes confiables de Internet.

B. Análisis legal

Dada la falta de regulación a nivel internacional en cuestiones de ciberataques, el análisis legal será realizado de conformidad con las fuentes establecidas en el artículo 38 inciso primero del Estatuto de la Corte Internacional de Justicia, y las otras fuentes analizadas en la introducción del presente trabajo.

C. Análisis deductivo

Finalmente, se utilizará el análisis deductivo para establecer las posibles aplicaciones de las fuentes existentes del Derecho Internacional Público, en la regulación de la responsabilidad internacional de los Estados en relación con los ciberataques.

VI. Contenido

Capítulo I

La responsabilidad internacional de los Estados por ciberataques

Sección I: antecedentes de responsabilidad internacional de los Estados

La responsabilidad de los sujetos por incumplimiento a sus obligaciones debe contemplarse en cualquier sistema de Derecho. Dicho esquema aplica tanto para los individuos como para los Estados. A pesar de que el derecho ha establecido parámetros de responsabilidad para individuos, por mucho tiempo la responsabilidad de los Estados no fue un punto central de estudio y solo se desarrolló incidentalmente por la doctrina. El principal interés era identificar reglas específicas y prácticas asociadas en distintos campos del derecho y, en ocasiones, identificar el mecanismo por el cual los Estados pudieran vindicar sus derechos, en especial respecto a represalias y la guerra.

En general, el desarrollo doctrinario del concepto de responsabilidad internacional de los Estados y su aplicación, no fue elaborado de manera sistemática y no fue sino hasta el siglo diecinueve donde de manera más concreta resultó objeto de estudio.

A pesar del trabajo de distintos juristas, no es hasta que se concretaron distintos esfuerzos como la Conferencia de Codificación de La Haya de 1930, las Investigaciones Preliminares de la Universidad de Harvard de 1929 y 1961, cuando se establecieron las bases en las cuales se fundamentó la Comisión de Derecho Internacional para concretar un verdadero esfuerzo en la codificación de la responsabilidad internacional de los Estados.

i. El trabajo de la Comisión de Derecho Internacional

La Asamblea General de las Naciones Unidas en 1948, estableció la Comisión de Derecho Internacional, la cual en su primer período de sesiones en 1949, colocó la responsabilidad del Estado como uno de los primeros catorce temas a ser tratados[111].

[111] James Crawford, "Proyecto de Artículos sobre la Responsabilidad del Estado", *United Nations Audiovisual Library of International Law*, (2009), consultado el 28 de junio de 2016, http://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_ph_s.pdf.

El primer Relator Especial sobre el tema, fue García Amador de Cuba, quien comenzó su labor en 1956, quien presentó seis informes entre ese año y 1961 y centró la labor de la CDI en la responsabilidad del Estado por daños causados a la persona o bienes de los extranjeros; mientras abordaba también los aspectos generales de la responsabilidad. Estos informes estaban muy influenciados por el trabajo que había realizado la Universidad de Harvard. Debido a otras labores a las cuales se dedicaba adicionalmente, como temas de protección diplomática, la CDI no examinó sus informes en detalle[112].

Para 1962 la idea de que la Comisión debía centrar sus esfuerzos en *"la definición de las normas generales de la responsabilidad internacional del Estado"*, según como propuso R. Ago, había ganado apoyo. El Profesor Ago (Italia), en su calidad de segundo Relator Especial sobre el tema, entre 1969 y 1980, presentó ocho informes junto con un sustancial documento adicional. Durante ese período, la CDI aprobó 35 artículos, que constituyen la base de los actuales AREHII [113].

El tercer Relator Especial nombrado en 1979, William Riphagen de los Países Bajos, presentó siete informes entre 1980 y 1986 y su principal aporte fue lograr la aprobación provisional de una definición de "Estado lesionado".

Riphagen fue sucedido en 1988 por G. Arangio Ruiz de Italia, después del retiro de Riphagen en 1987 y cuando este concluyó su labor en la Comisión, la cual llevó a cabo entre 1988 y 1996 (trabajo que quedó plasmado en la presentación de ocho informes), la CDI aprobó un primer texto integral del proyecto de artículos con comentarios. El principal aporte de Arangio fueron los artículos sobre reparación, contramedidas, consecuencias del "crimen internacional" y solución de controversias[114].

En 1997 la CDI nombró Relator Especial a James Crawford de Australia, quien entre 1998 y 2001 realizó una segunda lectura del proyecto de artículos. En este mismo período, la CDI examinó de nuevo la totalidad del texto y aprobó un nuevo proyecto de

[112] James Crawford, *State Responsibility: The General Part*, 36.
[113] James Crawford, "Proyecto de Artículos sobre la Responsabilidad del Estado".
[114] Ídem

artículos que fue presentado a los gobiernos para que formularan sus respectivos comentarios al proyecto propuesto. Finalmente, en su 53° período de sesiones de 2001, la CDI aprobó la versión definitiva de los artículos con 59 numerales y, en ese mismo período, se elaboró un comentario al proyecto de artículos aprobado[115].

ii. Resoluciones de la Asamblea General de las Naciones Unidas

Posteriormente, mediante su resolución 56/83 de 12 de diciembre de 2001, la Asamblea General tomó nota de los artículos y llamó la atención de los gobiernos, sin perjuicio de la materia de su futura aprobación como texto de un tratado u otro tipo de medida, según correspondiera y adjuntó el texto de los artículos como anexo de la mencionada resolución[116].

La Asamblea General de Naciones Unidas llamó la atención de los Estados sobre el mismo tema posteriormente en distintas resoluciones, entre ellas la 59/35 de 2 de diciembre de 2004, la 62/61 de 6 de diciembre de 2007 y en la resolución 65/19 de 6 de diciembre de 2010. En realidad, los Artículos han sido aprobados y aplicados en forma amplia en la práctica, incluso por la Corte[117].

iii. Jurisprudencia de la Corte Internacional de Justicia

Debemos hacer referencia a algunos precedentes de la Corte Internacional de Justicia que resultarían aplicables. En el caso de la Opinión Consultiva sobre *La Legalidad de la Amenaza o Uso de Armas Nucleares*, la Corte estableció:

> These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly

[115] James Crawford, *State Responsibility: The General Part*, 39-42.
[116] Asamblea General de Naciones Unidas, Responsabilidad del Estado por hechos internacionalmente ilícitos, Resolución No. 56/83, (28 de enero de 2002).
[117] James Crawford, "Proyecto de Artículos Sobre la Responsabilidad del Estado", 2009, consultado el 28 de junio, 2016, United Nations Audiovisual Library of International Law, http://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_ph_s.pdf

prohibits, nor permits, the use of any specific weapon, including nuclear weapons[118].

De lo dicho por la Corte entonces se comprende que la prohibición del uso de la fuerza y las disposiciones establecidas en la Carta de Naciones Unidas, se aplican a cualquier tipo de arma; pues no hay prohibición expresa para un tipo de arma en específico, lo cual resulta aplicable a los ciberataques en el entendido de que puede ser considerada un tipo de arma y ser utilizada en contra de los principios establecidos en la Carta de las Naciones Unidas.

Por otro lado, se tiene el caso de *Nicaragua*, en el cual la Corte estableció:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. As noted above (paragraph 191). General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting State when the acts committed in another State "involve a threat or use of force". These forms of action are therefore wrongful in the light of both the principle of non-use of force, and that of non-intervention[119].

---

[118] *Legalidad de la Amenaza o Uso de Armas Nucleares,* Opinión Consultiva, I.C.J. Reportes 1996, para. 39, 226. *"Estas provisiones no hacen referencia a armas específicas. Ellas aplican a cualquier uso de la fuerza, sin importar el arma empleada. La Carta ni prohíbe, ni permite, el uso de cualquier arma específica, incluyendo las armas nucleares",* traducción hecha por las autoras.

[119] *Nicaragua*, Sentencia, 98. *"Una intervención prohibida debe ser una en la cual exista incidencia en asuntos en los que se permite a cada Estado, por el principio de soberanía de los Estados, a decidir libremente. Una de ellas es la elección de un sistema político, económico, social y cultural, y la formulación de la política exterior. La intervención es ilícita cuando se utilizan métodos de coacción con respecto a este tipo de posibilidades, que deben permanecer libres de incidencia. El elemento de coacción, que define, y que*

De lo antes señalado por la Corte, resulta aplicable al tema que atañe a este trabajo, que la intervención de un Estado en los asuntos de otro está prohibida, en virtud del principio de soberanía del Estado a decidir libremente y cualquier tipo de intervención, ya sea directa (interviniendo directamente en las hostilidades) o indirecta (apoyando con medios para la comisión de los hechos) constituyen medios de coerción que van en contra de los principios de no uso de la fuerza y no intervención. Este precedente sienta las bases para los tipos de responsabilidad que puede generar un ciberataque.

Sección II: naturaleza de un ciberataque y su tratamiento en el Derecho Internacional

i. Funcionamiento del Internet y naturaleza de un ciberataque

a) ¿Cómo funciona el internet?

Previo a entrar al análisis de la naturaleza de un ciberataque para su posible atribución, resulta necesario tener un conocimiento general sobre cómo funciona el internet. El experto W. Earl Boebert[120] explica que el Internet es una red de conmutación de paquetes y está compuesta de una malla de computadoras especializadas llamadas enrutadores o "*routers*". En forma simplificada, dicha red consta de nodos interconectados, cada uno de los cuales recibe un número llamado dirección IP. Las unidades de datos a transmitir, que se generan cuando se hace una solicitud en el buscador de una página web, se cortan en pedazos o paquetes. A modo de analogía puede verse estos paquetes como una postal en una carta de correo; pues a menos de que los datos estén cifrados, también es visible a medida que el paquete se mueve a través del Internet[121].

---

forma parte la esencia misma de, la intervención prohibida, es particularmente evidente en el caso de una intervención que utiliza la fuerza, ya sea en forma directa de la acción militar, o en la forma indirecta de apoyo a actividades armadas subversivas o terroristas dentro de otro Estado. Como se señaló anteriormente (párrafo 191). La resolución 2625 (XXV) de la Asamblea General equivale a ayuda de este tipo con el uso de la fuerza por parte del Estado que presta asistencia, cuando los actos cometidos en otro Estado "implican una amenaza o uso de la fuerza". Estas formas de acción son, por tanto, ilícitas a la luz tanto de los principios de no uso de la fuerza, y de no intervención", traducción hecha por las autoras.

[120] W. Earl Boebert, "A Survey of Challenges in Attibution", *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy,* (Washington, D.C., Estados Unidos: The National Academies Press, 2010), 40-42.

[121] David D. Clark y Susan Landau, "Untangling Attribution", Harvard Law School National Security Journal, Vol. 2, (2016): 4, consultado el 4 de febrero de 2017, http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf.

A cada paquete se le da un encabezado que contiene la dirección IP de origen y destino de la transmisión y otra información de control. Los paquetes se envían a los enrutadores, los cuales proporcionan un "enrutador siguiente razonable" para cualquier dirección IP dada. Esto libera a los *routers* de tener que conocer todas las rutas posibles a todos los destinos posibles; pues es importante tener en consideración que el internet está hecho para transmitir la mayor cantidad de datos por la vía más rápida y, si existe alguna dificultad, buscar medios alternos para el paso de la información.

El autor mencionado, ofrece un ejemplo geográfico para explicar este proceso; considérese un enrutador en Albuquerque que desea enviar un elemento de datos a Nueva York. El elemento se cortará en paquetes cuya dirección IP de origen designará Albuquerque y la dirección IP de destino designará Nueva York. Para iniciar la transmisión, el enrutador en Albuquerque solo necesita conocer la dirección IP de algún enrutador intermedio en la dirección general, por ejemplo: Ciudad de Kansas. A su vez, ese enrutador solo necesita saber que San Luis está "en camino" y así sucesivamente, "salto" por "salto", hasta que se alcance el destino. Finalmente, el paquete se une con otros para reconstituir el elemento de datos.

El escritor Boebert explica que la asignación dinámica de rutas en cada salto es lo que da a las redes de conmutación de paquetes su gran resistencia al fallo[122].

Asimismo, el experto W. Earl Boebert explica que, al principio del surgimiento de las redes de conmutación de paquetes, se evidenció que las direcciones IP numéricas eran difíciles de manejar para los seres humanos y se desarrolló una segunda instalación denominada Sistema de Nombres de Dominio o DNS, para permitir el uso de los nombres de dominio simbólicos con los cuales había familiaridad. El DNS es un sistema de búsqueda distribuida que, cuando se consulta, convierte un nombre simbólico para un nodo, denominado "*hostname*", a una dirección IP numérica[123].

[122] W. Earl Boebert, *op. cit*. 42.
[123] Íbid.

b) Naturaleza de un ciberataque y sus tipos

Los ciberataques se cometen cuando se saca provecho de las deficiencias de cada sistema. Esas vulnerabilidades se llaman "*cero day*" cuando aún no han sido publicadas y reciben el nombre de "vulnerabilidades" cuando son descubiertas al público. Ahora bien, el hecho de aprovecharse de las vulnerabilidades es solo la mitad de los elementos que hacen peligroso un ciberataque; pues el otro es el medio por el cual son cometidos.

En 1969 el ejército de los Estados Unidos diseñó el internet por medio del proyecto ARPANET (*Advanced Research Project Agency Net*), cuyo objetivo era crear un simple sistema de comunicaciones, para su funcionamiento en caso de ataque enemigo. Se trataba de una red en donde los ordenadores conectados a ella disponían de diversas rutas por las cuales alternaban las comunicaciones, con el fin de que las mismas continuaran funcionando, aunque alguna de ellas fuera destruida como consecuencia de algún ataque.

Con estas bases, el internet solo ha ido evolucionando y haciéndose más sofisticado, pero como se puede apreciar, desde sus inicios se le dio un poder y un potencial exacerbado a los ciberataques; pues el internet fue diseñado para encontrar una ruta que lleve la información, o en este caso los datos maliciosos de un ciberataque, a su destino final, aún y cuando una o varias de las rutas sean destruidas.

Con la difusión que hay en la actualidad del internet por el mundo, frenar un ciberataque resulta muy complicado y, de acuerdo con la naturaleza prácticamente imposible, pues no se pueden eliminar todos los medios existentes para que los datos no

lleguen al sistema que está siendo atacado. Por este motivo, deben buscarse opciones paralelas que protejan los sistemas[124].

Asimismo, cabe recordar lo anteriormente mencionado, respecto de que en la actualidad no existe una noción clara de lo que es considerado un ciberataque. No obstante, los autores David D. Clark y Susan Landau distinguen entre ciberataques y ciberexplotaciones, los autores explican que ambos tipos de ataques tienen en común que se aprovechan de una vulnerabilidad del software para tener acceso a él y utilizarlo para lograr sus objetivos. La diferencia es que los ataques cibernéticos están dirigidos a interrumpir, alterar o destruir el anfitrión (o algún sistema cibernético o físico asociado); mientras la ciberexplotación está dirigida a obtener información y utilizarla, no a causar interrupción, alteración o destrucción del sistema[125], como se da por ejemplo en el robo de identidad digital o el espionaje digital.

Ahora bien, bajo esta distinción, se puede indicar que hay dos tipos de ciberataques. El más importante de ellos, se conoce como DDoS, por ser las iniciales en inglés de *Distributed Denial of Service* y significa distribución de denegación de servicio. Estos ataques surgen cuando un gran número de máquinas, cientos o miles, en un solo lugar o en todo el mundo, atacan un sitio Web afectando el DNS de la página, lo cual significa que afecta el Sistema de Nombres de Dominio de Internet, base principal que genera los paquetes de información necesarios para que el usuario reciba la información que solicita. Todas estas máquinas juntas crean lo que se conoce como el Bot-Net, en otras palabras, una red de computadores coordinados para atacar un servidor específico y hacerlo colapsar, lo que genera la interrupción del servicio, fin último de este tipo de ciberataques[126].

Un ejemplo de esta categoría, se halla cuando se observan los ataques que se dieron el 21 de octubre de 2016. Durante once horas, el proveedor de Internet Dyn vio irrumpido

[124] Ángel L. Rubio Moraga, "Historia e Internet: Aproximación al Futuro de la Labor Investigadora", Departamento de Historia de la Comunicación, Facultad de Ciencias de la Información, Universidad Complutense de Madrid, consultado el 9 de febrero de 2017, http://pendientedemigracion.ucm.es/info/hcs/angel/articulos/historiaeinternet.pdf.
[125] David D. Clark y Susan Landau, *op. cit.* 6.
[126] Ídem, 7.

su servicio a grandes compañías y medios de comunicación internacionales, tales como Twitter, Spotify, Amazon, Reddit, Tumblr, Paypal, Netflix, The New York Times, Financial Times y CNN, lo cual aseguran afectó a más de mil millones de clientes en todo el mundo[127].

También se observan aquellos conocidos como los DoS o denegación de servicio, los cuales se producen cuando un gran número de solicitudes se dirigen a una URL de destino y, al igual que en el DDoS, las solicitudes se producen tan rápidamente que el servidor Web no puede responder y el sitio se vuelve inaccesible. La diferencia entre ambos es que el DoS lo produce un solo atacante y el DDoS lo cometen cientos o miles de computadoras atacantes. Este tipo de ataques son poco comunes cuando se habla de ataques a gran escala, pues son más fáciles de identificar y atribuir; pues son constantes y de una sola fuente.

El caso que ejemplifica los dos tipos de denegación de servicios mencionados, es el que impulsó todo un movimiento a nivel internacional en el estudio de los ciberataques por parte de los abogados internacionalistas y expertos en la materia, los ataques de 2007 en Tallin, Estonia.

Según como explican los expertos Eneken, Kadri y Liis, el tamaño reducido de la población (1,3 millones de habitantes), los recursos limitados y la baja densidad poblacional han desafiado a Estonia a buscar medios eficientes para prestar servicios públicos a sus residentes sin que se requieran recursos excesivos del Estado. Por este motivo, desde mediados de los 90, se han usado los medios digitales para brindarle muchos servicios a la población del lugar. Propiamente a partir de 1992, con la creación y el desarrollo del registro nacional de la población, en Estonia se comenzó la era de las bases de datos digitales gubernamentales y los sistemas de información del Estado. En el 2007,

[127] Beatriz Guillén, Joan Faus y Rosa Jiménez Cano, "Varios ciberataques masivos inutilizan las webs de grandes compañías", El País, Tecnología, 22 de octubre de 2016, Madrid, Washington, San Francisco, versión en línea, consultado el 9 de febrero de 2017, http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html. Esther Mucientes, "Así se gestó el ataque más grave de los últimos 10 años", El Mundo, Tecnología, 22 de octubre de 2016, Madrid, versión en línea, consultado el 9 de febrero de 2017, http://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html.

cuando Tallin fue atacado, los sistemas de información estatales y las bases de datos se habían convertido en un sistema estatal de información con la necesaria infraestructura funcional, la cual permitía el acceso a los servicios por medios electrónicos[128].

Los ataques tuvieron dos fases distintas, cada una consistente en varias ondas de intensidad elevada. La primera fase tuvo lugar del 27 al 29 de abril de 2007 y se estimó que había sido motivada por la decisión del Estado de eliminar un monumento de la Segunda Guerra Mundial, lo cual generó revueltas en la población; pues los ataques eran relativamente sencillos y se trataron de ataques DoS. La segunda fase fue la principal y más coordinada del ataque, la cual duró del 30 de abril al 18 de mayo y se describe como una operación mucho más sofisticada, donde se observó la coordinación de un profesional en la materia. En particular, se observó una clara correlación entre las fechas políticamente significativas de Estonia en la época y la intensificación de los ataques, pues los segundos correspondían a ataques DDoS[129].

ii. Desarrollo de los ciberataques a nivel internacional

En el Derecho Internacional, muchos autores han efectuado publicaciones donde hacen alusión al novedoso tema de ciberataques. No obstante, los dos esfuerzos más importantes que se han realizado a nivel doctrinario son los que corresponden a los Manuales de Tallinn, los cuales fueron el resultado de los movimientos que generaron los ataques del 2007, como fue explicado anteriormente. Estos dos Manuales los redactó un grupo de expertos, auspiciados por el Centro Cooperativo de Excelencia en Ciberdefensa (CCD COE por sus siglas en inglés). Dicha institución fue activada como Organización Militar Internacional (OMI) por la decisión del Consejo del Atlántico Norte y se convirtió en la primera OMI alojada por Estonia.

[128] Eneken Tikk, Kadri Kaska y Liis Vihul, International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCD COE), (2010), consultado el 9 de febrero de 2017, https://ccdcoe.org/publications/books/legalconsiderations.pdf.
[129] Íbid.

El Centro Cooperativo de Excelencia en Ciberdefensa es una organización militar internacional acreditada por la Organización del Tratado Atlántico Norte (OTAN), con el objetivo de mejorar las capacidades cooperativas de defensa cibernética de la OTAN y sus naciones, con el fin de mejorar así la interoperabilidad de la Alianza en el campo de la ciberseguridad cooperativa. El centro lo establecieron siete naciones: Estonia, Alemania, Italia, Lituania, Letonia, República Eslovaca y España, que firmaron el Memorando de Entendimiento el 14 de mayo de 2008[130].

Los Manuales de Tallinn estuvieron a cargo del profesor Michael Schmitt, miembro del Centro de la Escuela Superior de Guerra Naval de los Estados Unidos y la Universidad de Exeter. Y desde su creación, se dejó constancia que lo escrito en los mencionados manuales, representa solo las opiniones de sus autores y no de la OTAN, el COE de la CCD de la OTAN, sus patrocinadores o cualquier otro Estado u organización.

a. Manual de Tallinn sobre el Derecho Internacional Aplicable a la Guerra Cibernética

La importancia del Manual de Tallinn corresponde al primer intento de los expertos de recopilar en un solo documento regulación de Derecho Internacional y aplicarla a temas de ciberataques en tiempos de guerra, sin mencionar el hecho de que es el primer estudio formal de la materia y quizá el aporte doctrinario más extenso y profundo con el cual se cuenta actualmente en temas de regulación de ciberataques en tiempos de guerra a nivel internacional.

Las consecuencias de utilizar armas nuevas no reguladas, como lo pueden ser ciertas operaciones cibernéticas, resultan devastadoras, un claro ejemplo de esto dejó las bombas nucleares que fueron lanzadas a finales de la segunda guerra mundial. En ocasiones, las leyes internacionales no logran alcanzar con la suficiente rapidez el desarrollo tecnológico

[130] NATO Cooperative Cyber Defense Center of Excelence, *Centre is the first International Military Organization hosted by Estonia*, página oficial de NATO CCDCOE, (2008), consultada el 5 de febrero de 2017, https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html.

empleado en las armas; por lo tanto, esfuerzos como el realizado por los expertos del Manual de Tallinn tienen particular relevancia.

En este sentido, el Comité Internacional de la Cruz Roja (CICR) se pronunció de la siguiente manera:

> […] es crucial identificar cauces para limitar el coste humanitario de las operaciones cibernéticas y, en particular, para reafirmar la pertinencia del DIH [Derecho Internacional Humanitario] cuando se usa esta nueva tecnología en conflictos armados. Eso es exactamente lo que aseveran los expertos en el Manual Tallinn. Los medios y métodos de hacer la guerra evolucionan con el paso del tiempo y es palmario que no se asemejan a los que existían cuando se redactaron los Convenios de Ginebra en 1949; no obstante, el DIH sigue siendo aplicable en todas las actividades que las partes conducen durante un conflicto armado, y se debe respetar. No se puede descartar, sin embargo, que quizás sea necesario continuar desarrollando el derecho a fin de que brinde suficiente protección a la población civil, a medida que evolucionan las tecnologías cibernéticas o se comprenden mejor sus consecuencias humanitarias[131].

Como bien fue mencionado por el CICR, existen armas o medios que se utilizan en la guerra actualmente que para 1949, en el momento de la redacción de los Convenios de Ginebra o después de sus protocolos adicionales, no existían. Esta particularidad significa que ahora surge una laguna y una desprotección importante para los ciudadanos que necesita ser cubierta y este Manual representa un primer paso hacia delante en el tópico.

Aún y cuando el Manual de Tallinn ofrece las ventajas anteriormente mencionadas, debe recordarse, tal como lo reconoce el propio CICR, que las empresas y los gobiernos están tan expuestos al espionaje cibernético, los crímenes cibernéticos y otras actividades

[131] Comité Internacional de la Cruz Roja. *¿Qué limites impone el derecho de la guerra a los ataques cibernéticos?,* página oficial del Comité Internacional de la Cruz Roja, (2013), consultado el 5 de febrero de 2017. https://www.icrc.org/spa/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

cibernéticas malintencionadas como a los ataques cibernéticos que incumben al DIH y, si bien pueden emplearse medios técnicos similares para proteger una infraestructura cibernética del espionaje o un ataque, el derecho por el que se rigen estas operaciones es distinto y esta cuestión debe ser zanjada por los propios Estados[132].

El Manual de Tallinn es un documento no vinculante, elaborado por un grupo de expertos, el cual, aunque se espera pueda contribuir de forma provechosa a fomentar las deliberaciones entre Estados relativas a esta compleja cuestión[133], no cubre todos los aspectos ni escenarios posibles bajo los cuales se puede dar un ciberataque.

El mencionado Manual enfoca sus esfuerzos en tiempos de guerra, bajo los cuales el DIH resulta aplicable, pero deja por fuera los ataques que se generen en tiempos de paz. Además, resulta importante que el Manual se basa en opinión y conocimiento de los expertos, así como en tratados internacionales ya existentes, lo que no es igual a la opinión ni práctica de los Estados, razón por la cual no resulta vinculante el mencionado estudio.

Por todo lo anterior, en la presente investigación se pretende analizar la posible responsabilidad de un Estado por un ciberataque cometido en tiempos de paz y los medios para atribuir esa responsabilidad, basadas en costumbre internacional.

b. Manual de Tallinn sobre el Derecho Internacional Aplicable a Operaciones Cibernéticas (Tallinn 2.0)

El Manual de Tallinn 2.0[134], corresponde al trabajo continuado de los expertos encargados de desarrollar el Manual de Tallinn sobre el Derecho Internacional Aplicable a la Guerra Cibernética, donde como en el primer manual, se establece una serie de reglas aplicables a actividades cibernéticas. Sin embargo, en el Tallinn 2.0, el análisis se centra en ciberactividades de un nivel menor al de un contexto de guerra y en su lugar se centra en pequeñas actividades cibernéticas que constituyen la mayoría de ciberataques del día a día.

[132] Íbid.
[133] Íbid.
[134] Schmitt, Michael N. *Tallinn Manual 2.0 on the international law applicable to cyber operations.* Cambridge, United Kingdom: Cambridge University Press, 2017.

Las ciberoperaciones y ciberataques, hoy usualmente están por debajo del umbral para considerarse actos de guerra en el Derecho Internacional.

A través de las 154 Reglas establecidas en el Manual, se presenta una serie de preguntas comunes en el ámbito de las ciberoperaciones y se discute el estado actual del Derecho Internacional y como puede aplicarse a cada escenario. A su vez, en cada regla se hace mención sobre los puntos en donde los expertos lograban tener consenso y aquellos puntos en donde no existía consenso debido a lo complejo y a las imprevisiones del mundo cibernético.

Debido a la prominencia del ciberespionaje en la era de Edward Snowden y Wikileaks, el Tallin 2.0 explora la legalidad de ciertos métodos empleados por la Agencia Nacional de Seguridad de los Estados Unidos de América (NSA) y determinan que fueron incapaces de alcanzar consenso de si las operaciones de espionaje remoto llegan a un límite de severidad que viole el Derecho Internacional.

Uno de los escenarios que contempla el Manual explora la legalidad de actuaciones de naciones que *hackean* plantas nucleares en otras naciones y mantenerlas como rehenes para obligar al Estado a actuar de cierta forma. Esto es especialmente interesante en razón de que gobiernos, como el de los Estados Unidos, han planteado realizar acciones de esta naturaleza.

Parte del valor del Tallinn 2.0, al igual que el primer manual, es la utilización de reglas generales del Derecho Internacional, lo cual permite que el trabajo sea de referencia para gobiernos y departamentos legales en la evaluación de determinadas situaciones cibernéticas. Sin embargo, se debe recalcar que este tampoco es un cuerpo normativo vinculante ni refleja las opiniones o práctica de los Estados.

Sección III: atribución de Responsabilidad Internacional a los Estados por ciberataques

Según el numeral segundo[135] de AREHII, así como la propia jurisprudencia de la CPJI[136] y luego de la CIJ[137], las condiciones necesarias para que la acción u omisión de un Estado constituya un hecho internacionalmente ilícito son: (i) que el hecho le sea atribuible al Estado; y, (ii) constituya una violación a una obligación internacional del mismo. Bajo este entendido, el capítulo II de los mencionados artículos posee disposiciones que ayudan a determinar la atribución requerida, los cuales se analizarán en los siguientes apartados, en conjunto con otras fuentes del derecho, para lograr determinar la posible atribución de un ciberataque a un Estado y su calificación como un hecho internacionalmente ilícito.

i. Atribución de responsabilidad internacional a los Estados por la comisión de un ciberataque

a) Atribución directa

Se podría pensar que la conducta de todos los seres humanos, corporaciones o colectividades vinculadas al Estado por nacionalidad, residencia habitual o incorporación podría atribuirse al Estado, independientemente de que tengan alguna relación con el gobierno. No obstante, en el Derecho Internacional se evita tal enfoque, tanto para limitar la responsabilidad a la conducta que involucra al Estado como organización, como para reconocer la autonomía de las personas que actúan por cuenta propia y no a instancias de una autoridad pública[138]. Por lo tanto, la regla general es que la única conducta atribuida al

[135] AREHII, Art. 2. Elementos del hecho internacionalmente ilícito del Estado. Hay hecho internacionalmente ilícito del Estado cuando un comportamiento consistente en una acción u omisión: a) Es atribuible al Estado según el derecho internacional; y b) Constituye una violación de una obligación internacional del Estado.
[136] *Cfr*. *Fosfato en Marruecos*, objeciones preliminares, (1938) CPJI (ser A/B) No. 74, para. 28.
[137] *Cfr*. *Agentes Diplomáticos y Consulares Estadounidenses en Teherán*, p. 3, para. 56, *Nicaragua*, Sentencia, para. 226; y *Gabćíkovo*, para. 78.
[138] *Cfr*. Ian Brownlie, *System of the Law of Nations: State Responsibility*, Parte I (Oxford, Inglaterra: Clarendon Press, 1983), ps. 132-166 y David D. Caron, "The basis of responsibility: attribution and other trans-substantive rules", *The Iran-United States Claims Tribunal: Its Contribution to the Law of State Responsibility*, R. B. Lillich y D. B. Magraw, eds. (Irvington-on-Hudson, Nueva York, Estados Unidos: Transnational, 1998), 109.

Estado en el plano internacional es la de sus órganos de gobierno[139] y solo en dos situaciones excepcionales la atribución le viene establecida por los hechos de los particulares, un caso es cuando particulares han actuado bajo la dirección, instigación o control de esos órganos; es decir, como agentes del Estado[140], o bien, cuando el Estado asume una determinada conducta, por consecuencia directa de los hechos ilícitos previamente cometidos por los particulares[141].

Lo anterior se evidencia en los artículos del capítulo II de AREHII. Se extrae que el elemento principal para establecer la responsabilidad internacional del Estado por un acto u omisión, es poder probar o establecer el nexo entre la persona, organismo o entidad que cometió el hecho o la omisión y el Estado, por ende, probar la atribución del hecho internacionalmente ilícito al Estado.

En el tema objeto de análisis, la atribución directa de un ciberataque puede resultar particularmente problemática debido al avanzado desarrollo de las tecnologías y la naturaleza misma del ciberataque y el Internet, explicadas con anterioridad. En gran cantidad de casos, el proveedor de un servicio o la aplicación utilizada pueden tener acceso a la geolocalización desde la cual se generó el ataque; por ejemplo, se puede obtener la conexión Wi-Fi o el Sistema de Posicionamiento Global (GPS por sus siglas en inglés) desde los cuales se cometió la acción[142]. Asimismo, se puede identificar la ubicación desde la que fue lanzado el ataque, por medio de la dirección IP de origen, como se mencionó

[139] Artículo 4 de AREHII, el cual establece: Comportamiento de los órganos del Estado 1. Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado.
[140] Artículo 8 de AREHII, el cual establece: Comportamiento bajo la dirección o control del Estado. Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento.
[141] Artículo 11 de AREHII, el cual establece: Comportamiento que el Estado reconoce y adopta como propio. El comportamiento que no sea atribuible al Estado en virtud de los artículos precedentes se considerará, no obstante, hecho de ese Estado según el derecho internacional en el caso y en la medida en que el Estado reconozca y adopte ese comportamiento como propio.
[142] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York, Estados Unidos: Cambridge University Press, 2013, ps. 27-28.

antes, es el número o código que indica de dónde vino el paquete (algo así como la dirección de retorno en una carta o postal)[143].

Sin embargo, eso no indica quién utilizaba el dispositivo en ese momento, ni asegura quién es el responsable de la comisión del ciberataque; pues esa información puede ser forjada o falsa, sin mencionar el hecho de que puede tratarse de un lugar donde varias personas tengan acceso. Esto genera el grave problema de vaguedad que abre la importante discusión sobre la aplicación del principio de inocencia y al hablar de una responsabilidad estatal, solo se complica más el panorama, pues si no se logra identificar con exactitud quién cometió la falta, no se puede determinar si era agente del Estado o una persona que pueda generar su responsabilidad.

Cabe mencionar que existe la posibilidad de que se haya contratado un grupo de mercenarios para la comisión del ciberataque; por lo tanto, se requeriría de medios probatorios sumamente complejos de conseguir, por no decir imposibles, para asegurar que fue una persona específica quien realizó el ataque y esta le genera responsabilidad internacional al Estado.

Por su parte, los ataques DDoS representan un desafío para el objetivo de la atribución. El atacante (el llamado bot-master o el cliente que ha alquilado el bot-net desde el bot-master), por lo general tiene el cuidado de asegurar varios grados de separación de las máquinas donde realizan el ataque y, de esa forma, el rastreo de las mismas puede implicar cruzar líneas jurisdiccionales, lo cual añade complejidad y demora. Si el ataque real involucraba direcciones de origen falsificadas, tal rastreo puede ser muy difícil o incluso imposible[144].

Además, existe la estrategia de utilizar un ordenador zombi, esto consiste en un ordenador infectado con un tipo de software malicioso, el cual permite que una tercera persona ejecute actividades hostiles sin autorización o conocimiento del usuario. También

[143] David D. Clark y Susan Landau, *op. cit.* 5.
[144] Ídem, 7.

se tiene los conocidos Bot-net que son un conjunto de estos ordenadores con *malware*, como los que fueron identificados en los segundos ataques en Tallin, Estonia[145]. Por lo tanto, se observa que lograr probar la atribución directa de un ciberataque es prácticamente imposible; pues el grado de indefinición y las posibilidades de burla de la dirección IP del ataque son muchas.

Una forma que se utiliza a nivel nacional en la persecución de crímenes cibernéticos para probar la atribución de los mismos, es la de confiscar el equipo desde el cual se rastreó el ataque. No obstante, a nivel internacional esto resulta casi imposible sin cooperación del Estado atacante y no hay forma de saber que el movimiento de confiscación sea lo suficientemente rápido como para estar seguros de que el ordenador confiscado era del verdadero responsable, sin mencionar la posibilidad de que se trate de un computador zombi que no genere muchos medios de prueba.

Por otra parte, los DoS son relativamente más sencillos de ubicar; pues se trata de un solo ordenador realizando el ataque. Además, estos ataques son constantes debido a que se necesitan muchos de ellos saliendo de un solo ordenador para hacer colapsar un sistema, razón por la cual no son muy comunes a nivel internacional y si se dan, son fáciles de identificar y mitigar el daño, como lo hicieron en el caso de Estonia en el 2007. No obstante, a niveles internacionales, puede resultar complicado que un Estado tenga acceso a la máquina desde la cual se generaron dichos ataques y de ubicar a la persona que los realizó, con el objetivo de atribuirle la responsabilidad al Estado.

En virtud de todo lo anterior, queda demostrado que existen muchas formas y muchos espacios oscuros que ofrece el anonimato de la Web para cometer ciberataques, esto deja un margen muy amplio para asegurar el alto grado de certeza que requiere la atribución directa. No obstante, si se tiene el conocimiento del funcionamiento del *malware* y suficiente conocimiento del rastreo del ciberataque, podría llegarse a la atribución del mismo, especialmente si se toman en cuenta los estándares de la prueba en la práctica

[145] International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCD COE).

jurisprudencia de la CIJ en relación con la atribución indirecta.

b) Atribución indirecta y estándares de la prueba

En razón de los desarrollados obstáculos para la atribución directa de un hecho internacionalmente ilícito a un Estado, cabe recalcar cuáles son los criterios e interpretación de la CIJ respecto al estándar para determinar responsabilidad. Esto en especial consideración de los elementos de prueba disponibles en casos de ciberataques.

1. Los estándares de la Corte sobre la admisibilidad y valoración de la prueba

Es de importancia analizar, a partir de la jurisprudencia de la Corte, cuáles son los criterios de interpretación y el estándar utilizados para determinar la responsabilidad internacional de un Estado. En su jurisprudencia, la Corte ha dado un tratamiento distinto a ciertos elementos probatorios en la determinación de responsabilidad de los Estados, en especial respecto a medios indirectos de prueba y la utilización de prueba circunstancial.

De conformidad con el Artículo 60 del Estatuto de la CIJ, la Corte no es solo el principal órgano judicial de las Naciones Unidas, sino también la última instancia[146]. Al ser las sentencias de la Corte finales y sin apelación[147], esta debe velar por establecer el marco fáctico y de derecho del proceso, y llegar a una conclusión sustentada y justa para las partes.

La importancia de los criterios de análisis de la prueba no se ve disminuida a pesar de que las decisiones de la CIJ no son vinculantes, más que para las partes en un caso en concreto. Los criterios utilizados en casos anteriores son de referencia no solo para la Corte, de conformidad con el Artículo 38.1.d del Estatuto de la Corte, sino son de referencia para los Estados que presentan casos contenciosos ante esta.

[146] Artículo 60, Estatuto de la CIJ.
[147] Íbid.

a. Estándares de la prueba: amplios poderes y liberalidad procesal

En relación con los estándares de la prueba, el sistema de la CIJ no tiene un estándar definido. La Corte puede determinar si aplica un alto estándar para la atribución de responsabilidad, donde esta se debe probar más allá de toda duda razonable, o aplicar un estándar más bajo, donde la prueba debe ser única y lo suficientemente convincente para probar la alegada violación de Derecho Internacional. En el análisis para la determinación de un estándar, la Corte mantiene un criterio liberal en la evaluación de la evidencia y se basa en los hechos y las circunstancias de cada caso[148].

La Corte realizó algunas observaciones en relación con el estándar de la prueba en *Corfu (Reino Unido v. Albania)* en 1949, donde rechazó evidencia que no alcanzaba el nivel de prueba irrefutable y se refirió al grado de certeza requerido para atribuir responsabilidad por una acusación de tal gravedad[149].

Sin embargo, desde entonces la Corte no ha sido tan específica respecto al estándar de prueba requerido, incluso en asuntos particulares. En el caso de *Plataformas Petroleras (República Islámica de Irán v. Estados Unidos de América),* la Corte no explicó el estándar que se debía cumplir, y quedó satisfecha al establecer que no debía decidir con base en un *"balance de evidencia"*[150]. No obstante, por su parte la Jueza Rosalyn Higgins en su opinión separada del caso mencionado, hizo hincapié en que más allá de un acuerdo generalizado de que entre más grave la violación, mayor confianza debe haber respecto a la evidencia; regularmente hay poco para ayudar a las partes (quienes asumen tienen la carga de la prueba) que acuden a la Corte a determinar qué es considerado como prueba suficiente para satisfacer a la misma[151]. La Jueza Higgins menciona a otros tribunales judiciales y arbitrales que se han dado a la tarea de reconocer la necesidad de determinar

[148] Higgins, Rosalyn. "Speech by H.E. Judge Rosalyn Higgins President of the International Court of Justice." Speech, November 2, 2007. Consultado en enero 2017. http://www.icj-cij.org/presscom/files/3/14123.pdf, 4.
[149] *Cfr. Corfu*, 17.
[150] *Cfr*. Plataformas Petroleras (República Islámica de Irán v. Estados Unidos de América), Sentencia, Reportes CIJ 2003, p. 161, para. 57.
[151] *Cfr*. Plataformas Petroleras (República Islámica de Irán v. Estados Unidos de América), Sentencia, Reportes CIJ 2003, Opinión Separada Jueza Higgins, para. 33.

estos estándares con mayor detalle como, por ejemplo, la Corte Interamericana de Derechos Humanos[152] y las Comisiones de Reclamos Eritrea-Etiopía[153].

La Jueza Higgins continúa mencionando que el principal órgano de las Naciones Unidas para la resolución de conflictos entre Estados debería, al igual que lo han hecho otros organismos internacionales, hacer claros cuáles son los estándares necesarios de prueba para establecer los hechos en un caso. Asimismo, indica que si la Corte no desea enunciar el estándar general en casos no criminales, en su opinión, debería ser transparente respecto al estándar requerido en este caso en particular[154]. En dicha opinión no queda claro si la Corte está rechazando prueba indirecta *per se*, (aún y cuando fue claramente admitida en el caso de Corfu en 1949), o si estaba aceptando prueba indirecta que en particular no se cumplió con el estándar *"sin espacio para duda razonable"* enunciado en 1949 en Corfu[155].

Por el contrario, en el caso de *Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro),* la Corte sí consideró necesario determinar el estándar de prueba necesario. En ese sentido, indica la sentencia:

> The Court has long recognized that claims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive (cf. Corfu Channel (United Kingdom v. Albania), Judgment, I.C.J. Reports 1949, p. 17). The Court requires that it be fully convinced that allegations made in the proceedings, that the crime of genocide or the other acts enumerated in Article III have been committed, have been clearly established. The same standard applies to the proof of attribution for such acts[156].

---

[152] Corte IDH. Caso Velásquez Rodríguez vs. Honduras. Fondo. Sentencia de 29 de julio de 1988. Serie C No. 4, paras. 127-139.
[153] Reclamo 17 de Etiopía, Comisión de Reclamos Eritrea-Etiopía, Laudo Parcial del 1 de julio de 2003, paras. 43- 53.
[154] *Cfr*. Plataformas Petroleras, Opinión Separada Jueza Higgins, para. 33.
[155] *Cfr. Ídem*, para.35.
[156] Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro), Sentencia, para.209. *"La Corte ha reconocido desde hace tiempo que los alegatos contra un Estado que involucran casos de especial gravedad deben de ser probados por evidencia que es completamente concluyente (cf. Canal de Corfu (Reino Unido v. Albania), Sentencia, Reportes CIJ 1949, p. 17). La Corte requiere estar completamente convencida, que las acusaciones hechas en el proceso, que el crimen de genocidio u otros actos enumerados en el Artículo III que*

De lo anterior se puede interpretar que la Corte no utiliza un estándar definido y por medio de su jurisprudencia ha utilizado estándares diversos. Esto en virtud de que la CIJ analiza las circunstancias caso por caso, analizando la gravedad del incumplimiento y los elementos de prueba disponibles.

Así es como en casos de ciberataques, la Corte podría analizar las circunstancias específicas y establecer un estándar según la gravedad del incumplimiento. Por ejemplo, se podría considerar un estándar diferente para casos en donde el ciberataque traiga como consecuencia pérdida de vidas humanas, a casos en donde el daño se limita a una estructura o sistema del Estado.

A pesar de que la Corte analiza las circunstancias y las violaciones del derecho en cada caso, cabe mencionar que la violación en el Derecho Internacional no requiere de la acreditación un daño, para ser considerada como tal[157].

b. Admisibilidad de la prueba

En sistemas nacionales existen lineamientos más rígidos respecto a la evidencia que es admisible en procesos legales. Por el contrario, la regla en la admisibilidad de prueba ante la CIJ es flexible. En principio no hay reglas altamente codificadas respecto al procedimiento de ingreso y administración de la prueba, ni hay restricciones respecto al tipo de evidencia que las partes pueden presentar. Este enfoque flexible de la Corte respecto a la admisibilidad de la prueba, ha sido percibido como su habilidad de determinar la carga y la relevancia de la evidencia en cada caso, debido a la alta calificación y experiencia de los jueces[158].

Es así, como cabe apreciar que la Corte se inspira tanto en el sistema de tradición anglosajona, como en el continental de derecho civil. Ejemplo de esto es como, por un lado,

---

han sido cometidos, hayan sido claramente establecidos. El mismo estándar aplica para la prueba de atribución para dichos actos". Traducción realizada por las autoras.

[157] AREHII, Art. 2.

[158] Eduardo Valencia-Ospina. "Evidence before the International Court of Justice". *International Law FORUM du droit international* 1, No. 4 (noviembre 1999): 202-07, 205.

inspirado en el sistema de *common law*, la CIJ, al igual que su predecesora la CPJI, ha admitido la introducción a los procesos de declaraciones juradas[159] como prueba. Por otro lado, inspirada en el sistema continental, la Corte tiene la potestad de activamente buscar prueba, tal como determina el Artículo 62 de las Reglas de la Corte, la cual indica:

> 1. The Court may at any time call upon the parties to produce such evidence or to give such explanations as the Court may consider to be necessary for the elucidation of any aspect of the matters in issue, or may itself seek other information for this purpose.
>
> 2. The Court may, if necessary, arrange for the attendance of a witness or expert to give evidence in the proceedings[160].

En relación con el artículo 62 anteriormente mencionado, la categoría de perito o *expert-witness* no está mencionada en forma expresa en el Estatuto o las Reglas de la Corte, pero ha sido reconocido en casos como el de *Corfu*[161], *Templo de Preah Vihear (Cambodia v. Thailand)* [162] y el *Caso África Sur-Oeste (Ethiopia v. Africa del Sur)*[163].

A pesar de que a las partes se les garantiza un amplio margen de libertad para la presentación de prueba, el Estatuto establece que los elementos probatorios que las partes deseen introducir al proceso, deben presentarse durante la fase escrita[164].

---

[159] *Mavrommatis*, *Corfu*, Sentencia.
[160] Art. 63, Reglas de la Corte. Adoptadas el 14 de abril y en vigor el 1 de julio de 1978. 1. *"La Corte puede en cualquier momento llamar a las partes a producir dicha evidencia o a dar explicaciones según la Corte considere necesarias para elucidar cualquier aspecto de la materia en cuestión, o puede por sí misma buscar información para este fin. 2. La Corte puede, de ser necesario, coordinar la asistencia de testigos o expertos a dar evidencia en los procedimientos Del anterior artículo son evidentes los amplios poderes que tiene la Corte para la solicitud de evidencia de cualquier naturaleza".* Traducción realizada por las autoras.
[161] *Cfr. Corfu*, 7.
[162] Caso del Templo de Preah Vihear (Cambodia v. Thailand), Sentencia del 15 junio 1962: Reportes CIJ 1962, p. 10.
[163] Caso África Sur-Oeste (Ethiopia v. Africa del Sur), Segunda Fase, Sentencia, Reportes CIJ, 1966, p. 6, 9 y 25.
[164] Artículo 56, Reglas de la Corte.

Es de importante consideración también que, dentro de las pocas limitaciones para la admisibilidad de la prueba, existe aquella limitación a prueba que haya sido obtenida por medios ilegales, la cual puede ser excluida del procedimiento ante la Corte. Esta situación fue explorada en el caso de *Corfu*, en donde el Reino Unido presentó evidencia obtenida mediante una operación no autorizada por el gobierno de Albania[165]. A pesar de la violación a la soberanía de Albania[166], la Corte admitió la prueba con la salvedad de que el Reino Unido si había cometido un hecho ilícito internacionalmente [167]. A partir de esto se ha interpretado que la Corte no hace aplicación de la regla de exclusión respecto a la admisibilidad de la prueba obtenida de manera ilegal[168].

Cabe hacer la salvedad de que, a pesar del precedente, se debe considerar que la prueba obtenida en contravención de normas de *ius cogens*[169], tiene un tratamiento diferente. Tal es el caso de la prueba obtenida mediante tortura, en directa contravención de la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes[170], la cual no admite excepción alguna, como norma imperativa de Derecho Internacional Público. De igual forma, se debe considerar la prohibición de los Estados al uso de la fuerza[171] y la violación de la soberanía[172] de otro Estado, por lo tanto, existen limitaciones a la obtención de prueba por medios que violenten estas disposiciones.

---

[165] *Corfu*, 33.
[166] *Corfu*, 35.
[167] Michael W Reisman, y Eric E. Freedman, "The Plaintiff's Dilema: Illegally obtained Evidence and Admissibility in International Adjudication", *Yale Law School Legal Scholarship Repository.* Paper 730, (1982): 747, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1722&context=fss_papers.
[168] Peter Tomka, y Vincent-Joel Proulx, "The Evidentiary Practice of the World Court", *NUS Law Working Paper Series*, Working Paper 2015/010, (2015): 11, http://law.nus.edu.sg/wps/pdfs/010_2015%20_Vincent-Joel%20Proulx_Tomka.pdf.
[169] Art. 53, Convención de Viena sobre el Derecho de los Tratados, 1969.
[170] Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes. Adoptada y abierta a la firma, ratificación y adhesión por la Asamblea General en su resolución 39/46, de 10 de diciembre de 1984.
[171] Art. 2.4, Carta de las Naciones Unidas.
[172] Art. 2.1, Carta de las Naciones Unidas. Resolución 2625 (XXV) de la Asamblea General de Naciones Unidas, de 24 de octubre de 1970, que contiene la Declaración Relativa a 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.

El Artículo 48 del Estatuto indica que la Corte podrá hacer todas las gestiones para obtener evidencia[173]. Asimismo, el Artículo 49 del Estatuto indica también que: *"The Court may, even before the hearing begins, call upon the agents to produce any document or to supply any explanations. Formal note shall be taken of any refusal"*[174]. Adicionalmente, el Artículo 50 del Estatuto de la Corte indica que: *"The Court may, at any time, entrust any individual, body, bureau, commission, or other organization that it may select, with the task of carrying out an enquiry or giving an expert opinion"*[175]. Dichas potestades evidencian los amplios poderes de la Corte de llevar a cabo actos para recopilar evidencia y solicitarle a los Estados la producción de cualquier elemento probatorio que considere necesario.

Este amplio margen de admisibilidad es valioso; pues al recibir casos de distinta naturaleza el mismo tipo de prueba, no siempre está disponible para todos. Esto permite a las partes recurrir a diferentes medios para defender sus alegatos y probar su caso. Sin embargo, se debe considerar que, a pesar de tener amplios poderes para la solicitud de prueba otorgados por el Estatuto, en la práctica la Corte tiene limitada inherencia sobre los Estados para que cumplan con su mandato en este sentido. Para esto existe la posibilidad de que la Corte utilice métodos alternos con el fin de que las partes cooperen.

En el marco de los ciberataques y las ciberoperaciones, la prueba puede derivar de distintas fuentes, esto incluye el disco duro de una computadora, un dispositivo de almacenamiento extraíble como las unidades flash USB, teléfonos móviles, satélites y el Internet; asimismo, puede presentarse en distintas formas como documentos de texto (correos electrónicos, mensajes instantáneos, hojas de cálculo), mapas, bases de datos, imágenes digitales, videos, datos de posicionamiento global (GPS), historial de internet y metadatos. Esta prueba puede estar en una fuente abierta, la cual no requiere de una

[173] Art. 48, Estatuto de la CIJ.
[174] Art.49, Estatuto de la CIJ. "*La Corte puede, incluso antes de las audiencias, llamar a los agentes a producir cualquier documento o a suministrar cualquier explicación. Nota formal debe ser tomada de la negativa a acatar".* La traducción fue realizada por las autoras.
[175] Art. 50, Estatuto de la CIJ. *"La Corte puede, en cualquier momento, investir a cualquier individuo, órgano, oficina, comisión u otra organización que pueda seleccionar, con la tarea de llevar a cabo cualquier investigación o dar una opinión experta".* La traducción fue realizada por las autoras.

contraseña o encriptación y aquella para la cual solo tengan accesos usuarios autorizados[176]. Por esto, es de valor que los parámetros de admisibilidad sean tan amplios; pues permite que los Estados introduzcan prueba de distinta naturaleza y queda entonces en manos de los jueces determinar su valor, autenticidad y relevancia en el caso en específico.

c. Interpretación adversa a la no producción de evidencia

De conformidad con lo indicado en el artículo 49 del Estatuto, la Corte ha aplicado la disposición de tomar nota formal de la negativa a la producción de evidencia en distintas ocasiones[177]. Este criterio se considera en casos en donde, en la negativa, la Corte tiene la facultad de interpretar de manera adversa la no producción de evidencia[178].

A partir del enfoque que también se utiliza en otros tribunales internacionales, la Corte podría inferir que la no producción de evidencia sería adversa a los intereses de la parte que no produzca la prueba[179]. Asimismo, podría usar el enfoque utilizado por las cortes en los Estados Unidos de América para lidiar con la solicitud de producción de prueba de fuentes internacionales, en las cuales no tienen jurisdicción. En estos casos las cortes estadounidenses pueden interpretar de manera adversa a la parte que incumple con la orden de producir la prueba[180].

Ninguno de los enfoques anteriormente mencionados está diseñado como una penalidad, sino como una forma de imponer presión para inducir al cumplimiento y poner a

[176] Marco Roscini, "Digital Evidence as a Means of Proof before the International Court of Justice", *Journal of Conflict & Security* 21, No. 3 (2016): 542, 541-554, consultado 11 de enero de 2017. doi:10.1093/jcsl/krw016.
[177] *Derechos de los Nacionales de los Estados Unidos de América en Marruecos*, Sentencia, 27 de agosto de 1952, Reportes CIJ 1952, p. 176. *Corfu*, Sentencia. *Caso del Oro Monetario Removido de Roma en 1943* (Italia v. Francia, Reino Unido de Gran Bretaña y el Norte de Irlanda, y Estados Unidos de América), Orden del 3 de noviembre, 1953, Reportes CIJ 1953, p.44.
[178] Michael P. Sharf y Margaux Day. "The International Corurt of Justice's Treatment of Circumnstantial Evidence and Adverese Inferences", *Chicago Journal of International Law.* Vol. 13. No 1. Artículo 6, (2012): 127-128, http://chicagounbound.uchicago.edu/cjil/vol13/iss1/6.
[179] "International Bar Association Rules on the Taking of Evidence in International Commercial Arbitrations". International Bar Association, Art. 9.4 y 9.5, consultado el 23 de enero de 2017. http://www.ibanet.org/Document/Default.aspx?DocumentUid=68336C49-4106-46BF-A1C6-A8F0880444DC. Recopilación de Laudos Arbitrales, Comisión de Reclamos Eritrea-Etiopía – Laudo Parcial: Frente Principal –Reclamos de Eritrea 2, 4, 6, 7, 8 & 22. 28 de abril 2004 VOLUMEN XXVI pp. 115-153.
[180] *Restatement (Third) of Foreign Relations Law of the United States §442(2)(c)2009*.

las partes en igualdad de condiciones[181] y, por tanto, a partir de la aplicación de esta interpretación los Estados estarían inclinados a cooperar con la Corte en la producción de evidencia. Esta sería una interpretación factible en casos de ciberataques donde, el Estado acusado tenga control sobre la prueba y no esté dispuesta a cooperar con la Corte.

d. Valoración de la prueba

Como se mencionó anteriormente en relación con la admisibilidad, el Estatuto y las Reglas de la Corte, no proveen mayores restricciones respecto a la presentación de pruebas. En principio, el marco permisivo de la Corte faculta a las partes a presentar cualquier tipo o forma de evidencia que consideren pertinente, en consideración de que la Corte tiene completa libertad para evaluar la prueba de conformidad con las circunstancias de cada caso y según las reglas pertinentes del Derecho Internacional[182].

Consecuentemente, la Corte no opera sobre la base de ningún filtro preliminar para la inadmisibilidad de la prueba, pero en cambio, tiene un amplio margen de apreciación para otorgarle diferente valor a elementos probatorios originarios de distintas fuentes.

De igual manera, no tiene un marco establecido de jerarquía entre los distintos tipos de evidencia. Ejemplo de esto es cómo la Corte constantemente es llamada a darle valor probatorio a reportes preparados por oficiales de los Estados o cuerpos independientes, en relación con hechos importantes. Esto ocurre en casos con gran cantidad de hechos a ser probados en contextos de conflictos armados[183].

En el caso de *Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro)*, la Corte indicó que el valor probatorio dado a cierto tipo de evidencia, depende de:

> […] among other things, on (1) the source of the item of evidence (for instance partisan, or neutral), (2) the process by which it has been generated (for instance an

[181] Íbid.
[182] Tomka, "The Evidentiary Practice of the World Court", 9
[183] Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro), Sentencia, Reportes CIJ, 2007, p. 43. Actividades Armadas en el Territorio del Congo (República Democrática del Congo v. Uganda) Sentencia, Reportes CIJ 2005, p. 168.

anonymous press report or the product of a careful court or court-like process), and (3) the quality or character of the item (such as statements against interest, and agreed or uncontested facts) [184].

La Corte ha hecho valer sus amplias facultades en la admisibilidad de la prueba en casos con hechos ampliamente complejos. Por ejemplo, en *Caza de Ballenas en la Antártida* [185] y *Genocidio (Croacia v. Serbia)* [186], donde se disputó la protección del ambiente y recursos vivos con evidencia científica de consideración; así como la violatoria de la Convención sobre la Protección y Castigo del Crimen de Genocidio, la Corte utilizó prueba testimonial, lo cual incluyó peritos para el estudio de los hechos.

En el caso entre la República Democrática del Congo (RDC) y Uganda, la Corte se refirió a distintos elementos probatorios de la siguiente manera:

> The Court will treat with caution evidentiary materials specially prepared for this case and also materials emanating from a single source. It will prefer contemporaneous evidence from persons with direct knowledge. It will give particular attention to reliable evidence acknowledging facts or conduct unfavourable to the State represented by the person making them […] The Court will also give weight to evidence that has not, even before this litigation, been challenged by impartial persons for the correctness of what it contains. The Court moreover notes that evidence obtained by examination of persons directly involved, and who were subsequently cross-examined by judges skilled in examination and experienced in assessing large amounts of factual information, some of it of a technical nature, merits special attention […][187].

---

[184] Ídem, para. 227. *"[…], entre otras cosas, (1) la fuente de la evidencia (por ejemplo, partidarias o neutrales), (2) el proceso mediante el cual fueron generados (por ejemplo, un reporte periodístico anónimo o el producto de un cuidadoso proceso similar al de una corte), y (3) la calidad o el carácter del objeto (como declaraciones contra interés, y hechos aceptados e indiscutibles)".* Traducción realizada por las autoras.

[185] *Caza de Ballenas en la Antártida* (Australia v. Japón: interviniendo Nueva Zelanda), Juzgamiento, Reportes CIJ 2014, p. 226.

[186] Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Croatia v. Serbia), Objeciones Preliminares, Sentencia, Reportes CIJ 2008, p. 412.

[187] Actividades Armadas en el Territorio del Congo (República Democrática del Congo v. Uganda), Sentencia, Reportes CIJ 2005, p. 168, para. 61. *"La Corte tratará con cautela, material probatorio*

En conclusión, distintas clases de evidencia pueden introducirse por las partes que comparecen frente a la CIJ, la cual estará sujeta a los parámetros de evidencia indicados con anterioridad y al amplio margen de apreciación de la misma para determinar el valor probatorio de cada elemento.

e. Carga de la prueba

La regla general indica que la carga de la prueba en procesos ante la Corte, igual en sistemas domésticos de naturaleza civil, es que la parte alegante del hecho típicamente debe probarlo, *onus probandi incumbit actor*i. La jurisprudencia de la Corte ha reiterado esta como la regla general, mediante la cual se espera que la parte que alega un hecho, lo pruebe[188].

En el caso de *Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo),* a pesar de reconocer la existencia de la regla sobre la carga de la prueba, la CIJ calificó la aplicación de esta regla de la siguiente manera:

> However, it would be wrong to regard this rule, based on the maxim onus probandi incumbit actori, as an absolute one, to be applied in all circumstances. The determination of the burden of proof is in reality dependent on the subject-matter and the nature of each dispute brought before

---

especialmente preparado para este caso y también cualquier material que provenga de una sola fuente. Va a preferir evidencia contemporánea de personas con directo conocimiento. Va a dar particular atención a evidencia confiable reconociendo hechos o conductas no favorables para el Estado representado por la persona haciéndolas […] La corte también dará valor a evidencia que no ha sido cuestionada, incluso antes del litigio, por personas imparciales por exactitud de su contenido. La Corte además toma nota de que evidencia obtenida por examinación de personas directamente involucradas, y que fueron subsecuentemente interrogadas por habilidosos jueces en interrogatorios y expertos en evaluar gran cantidad de información fáctica, alguna de ella de naturaleza técnica, merece atención especial […]". Traducción realizada por las autoras.

[188] Caso de Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo), Méritos, Juzgamiento, Reportes CIJ 2010 ("Diallo"), para 54. Aplicación de los Acuerdos Interinos del 13 de setiembre de 1995 (La Antigua República Yugoslava de Macedonia v. Grecia), Juzgamiento 5 diciembre 2011. Reportes CIJ 2011, para 72. Pulp Mills, para 162. Delimitación Marítima del Mar Negro (Romania v. Ukrania) Juzgamiento. Reportes CIJ, para 68. Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos de América), Jurisdicción y Admisibilidad, Reportes CIJ, 1984, para. 101. Caso en relación con la soberanía sobre Pedra Branca/Pulau Batu Puteh, Rocas Medias y Borde del Sur (Malasia v. Singapur), Juzgamiento del 23 de mayo de 2008. Reportes CIJ 2008, par. 45.

> the Court; it varies according to the type of facts which it is necessary to establish for the purposes of the decision of the case[189].

En este caso, la República de Guinea argumentaba que el señor Diallo –su nacional– sufrió de varias violaciones a sus Derechos Humanos en el territorio de la RDC. Sin embargo, estricta adherencia a la regla anteriormente mencionada, hubiera puesto a Guinea en una situación de difícil acceso probatorio, al tener que probar violaciones ocurridas dentro del territorio de la RDC. Al determinarse que estos son "hechos negativos", la RDC estuvo en una mejor posición para producir evidencia sobre su cumplimento en las obligaciones pertinentes.

La Corte señaló entonces, una mayor consideración para aplicar la carga de la prueba en casos de hechos negativos:

> In particular, where, as in these proceedings, it is alleged that a person has not been afforded, by a public authority, certain procedural guarantees to which he was entitled, it cannot as a general rule be demanded of the Applicant that it prove the negative fact which it is asserting. A public authority is generally able to demonstrate that it has followed the appropriate procedures and applied the guarantees required by law — if such was the case — by producing documentary evidence of the actions that were carried out. However, it cannot be inferred in every case where the Respondent is unable to prove the performance of a procedural obligation that it has disregarded it: that depends to a large extent on the precise nature of the obligation in question; some obligations normally imply that written documents are drawn

[189] *Diallo*, para 54. *"Sin embargo, sería equivocado considerar esta regla, basada en la máxima onus probando incumbit actori, como una absoluta, a ser aplicada en todas las circunstancias. La determinación de la carga de la prueba es en realidad dependiente de la materia y por la naturaleza de cada disputa llevada ante la Corte; varía de acuerdo con el tipo de hechos necesarios a establecer con el propósito de la decisión del caso".* Traducción realizada por las autoras.

up, while others do not. The time which has elapsed since the events must also be taken into account[190].

Este escenario no era novedoso para la Corte en ese momento; pues se había enfrentado a situaciones similares en casos anteriores, en donde una de las partes que comparece ante ella está en control exclusivo de importantes elementos probatorios, pero se rehúsa a producirlos en razón de consideraciones de seguridad u otras razones.

En *Corfu*, la Corte resolvió el dilema al recurrir a una inferencia flexible de los hechos contra el Estado que negó producir la evidencia en cuestión. En ese sentido la Corte indicó:

> […] the fact of this exclusive tentorial control exercised by a State within its frontiers has a bearing upon the methods of proof available to establish the knowledge of that State as to such events. By reason of this exclusive control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence. This indirect evidence is admitted in al1 systems of law, and its use is recognized by international decisions. It must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion[191].

---

[190] *Diallo*, para. 55. *"En particular, cuando, como es el presente caso, se alega que a una persona no se le proveyó, por las autoridades públicas, ciertas garantías procesarles a las cuales tiene derecho, no puede ser, como regla general, requerido del demandante que pruebe el hecho negativo que está asegurando. Una autoridad pública es generalmente capaz de demonstrar que ha seguido los procedimientos apropiados y aplicado las garantías requeridas por ley-si fuera el caso-al producir evidencia de las acciones que se llevaron a cabo. Sin embargo, no puede inferirse en todos los casos donde el demandado es incapaz de probar la ejecución de una obligación procesal que este la ignoró: depende en gran medida en la naturaleza precisa de la obligación en cuestión; algunas obligaciones normalmente implican la producción de documentos escritos, mientras otras no. El tiempo que ha pasado desde los eventos también debe ser tomado en consideración".* Traducción realizada por las autoras.

[191] *Corfu*, pag. 18. *"[…] el hecho de este control territorial exclusivo, ejercido por un Estado dentro de sus fronteras tiene influencia en los métodos de prueba disponibles para determinar el conocimiento de ese Estado en dichos eventos. Por razón de su control exclusivo, el otro Estado, la víctima de una violación de derecho internacional, es a menudo incapaz de producir prueba directa de los hechos que dan pie a la responsabilidad. Dicho Estado debe ser permitido un recurso liberal a la inferencia de hechos y evidencia*

En contraste, la misma Corte en el caso de *Genocidio (Bosnia Herzegovina v. Serbia Montenegro)*, decidió no utilizar el mismo estándar y confirmó que el enfoque de la CIJ al tratamiento de la prueba circunstancial e inferencia adversa de la misma, dependerá según la materia y las circunstancias del caso. El tratamiento de no utilizar dicha interpretación se basó principalmente en la necesidad de la Corte de comprobar el dolo requerido en el delito de genocidio por parte del gobierno serbio.

Cabe recalcar que la Corte ha permitido la aplicación liberal de evidencia circunstancial cuando se cumplen las siguientes circunstancias: (i) la prueba directa está en el control exclusivo de la parte contraria[192]; y, (ii) la evidencia circunstancial no contradice ninguna prueba directa o hechos aceptados por la Corte[193]. La Corte ha utilizado evidencia circunstancial en varias ocasiones[194] en vista de la falta de evidencia directa.

Como se ha mencionado supra, por la existencia cada vez más de casos con grandes bases fácticas y complejos hechos de naturaleza científica, el cuestionamiento sobre la carga de la prueba se vuelve más relevante[195], como sucedió en el caso de *Pulp Mills*. En este caso, la Corte se enfrentó a una extensa cantidad de alegatos contradictorios por las partes, justificadas con inmensa cantidad de información. Argentina argumentó que la carga de la prueba, la cual se basó en el principio precautorio del Estatuto en cuestión, recaía en Uruguay[196]. Además, Argentina indicó que, en todo caso, la carga debería ser compartida por ambas partes con base en lo indicado en el Estatuto. Aunque la Corte reafirmó la importancia del principio *onus probando incumbit actori*[197], también indicó que: *"this did*

---

circunstancial. Esta prueba indirecta es admitida en todos los sistemas de derecho, y su uso es reconocido en decisiones internacionales. Debe ser considerado de valor especial cuando se basa en una serie de hechos los cuales vinculados entre sí y llevan a una única conclusión lógica". Traducción realizada por las autoras.

[192] *Corfu*, at 18.

[193] *Corfu*, at 32.

[194] *Corfu*, Caso África Sur-Oeste, Segunda Fase, Sentencia, Reportes CIJ, 1966. Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos) Méritos, Sentencia, Reportes CIJ 1986, p. 14. Caso Relacionado a la Soberanía sobre Palau Ligitan y Palau Sipadan (Indonesia v. Malasia), Juzgamiento, Reportes CIJ 2002, p.625. Plataformas Petroleras. Actividades Armadas en el Territorio del Congo (República Democrática del Congo v. Uganda) Sentencia, Reportes CIJ 2005, p. 168. Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro), Sentencia, Reportes CIJ, 2007, para. 127.

[195] Tomka, *op. cit*., 21.

[196] Pulp Mills, para.160.

[197] Ídem, para. 162.

not […] mean that the Respondent should not co-operate in the provision of such evidence as may be in its possession that could assist the Court in resolving the dispute."[198].

La inversión de la carga de la prueba también ha sido utilizada en otros tribunales internacionales, como es el caso de la Comisión de Reclamos Eritrea-Etiopía, donde este último debió haber probado la no atribución y este no presentó ninguna evidencia en su defensa[199], por lo tanto, el tribunal falló en contra de Etiopía.

Dicho esto, dado que la atribución indirecta requiere de un análisis caso por caso y, tal y como se ha explicado, la Corte trata con gran cautela ciertos elementos probatorios, se estudia minuciosamente toda la evidencia presentada ante ella y se balancea la evidencia relevante contra los hechos, circunstancias y materia del caso, se puede concluir que existen posibilidades reales de atribución indirecta de la comisión de un ciberataque. Asimismo, es importante rescatar la práctica de la Corte de ser progresiva respecto a la introducción de nuevas formas de producir evidencia y su costumbre de adoptar nuevas tecnologías e innovadoras formas de establecer el marco fáctico[200], lo cual solo demuestra que la Corte posee las facultades y la libertad de recibir y analizar elementos probatorios de distinta naturaleza, para establecer la responsabilidad internacional de un Estado por la comisión de un ciberataque, de acuerdo con su naturaleza.

En esta misma línea, a pesar de que continúa siendo difícil atribuir un ciberataque de manera inequívoca en virtud de las complejidades que lo envuelven, la reconstrucción y el análisis forense resulta esencial para determinar la responsabilidad. Hoy, Estados han incorporado de manera sistemática la búsqueda de riesgos en sus sistemas, en vez de solo reaccionar a los ataques[201]. Recolectar evidencia de una gran y compleja base de datos toma

[198] Ídem, para. 163. *"esto no […] significa que el Demandado no debe de cooperar en otorgar de dicha evidencia la cual estando en su posesión puede asistir a la Corte en resolver la disputa".* Traducción realizada por las autoras.
[199] Recopilación de Laudos Arbitrales, Comisión de Reclamos Eritrea-Etiopía – Laudo Parcial: Frente Principal –Reclamos de Eritrea's 2, 4, 6, 7, 8 & 22. 28 de abril 2004 VOLUMEN XXVI, 115-153, para. 95.
[200] Tomka, *op. cit*., 23.
[201] Bendiek, Annegret. "Due Dilligence in Cyberspace", *Stiftung Wissenscharft und Politik German Institute for International and Security Affairs*, mayo 2016. Consultado el 19 de setiembre 2016. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf, 25.

tiempo y requiere de computadoras capaces. Por eso, usualmente las autoridades de gobierno recaen en soporte de científicos forenses privados.

En razón de lo anterior, los estándares anteriormente analizados son de vital importancia en la posibilidad de los Estados de recurrir ante la CIJ en situaciones de ciberataques, para que sea determinada la responsabilidad internacional del Estado.

Sección IV: atribución de responsabilidad al Estado por ciberataques realizados por actores no estatales

En la Edad Media se utilizaba el concepto de responsabilidad colectiva, la cual se basaba en una noción feudal que tenía sus orígenes en el *jus gentium* romano[202]. Este concepto implicaba que el grupo era responsable por lo que hiciera uno de sus miembros; por lo tanto, en términos internacionales, la acción de una persona podía justificar la toma de contramedidas contra el pueblo entero. Con el tiempo, explica el autor Becker, se pasó a una perspectiva en donde se daba la oportunidad al Estado de remediar los daños cometidos por sus miembros[203] y, actualmente, se maneja una teoría regida por el principio de no atribución de actos privados, el cual establece que el Estado es responsable a nivel legal solo por sus propias actuaciones u omisiones, y, explica que un Estado no puede ser responsable por las actuaciones de un privado sin ninguna relación con el mismo[204].

En ese sentido, resulta de vital importancia analizar los artículos de AREHII, los cuales contemplan las posibles formas de atribución de un acto u omisión de un particular a un Estado. Primero, debe considerarse que el artículo 4 del mencionado instrumento define que los hechos tomados en cuenta por el Estado, son los realizados por todo órgano del

[202] Jan Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law", New York University Journal of International Law and Politics (JILP), Vol. 36, No. 4 (2004): 79, consultado 16 de febrero de 2017, https://ssrn.com/abstract=2408953.
[203] Tal Becker, *Terrorism and the State Rethinking the Rules of State Responsability*. Oregon, Oxford y Portland: Hart Publishing, 2006, 13-14.
[204] Ídem, 12.

mismo que ejerza funciones legislativas, ejecutivas o de otra índole y se entenderá, que órgano es toda persona o entidad que tenga esa condición según el derecho interno del país[205]. Por lo tanto, ha de entenderse que cualquier otra persona o entidad que no entre en la definición antes dada o las subsecuentes excepciones establecidas por AREHII, ha de considerarse como terceros ajenos al Estado y, por ende, no le generan responsabilidad al mismo.

Ahora bien, el artículo 5 de AREHII establece que

> Se considerará hecho del Estado según el Derecho Internacional el comportamiento de una persona o entidad que no sea órgano del Estado según el artículo 4, pero esté facultada por el derecho de ese Estado para ejercer atribuciones del poder público, siempre que, en el caso de que se trate, la persona o entidad actúe en esa capacidad.

Este artículo abre el portillo para que empresas privadas y transnacionales funjan como órganos del Estado y, por tanto, generen su responsabilidad. No obstante, tal como lo señala el especialista Crawford, no todas las entidades privadas con lazos con el gobierno han de considerarse agentes del Estado en los términos del artículo 5 y señala que la jurisprudencia del Tribunal de Reclamos entre Irán y los Estados Unidos reconoce esta afirmación, así como la posibilidad de que este tipo de organismos le causen responsabilidad internacional a un Estado[206].

Un ejemplo claro de este tipo de situaciones en ciberataques, es que actualmente los Estados contratan empresas privadas o empresas transnacionales para que desarrollen la protección cibernética necesaria para organismos estatales o bien, para utilizar los medios cibernéticos de la empresa para distribuir algún servicio. Entonces surge la interrogante, ¿si estas empresas cometen un ciberataque podría ser atribuido al Estado?

[205] AREHII, Art. 4.
[206] James Crawford, *op. cit.*, 128.

De los comentarios realizados por la CDI a los artículos en estudio[207], al momento que fueron redactados como un borrador, específicamente de los comentarios realizados al artículo 5, se extrae una serie de elementos que deben analizarse para lograr determinar si el organismo en cuestión está en realidad "facultado" en el sentido establecido por el numeral quinto. Estos elementos los enumera el profesor especialista James Crawford[208] como: a) contenido del poder, b) la manera en que el poder es conferido a la entidad, c) el propósito para los cuales el poder debe ser ejercido, y, d) la medida en que la entidad es públicamente responsable del ejercicio de sus funciones.

Ahora bien, una vez efectuado este análisis y establecido que la empresa se encontraba facultada para realizar determinadas labores, el Estado podría ser considerado como responsable por una omisión en la obligatoriedad de debida diligencia de la empresa, por fallar en el compromiso de prevenir que los sistemas estatales sean utilizados para la realización de un ciberataque. El tema de debida diligencia se desarrollará con detalle más adelante, pero cabe rescatar que es uno de los únicos supuestos bajo el cual se señala la atribución de responsabilidad por la omisión de una empresa privada o transnacional.

Por otro lado, se maneja la posibilidad de que sea la misma empresa contratada la que cometa el ciberataque por medio de los sistemas estatales. Bajo este supuesto, el Estado sería responsable por omitir la persecución del hecho internacionalmente ilícito[209] o por no tener una previsión, la cual evitara que este supuesto se diera, esto vendría a ser una falta al deber de debida diligencia. Ahora bien, en cuanto a la atribución misma del ciberataque, el artículo 7 de AREHII establece:

---

207 Comisión de Derecho Internacional, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*"*, Naciones Unidas Copyright, 2001, consultado el 17 de febrero de 2016. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

208 James Crawford, *op. cit.*, 129.

209 La Corte Interamericana de Derechos Humanos se ha pronunciado en este mismo sentido al establecer que *"[l]a obligación referida se mantiene "cualquiera sea el agente al cual pueda eventualmente atribuirse la violación, aún los particulares, pues, si sus actos no son investigados con seriedad, resultarían, en cierto modo, auxiliados por el poder público, lo que comprometería la responsabilidad internacional del Estado"*. Véase *Caso Velásquez Rodríguez vs. Honduras*. Fondo. Sentencia del 29 de julio de 1988. Serie C No. 4, párr. 177, *Caso Espinoza Gonzáles vs. Perú*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 20 de noviembre de 2014. Serie C No. 289, párr. 238 y el *Caso Velásquez Paiz y otros vs. Guatemala*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 19 de noviembre de 2015. Serie C No. 307, párr. 143.

> El comportamiento de un órgano del Estado o de una persona o entidad facultada para ejercer atribuciones del poder público se considerará hecho del Estado según el Derecho Internacional si tal órgano, persona o entidad actúa en esa condición, aunque se exceda en su competencia o contravenga sus instrucciones.

Esta disposición ha sido reconocida como un principio general de la responsabilidad internacional de los Estados por otros tratados[210] y por otras Cortes Internacionales[211]. Esto lleva a concluir que sí existe la posibilidad de una atribución del ciberataque al Estado, pues, aunque el mismo no haya dado la orden de cometerlo, si la persona u organismo estaba ejerciendo sus atribuciones de poder público al momento de cometer el hecho internacionalmente ilícito y utilizó los medios del Estado para cometerlo[212], el Estado es responsable[213].

---

[210] En el artículo 91 del Protocolo Adicional a los Convenios de Ginebra de 12 de agosto de 1949, que se refiere a la protección de las víctimas de los conflictos armados internacionales (Protocolo I), se afirma que: *"Una Parte en conflicto [...] será responsable de todos los actos cometidos por personas que formen parte de sus fuerzas armadas "*: esto abarca claramente actos cometidos en contra de órdenes o instrucciones.

[211] En este sentido, la Corte Interamericana de Derechos Humanos ha establecido que "*independiente[mente] de que el órgano o funcionario haya actuado en contravención de disposiciones del derecho interno o desbordado los límites de su propia competencia, puesto que es un principio de Derecho Internacional que el Estado responde por los actos de sus agentes realizados al amparo de su carácter oficial y por las omisiones de los mismos aun si actúan fuera de los límites de su competencia o en violación del derecho interno"*, véase Caso *Velásquez Rodríguez vs. Honduras*, párr. 170; *Caso de la Masacre de Mapiripán vs. Colombia*. Fondo, Reparaciones y Costas. Sentencia del 15 de septiembre de 2005. Serie C No. 134, párr. 110; *Caso Masacre de Pueblo Bello vs. Colombia*. Fondo, Reparaciones y Costas. Sentencia del 31 de enero de 2006. Serie C No. 140, párrs. 111 y 112; *Caso Albán Cornejo y otros. vs. Ecuador*. Fondo, Reparaciones y Costas. Sentencia del 22 de noviembre de 2007. Serie C No. 171, párr. 60; *Caso Cantoral Huamaní y García Santa Cruz vs. Perú*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia del 10 de julio de 2007. Serie C No. 167, párr. 79; y *Caso Yvon Neptune vs. Haití*. Fondo, Reparaciones y Costas. Sentencia del 6 de mayo 2008. Serie C No. 180, párr. 37. Asimismo, la responsabilidad internacional del Estado por actos de particulares ha sido abordada por la Corte Europea de Derechos Humanos, por ejemplo, en casos como: Kiliç vs. Turquía, Sentencia del 28 de marzo de 2000, Aplicación No. 22492/93; *Osman vs. El Reino Unido*, Sentencia del 28 de octubre de 1998, Reportes de sentencias y Decisiones 1998-VIII; *Adali vs. Turquía*, Sentencia del 31 de marzo de 2005, Aplicación No. 38187/97.

[212] Según como señala la CDI en los comentarios realizados al artículo 7 de AREHII, en el caso *Caire* (Francia vs. México), el cual versaba sobre el asesinato de un ciudadano francés por dos oficiales mexicanos, fue establecido *"that the two officers, even if they are deemed to have acted outside their competence ... and even if their superiors countermanded an order, have involved the responsibility of the State, since they acted under cover of their status as officers and used means placed at their disposal on account of that status" ("que los dos oficiales, aunque se considere que han actuado fuera de su competencia [...] e incluso si sus superiores derogaron una orden, han incurrido en la responsabilidad del Estado, ya que actuaron bajo su condición de oficiales y utilizaron medios colocados a su disposición en razón de ese estatus"*. Traducción

En este sentido, cabe rescatar que, para llegar a esta conclusión, resulta necesario entonces, en palabras del Tribunal de Reclamos entre Irán–Estados Unidos, determinar si la conducta ha sido *"llevada a cabo por personas envueltas con autoridad gubernamental"*[214] o si la persona actuó en su condición de persona privada. Esta observación es particularmente importante al tomar en cuenta que empresas privadas y transnacionales, no tienen como único cliente al Estado, por lo que gozan de autonomía cuando no realizan las atribuciones públicas para las cuales fueron contratadas, por tanto, el Estado no podría ser considerado responsable por la comisión de un ciberataque ejecutado por una empresa privada en ejercicio de su autonomía del mismo.

Por otro lado, se cuenta con el artículo 8 de AREHII, el cual establece que el control o la dirección que tenga el Estado sobre el comportamiento de una persona o grupo de personas puede generar su responsabilidad internacional por los hechos que estos comentan.

En relación con este punto, existen dos tipos de control: el control efectivo y el general. El caso principal de la CIJ en donde se desarrollaron estos conceptos fue el denominado *Nicaragua* [215], que fueron cuestionadas por la Sala de Apelaciones del Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY)[216], pero la CIJ mantuvo su posición en el caso de las *Actividades Armadas en el Territorio del Congo (Democrática República del Congo Vs. Uganda*) y en el caso de la *Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina Vs. Serbia y Montenegro),* dos casos importantes y subsiguientes al de Nicaragua.

---

hecha por las autoras). Por lo que se comprende que el hecho de utilizar los medios del Estado es un elemento importante para establecer la responsabilidad internacional del mismo; pues fue considerado a la hora de la redacción de los artículos por parte de la CDI.

[213] *Cfr.* Tallinn 2.0, 89.

[214] *Petrolane, Inc. vs. el Gobierno de la República de Irán*, Irán- Estados Unidos. C.T.R., vol. 27, 64.

[215] Nicaragua, Sentencia, párrs. 105–115.

[216] TPIY, Sala de Apelaciones, *Tadić*, 15 de julio de 1999 (Caso no. IT-94-1-A).

En el Caso Nicaragua, la Corte afirmó que:

> *[…] even the general control by the respondent State over a force with a high degree of dependence on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of acts contrary to human rights and humanitarian law alleged [...] Such acts could well be committed by members of the contras without the control of the United States. For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed*[217].

Tal como se deriva de la cita anterior, la CIJ desarrolla el tema de control efectivo, al indicar que la asistencia brindada por los Estados Unidos no es suficiente para establecer que son responsables de las actuaciones de "los contras"; pues la forma de intervención de este Estado solo demuestra un control general más no efectivo y, este último, es el tipo de control que se requiere para condenar a un Estado por las actuaciones de un grupo insurgente. Este mismo análisis fue sostenido por la Corte en el caso sobre la *Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina vs. Serbia y Montenegro),* donde adicionalmente reconoce al artículo 8 de AREHII como costumbre internacional[218].

En este mismo caso, la Corte analizó la posición de la Sala de Apelaciones del TPIY, en el cual se estableció que el control general sobre la Republika Srpska y su ejército era suficiente para que generara responsabilidad internacional a la República Federal de

---

[217] *Nicaragua*, Sentencia, párr. 105, *"incluso el control general por parte del Estado demandado sobre una fuerza con un alto grado de dependencia de ella no significaría, en sí mismo, sin más pruebas, que los Estados Unidos dirigieron o hicieron cumplir la comisión de actos contrarios a los Derechos Humanos y al Derecho Humanitario alegados [...] Tales actos podrían ser cometidos por miembros de los contras sin el control de los Estados Unidos. Para que esta conducta dé lugar a la responsabilidad jurídica de los Estados Unidos, en principio habría que probar que ese Estado tenía un control efectivo de las operaciones militares o paramilitares en el curso de las cuales se cometieron las presuntas violaciones",* traducción realizada por las autoras.

[218] Genocidio (Bosnia y Herzegovina vs. Serbia y Montenegro), Sentencia, paras. 398 y 399.

Yugoslavia por los hechos internacionalmente ilícitos cometidos por los serbios de Bosnia. En este caso, la Corte señaló que se veía incapaz de suscribir la opinión de la Cámara por dos razones: en primer lugar, porque el TPIY no fue invocado en el caso Tadić, ni se le pide en general que se pronuncie sobre cuestiones de responsabilidad de los Estados; pues su jurisdicción es penal y se extiende solo a personas. Por lo tanto, determinó que en dicha sentencia el Tribunal trató una cuestión que no era indispensable para el ejercicio de su jurisdicción.

En segundo lugar, según la CIJ, el criterio de control general que se utiliza en Tadić, si bien puede ser aplicable a la hora de determinar si un conflicto armado es internacional, considera que el mismo es "poco persuasivo" si se utiliza para definir si un Estado es responsable de actos realizados por fuerzas armadas y unidades paramilitares que no forman parte de sus órganos oficiales, esto en virtud de dos puntos, primero porque considera que no es lógico que se adopte el mismo criterio para resolver dos cuestiones de naturaleza muy diferente y dos, la prueba del control general amplía excesivamente el alcance de la responsabilidad estatal, porque va más allá de las tres normas establecidas por la CDI en el artículo 8 de AREHII[219].

Ahora bien, en el caso de marras, el artículo 8 podría ser aplicable tanto a empresas transnacionales o privadas, como a grupos insurgentes o los llamados grupos terroristas. Desde esta perspectiva y según los criterios utilizados por la CIJ, cabe indicar que no le resultaría atribuible a un Estado un ciberataque cometido por cualquiera de los grupos o empresas antes mencionadas, a menos de que se logre comprobar un planeamiento directo del Estado en el ciberataque y una intervención del mismo para la comisión de un hecho internacionalmente ilícito, el cual sea suficiente para probar el control efectivo del Estado en la ciberoperación, esto particularmente resulta difícil de probar, dada la naturaleza de los ciberataques que fue explicada con anterioridad.

[219] Ídem, párrs. 402 a 406.

Además, es importante señalar que todo este supuesto de atribución se desarrolla en un concepto de *intra vires*, si existe control efectivo de un Estado A en una ciberoperación que se planea ejecutar contra un segundo Estado B, pero si se da que sin autorización de A, la empresa o el grupo terrorista envía el mismo ciberataque que se había planeado con control efectivo del Estado A, contra un tercer Estado C, este ataque no le sería atribuible al Estado A, pues se rompió el control efectivo sobre el ciberataque y se dio como un hecho *ultra vires* considerado como un incidente en la misión[220].

El tema de terrorismo y la responsabilidad internacional en términos del tipo de control requerido, han generado críticas y preocupaciones particularmente importantes, en especial después del incidente del 11 de setiembre de 2001 en los Estados Unidos. Esto porque el borrador de AREHII se presentó en setiembre de 2001 y tan solo un mes después Al-Qaeda atacó Nueva York y Washington, DC[221]. Estas críticas se centran mucho en que el criterio adoptado por la CIJ en términos de control efectivo, puso la barrera muy alto como para encontrar un responsable a nivel internacional por ataques terroristas[222]. La crítica gira entorno a que si el financiamiento, el suministro y la coordinación de los ataques no son considerados como elementos suficientes para atribuir ataques terroristas a un Estado, entonces se vuelve fácil que un Estado se exima de una responsabilidad internacional por estos temas, a pesar de que provea de todo lo necesario a los grupos terroristas para la comisión de ciberataques[223].

Sin embargo, es relevante mencionar que existen opciones, las cuales pueden ayudar a solventar esta falencia en los AREHII, para que no resulten impunes situaciones de ciberataques, de los cuales no se logró demostrar el control efectivo del Estado atacante. Cagbe tener claro que esta posibilidad no implica una atribución del ciberataque en sí, sino que ofrece opciones para procesar a un Estado por colaborar con el grupo terrorista para

[220] *Cfr.* Tallinn 2.0, 99.
[221] James Crawford, *op. cit.*, 156.
[222] Íbid.
[223] Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", European Journal of International Law, segunda edición (2007):666, consultado el 20 de febrero de 2017, **http://www.ejil.org/article.php?article=233&issue=9**.

que se diera el ciberataque. Asimismo, resulta esencial tener presente que la regla general es que un Estado no puede ser responsable por actos de grupos insurgentes[224].

A partir de 1999 existe el Convenio Internacional para la Represión de la Financiación del Terrorismo[225] la cual establece la prohibición de proveer o recolectar fondos que se utilizarán en los términos del artículo 2.1 del Convenio[226]. El problema de aplicar este convenio a ciberataques es que el artículo 2.1.b) de la Convención, lo limita a actos que causen la muerte o lesiones físicas graves en las personas, con el objetivo de intimidar a una población u obligar a un gobierno o una organización internacional a realizar un acto o abstenerse de hacerlo. Por este motivo, al aplicar la convención se ve limitada en el tema de análisis; pues a menos que el ciberataque vaya dirigido a un medio que implique que mueran personas por causa del mismo, aplicar la Convención no sería posible.

En ese mismo sentido, la Convención Interamericana contra el Terrorismo, establece en su artículo 4, que: *"[c]ada Estado Parte, en la medida en que no lo haya hecho, deberá establecer un régimen jurídico y administrativo para prevenir, combatir y erradicar la financiación del terrorismo y para lograr una cooperación internacional efectiva al respecto"*. El único factor que se debe tomar en cuenta para aplicar esta obligación, es que el Estado haya ratificado la misma; por lo tanto, no es una disposición que se pueda aplicar de forma general a nivel internacional, pero representa una posibilidad

[224] James Crawford, *op. cit.*, 170.

[225] Convenio Internacional para la Represión de la Financiación del Terrorismo. Aprobado por la Asamblea General de Naciones Unidas en su resolución A/RES/54/109 de 9 de diciembre de 1999 y abierta a la firma el 10 de enero de 2000. Entrada en vigor: 10 de abril de 2002 de conformidad con el artículo 26 (1).

[226] Artículo 2

> 1. Comete delito en el sentido del presente Convenio quien por el medio que fuere, directa o indirectamente, ilícita y deliberadamente, provea o recolecte fondos con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte, para cometer:
> a) Un acto que constituya un delito comprendido en el ámbito de uno de los tratados enumerados en el anexo y tal como esté definido en ese tratado;
> b) Cualquier otro acto destinado a causar la muerte o lesiones corporales graves a un civil o a cualquier otra persona que no participe directamente en las hostilidades en una situación de conflicto armado, cuando, el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo.

de solución al vacío jurídico como en casos de que el Estado facilite por medios activos o pasivos, la comisión de ciberataques por grupos terroristas.

Finalmente, existe una solución que sí aplica en general internacionalmente y por la cual todos los Estados miembros de Naciones Unidas pueden responder en este tema, a pesar de que no formen parte de las convenciones mencionadas supra. Según el artículo 25 de la Carta de Naciones Unidas *"[su]s Miembros […] convienen en aceptar y cumplir las decisiones del Consejo de Seguridad de acuerdo con [l]a Carta"*. Esta disposición ha sido objeto de gran discusión en el Derecho Internacional, sobre el tipo de fuente que constituye una resolución del Consejo de Seguridad, pero sin importar que clasificación se le dé dentro del artículo 38 del Estatuto de la CIJ, es una obligación que deben acatar todos los Estados pertenecientes a Naciones Unidas.

En esta misma línea, resulta importante hacer referencia a la resolución del Consejo de Seguridad número 1373, por medio de la cual el Consejo, en virtud del capítulo VII de la Carta de Naciones Unidas, dispone que todos los Estados *"prevengan y repriman la financiación de todo acto de terrorismo"*, así como que se *"abstengan de proporcionar todo tipo de apoyo, activo o pasivo, a las entidades o personas que participen en la comisión de actos de terrorismo, en particular reprimiendo el reclutamiento de miembros de grupos terroristas y poniendo fin al abastecimiento de armas a los terroristas"* y requiere a los Estados que *"[a]dopten las medidas necesarias para prevenir la comisión de actos de terrorismo"*[227]. De acuerdo con las disposiciones del Consejo, si un Estado presta medios o colabora en la elaboración de un ciberataque por medio de financiamiento o equipo, resultaría responsable a nivel internacional por irrespetar las obligaciones ya mencionadas.

[227] La resolución 1373 del Consejo de Seguridad de Naciones Unidas se encuentra como anexo 1 al presente trabajo, debido a la importancia de las obligaciones específicas instauradas por el Consejo de Seguridad que resultan aplicables al presente tema.

Otra forma de que un ciberataque cometido por un grupo terrorista o insurgente sea atribuible a un Estado, sería que el mismo se dé bajo el supuesto del artículo 10 de AREHII, el cual establece:

> 1. Se considerará hecho del Estado según el Derecho Internacional el comportamiento de un movimiento insurreccional que se convierta en el nuevo gobierno del Estado.
>
> 2. El comportamiento de un movimiento insurreccional o de otra índole que logre establecer un nuevo Estado en parte del territorio de un Estado preexistente o en un territorio sujeto a su administración se considerará hecho del nuevo Estado según el Derecho Internacional.
>
> 3. El presente artículo se entenderá sin perjuicio de la atribución al Estado de todo comportamiento, cualquiera que sea su relación con el del movimiento de que se trate, que deba considerarse hecho de ese Estado en virtud de los artículos 4 a 9.

En el artículo mencionado se les reconoce a los grupos insurgentes la posibilidad de ser responsables por actos internacionalmente ilícitos, lo cual les otorga la posibilidad de crear un propio Estado interno. Esto en virtud de que, como se mencionó antes, la regla general es que un Estado no es responsable por los actos cometidos por estos grupos y este principio se evidencia con el artículo estudiado, el cual podría llamarse de "no atribución"; pues al darle la capacidad a estos grupos de cometer los hechos internacionalmente ilícitos por sí mismos, se deja de requerir la intervención del Estado y, por ende, se rompe la posibilidad de la atribución del ciberataque.

Ahora bien, si se toma este punto y el tema de la soberanía de los Estados, cabe anotar que en la opinión consultiva de Kosovo[228] se establece que el principio de integridad territorial está confinado a la relación entre Estados, pero al darle el estatus de Estado a un grupo insurgente, esto le otorga la capacidad de violentar la soberanía de un Estado por

[228] *Conformidad de la Declaración Unilateral de Independencia de Kosovo con el Derecho Internacional*, Opinión Consultiva. Reportes CIJ, 2010, p. 403, para. 80.

medio de un ciberataque, así se abre una ventana de atribución al grupo por sus propios actos y se libera de responsabilidad por una eventual violación al principio de soberanía a un Estado dentro del cual se encuentran estos grupos.

En virtud de todo lo anterior, se puede concluir que un Estado si podría ser responsable por un hecho internacionalmente ilícito que haya sido cometido por una empresa privada, semiprivada o transnacional, o bien, por colaborar en la comisión de un ciberataque realizado por un grupo terrorista o insurgente. No obstante, debe quedar claro que una atribución del ciberataque resulta compleja de establecer y las obligaciones irrespetadas que le pueden generar responsabilidad al Estado, como ya se analizó, son derivadas o van de la mano a la comisión del ciberataque, pero por su misma naturaleza, el nivel de complejidad para atribuirle el ciberataque en forma directa al Estado es muy alto.

Capítulo II

Obligaciones de los Estados respecto a la Comunidad Internacional

Sección I: soberanía en el contexto de ciberataques

Según indica Crawford, la soberanía de los Estados representa la base de la doctrina constitucional de la ley de naciones, la cual gobierna una comunidad de Estados, en principio, uniformes en cuanto a su personalidad legal[229]. Una definición de soberanía fue dada en el Laudo Arbitral del caso Isla de Palmas (Países Bajos vs. Estados Unidos), al establecer:

> 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[230].

Crawford explica que existen tres corolarios de la soberanía e igualdad entre Estados. El primero de ellos es la jurisdicción, *prima facie* exclusiva, sobre el territorio y las personas que en él habitan; el segundo, el deber de no intervención en el área de jurisdicción exclusiva de otros Estados y, finalmente, la dependencia del consentimiento de obligaciones que deriven de costumbre internacional o tratados[231].

En razón de todo lo anterior, se puede concluir que existen dos tipos de sentidos para el término soberanía, uno en cuanto a competencia sobre su territorio y otro de igualdad entre Estados; por lo tanto, se habla de una soberanía interna y una soberanía externa.

---

[229] James Crawford, *op. cit.*, 447.
[230] Recopilación de Laudos Arbitrales. Caso Isla de Palmas (Países Bajos vs. Estados Unidos). 4 de abril 1928. VOLUME II, 838. "*Soberanía en las relaciones entre Estados significa independencia. Independencia en relación con una parte del globo es el derecho a ejercer en ella, con exclusión de cualquier otro Estado, las funciones del Estado".* Traducción hecha por las estudiantes.
[231] James Crawford, *op. cit.*

El principio de soberanía es la fuente desde donde derivan otras obligaciones del Derecho Internacional provenientes de reglas o costumbre internacional, tales como el deber de debida diligencia[232], e incluso la CIJ ha establecido que el principio de soberanía está sumamente ligado a los principios de prohibición del uso de la fuerza y no intervención[233].

a) Soberanía aplicada como competencia del Estado

Al hablar del ciberespacio, este se ha descrito en la doctrina como un espacio que es de dominio global; por lo tanto, los expertos apoyan que ningún Estado puede hablar de soberanía sobre el ciberespacio *per se,* pero sí señalan que las ciberactividades que se realicen desde el territorio de un Estado y envuelve medios, personas o entidades, sobre las cuales el Estado sí ejerce su soberanía[234].

Los expertos del Tallinn 2.0 explican que cuando el Estado tenga posibilidad de ejercer su soberanía, como se mencionó con anterioridad, tiene dos consecuencias legales. La primera, es que la ciberinfraestructura, así como las actividades que se den por dichos medios, deben ser objeto de legislación nacional y el sistema de control propio de cada Estado; y, la segunda, es que la soberanía sobre su territorio da el derecho, amparado en el Derecho Internacional, de proteger la ciberinfraestructura y salvaguardar la ciberactividad localizada en, o que toma lugar, en el territorio del Estado[235].

Estas consecuencias entonces, para el Derecho Internacional, son importantes independientemente que la ciberinfraestructura sea de carácter privado o pública, o las actividades en el ciberespacio cometidas desde el territorio del Estado provengan de un ente del Estado o una persona u organismo privado; pues la soberanía interna le otorga la capacidad al Estado en cuestión, de disponer de reglas y medios a nivel interno para proteger que esta soberanía no sea violentada. Un ejemplo de esto se observa en Costa Rica

[232] *Cfr.* Tallinn 2.0, 11.
[233] *Nicaragua*, Sentencia, 212.
[234] *Cfr.* Tallinn 2.0, 12 y 13.
[235] Ídem, 13.

en el artículo 10 de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales[236], donde se imponen obligaciones de índole técnica y organización necesaria para proteger los datos personales con el propósito de que se evite su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a la ley mencionada.

En este punto cabe recordar que tal como lo señaló el juez Álvarez en su opinión separada del caso *Corfu* de la CIJ, la soberanía no solo ofrece derechos, pues también da deberes[237], como por ejemplo el deber de actuar conforme a la obligación de debida diligencia para determinar o prevenir daños a otros Estados provenientes de ciberataques de su territorio.

Este mismo principio lo reconoció la Corte en el caso *Nicaragua*, al establecer que la soberanía interna de un Estado, incluía decidir de forma independiente sus aspectos políticos, sociales, culturales, económicos, y legales[238]. Sin embargo, en algunas legislaciones internas, como en el caso de las libertades o los derechos civiles, se halan limitaciones autoimpuestas para el ejercicio de la soberanía del Estado. Por ejemplo, en Costa Rica, esto queda evidenciado en la Ley de Competencia y Defensa Efectiva del Consumidor[239] en su artículo 11[240], por medio de la cual se prohíben los monopolios absolutos en la prestación de bienes y servicios de Costa Rica.

b) Soberanía aplicada como igualdad entre Estados

El principio de soberanía aplicado en su aspecto internacional; es decir, frente a otros, se deriva del principio de igualdad entre Estados, el cual se encuentra contemplado en el artículo 2(1) de la Carta de Naciones Unidas. Todo Estado debe respetar la

[236] Asamblea Legislativa, Ley 8968 del 7 de julio de 2011. Ley de Protección de la Persona frente al tratamiento de sus datos personales. Publicado en La Gaceta número 170 del 5 de setiembre de 2011.
[237] *Corfu*, Opinión Separada Juez Álvarez, 43.
[238] *Nicaragua*, Sentencia, 212.
[239] Asamblea Legislativa, Ley 24222 del 20 de diciembre de 1994. Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. Publicado en La Gaceta número 14 del 19 de enero de 1995.
[240] Asamblea Legislativa, Ley 9072 del 20 de setiembre de 2012. Reforma Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. Publicado en La Gaceta número 193 del 5 de agosto de 2012.

personalidad, la integridad del territorio y la independencia política de los demás Estados y han de hacerlo de buena fe en cumplimiento de sus obligaciones internacionales[241].

La soberanía externa es la fuente misma de la inmunidad estatal, pues significa que un Estado es independiente de otros en sus relaciones externas y, por ende, siendo uno de los pilares antes mencionados, un Estado es libre de obligarse a nivel internacional o bien, decidir formar parte de la *opinio juris* y la práctica de los Estados que forma la costumbre internacional, lo cual resulta particularmente importante al tratarse del análisis de un tema como ciberataques que no cuenta con elementos dispositivos de obligaciones en el tópico a nivel internacional.

c) Violación a la soberanía por ciberataques

Cualquier ciberataque que le sea atribuido a un Estado, el cual afecte el ejercicio de la soberanía de otro Estado, sea externa o interna, constituye una violación a la soberanía del mismo y, por ende, constituye un hecho internacionalmente ilícito. El artículo 2(7) de la Carta de Naciones Unidas define que ninguna medida de ese instrumento *"autorizará a las Naciones Unidas a intervenir en los asuntos que son esencialmente de la jurisdicción interna de los Estados, ni obligará; a los Miembros a someter dichos asuntos a procedimientos de arreglo conforme a la […] Carta"*, pero aclara que esta disposición no se opone a aplicar las medidas coercitivas prescritas en el capítulo VII de la misma, por lo que sí existen supuestos de excepción en la Carta de Naciones Unidas, los cuales permiten la toma de medidas por parte de un Estado, como lo son que el ciberataque sea permitido en forma expresa por el Consejo de Seguridad o bien, se haya dado en respuesta a un ataque previo[242].

Ahora bien, debe recordarse que existen requerimientos específicos para que estas excepciones apliquen, un Estado no puede de forma unilateral decidir su aplicación sin

[241] *Cfr. Nicaragua*, Sentencia, para. 202 y el preámbulo de la Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas.
[242] Artículos 41 y 51 de la Carta de Naciones Unidas, respectivamente.

realizar los procedimientos necesarios, o bien, sin el análisis de procedencia de las excepciones que otorga la doctrina, la jurisprudencia y la interpretación de los expertos.

Un ejemplo en qué Estado consideró que se le vulneró la soberanía interna por una ciberoperación, son los recientes ataques que sufrió los Estados Unidos en sus elecciones presidenciales de 2016. El informe oficial publicado por el ICA (*Intelligence Community Assessment*), el cual viene respaldado por la Oficina del Director de Inteligencia de los Estados Unidos, establece que el presidente ruso, Vladimir Putin, ordenó una campaña de influencia del sistema de elecciones estadounidense [243], vulnerando así el sistema democrático de los Estados Unidos y, por ende, vulnerando su soberanía interna como país.

En el reporte se explica que la ciberoperación estuvo dividida en secciones, una parte de la misma iba destinada a extraer información y posteriormente publicarla para desacreditar a una de las candidatas más fuertes del momento, quien era Hilary Clinton y la otra fue una intrusión directa al Estado en su sistema de votaciones. Como se puede observar y según lo que fue explicado en la naturaleza de un ciberataque y sus tipos, la primera parte de la ciberoperación constituye una violación de la soberanía, pero desde una ciberexplotación, como se mencionó *supra*, consiste en la extracción de datos y el posterior uso de los mismos, mientras que la segunda parte si constituye un ciberataque en el sentido de que se ha entendido en el presente trabajo; por lo tanto, se analizará solo la parte de la ciberoperación que corresponde al ciberataque.

El reporte mencionado, señala que Rusia accedió a varios sistemas de votación en el país y aseguran que desde el 2014 los rusos se encontraban efectuando un estudio de los sistemas de votación utilizados por los Estados Unidos[244]. Si bien en el reporte publicado no se habla del análisis realizado que utilizaron los especialistas estadounidenses para

[243] Agencia del Centro de Inteligencia (CIA), Oficina de Investigación Federal (FBI) y Agencia de Seguridad Nacional (NSA), Background to "Assesing Russian Activities and Intentions in Recent US Elections": the Analitic Process and Cyber Incident Attribution, de 6 de enero de 2017, ii, consultado el 23 de febrero de 2017, https://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html
[244] Ídem, 13.

arribar a estas conclusiones, señalan que los expertos están conscientes de que rastrear un ciberataque para definir su atribución es sumamente complejo; sin embargo, afirman que no es imposible; pues indican que cualquier tipo de ciberoperación, maliciosa o no, deja rastro. Aseguran los analistas de la Comunidad de Inteligencia de los Estados Unidos que utilizaron esta información, pues con base en información anterior y conociendo los *malware* y su funcionamiento para eliminar el rastro, los llevó directo a las conclusiones que afirman con certeza[245] los tres organismos de investigación más fuertes de los Estados Unidos.

Por su lado, los expertos del Tallinn 2.0 analizan por medio de una analogía, que las ciberestructuras que no tienen fines comerciales, sino son propias del gobierno, gozan de inmunidad y, por lo tanto, si son destruidos esto constituye una violación a la soberanía del Estado. En el Tallinn 2.0 se hace referencia a la Convención de las Naciones Unidas sobre el Derecho del Mar; pues en sus artículos 95 y 96 establecen que los buques pertenecientes a un Estado y utilizados solo para un servicio oficial no comercial, tendrán completa inmunidad. Asimismo, se refieren a las aeronaves del Estado que disfrutan de inmunidad y señalan que, en razón de esto, una ciberinfraestructura que no sea para uso comercial, sino solo para uso del Estado, gozaría igualmente de inmunidad por analogía[246].

Por lo tanto, en conclusión, un Estado tiene derecho a ejercer las atribuciones de su soberanía, tanto interna como externa, sin que medie la intervención de otro Estado, porque de darse una intrusión del mismo, se estaría cometiendo un hecho internacionalmente ilícito capaz de causar responsabilidad internacional al Estado atacante.

[245] Ídem, 2.
[246] *Cfr.* Tallinn 2.0, 27-28.

Sección II: debida diligencia en el contexto de ciberataques

a) Debida diligencia en el Derecho Internacional

Adicional a los hechos internacionalmente ilícitos de los que un Estado puede ser responsable en el contexto de un ciberataque, existe también, en el Derecho Internacional, la obligación de debida diligencia de los Estados. Este requiere que los Estados utilicen un estándar de cuidado razonable para evitar la comisión de un ilícito[247]. El uso de debida diligencia hace al marco normativo internacional más flexible para acoplarse a las necesidades de los Estados en las cambiantes dinámicas en la comunidad internacional[248].

La debida diligencia como obligación en el Derecho Internacional tiene sus orígenes en el pensamiento de Hugo Grotius en el siglo XVII[249]; sin embargo, no fue hasta el siglo XIX donde la debida diligencia empezó a tomar forma y se aplicó tanto como una obligación como una limitación a las actuaciones de un Estado[250].

El concepto de debida diligencia se ha desarrollado a través del tiempo para ser considerado actualmente como costumbre internacional. Este refleja las bases de varios conceptos en el Derecho Internacional e incluye soberanía[251], igualdad soberana de los Estados[252], integridad territorial[253] y no interferencia[254]. Una visión tripartita debe

[247] ILA Comittee Due Dilligence in International Law "Due Diligence in International Law Second Report", *Study Groups - International Law Association*, (2015):2, consultado el 13 de enero de 2017. http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045.
[248] ILA Second Report, 2.
[249] Ibid.
[250] "Due Diligence in International Law First Report", 2.
[251] Carta de las Naciones Unidas, Art. 2(1), Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 XXV), penúltimo párrafo sobre los Principios de igualdad de derechos y auto-determiación de los pueblos. Convención de las Naciones Unidas sobre el Derecho del Mar, Arts. 56, 77. En el Caso Isla de Palmas, el Juez Huber en su laudo indicó: *"Sovereignty in relation to a portion of the surface of the globe is the legal condition necessary for the inclusion of such portion in the territory of any particular State... 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. The development of the national organization of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations [...] Territorial sovereignty belongs always to one, or in exceptional circumstances several States, to the exclusion of all others [...]"*.
[252] Carta de las Naciones Unidas, Art. 2(1), 78. Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 XXV).

considerarse en la debida diligencia: (i) un estado soberano está obligado a asegurar; (ii) que en su jurisdicción (la cual incluye todo el espacio en donde ejerce jurisdicción formal o control efectivo)[255]; (iii) los derechos e intereses de otros Estados no sean violados[256].

Como consecuencia del aumento en el movimiento de ciudadanos a través de fronteras, se empezó a reconocer que el Estado estaba bajo la obligación de tomar todas las medidas necesarias para proteger a extranjeros en su territorio. Como bien lo indicó el Juez Moore en el caso *SS Lotus*, por referencia de una decisión por la Corte Suprema de Justicia de los Estados Unidos de América en 1887, *"it is well settled that a State is bound to use due dilligence to prevent the comission within its dominions of criminal acts against another nation or its people"*.[257]

Asimismo, con el fortalecimiento de la noción de soberanía estatal, también se reconoció que los Estados estaban obligados a proteger la seguridad de otros en tiempos de paz y guerra. En el caso *Reclamos de Alabama de los Estados Unidos de América v. Gran Bretaña,* el Tribunal determinó una debida diligencia internacional de los Estados a mantener su neutralidad[258]. En este caso, el Tribunal estableció que el estándar para la debida diligencia debe ser en proporción a los riesgos a los cuales pueden ser expuestos los

---

[253] Carta de las Naciones Unidas, Art. 2(4), Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 XXV), Declaración sobre la concesión de la independencia a los países y pueblos coloniales, Aprobada por la resolución 1514 (XV) de la Asamblea General de las Naciones Unidas el 14 de diciembre de 1960. *Conformidad de la Declaración Unilateral de Independencia de Kosovo con el Derecho Internacional*, Opinión Consultiva. Reportes CIJ, 2010, p. 403, para. 80. Asamblea General, Resolución 3314 (XXIX), Definición del Crimen de Agresión.

[254] Carta Naciones Unidas Artículos 2.4 y 2.7. Nicaragua, paras. 202 y 205. Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 (XXV), Sección sobre el Principio relativo a la obligación de no intervención en asuntos de jurisdicción doméstica de cualquier Estado de conformidad con la Carta de las Naciones Unidas. Resolución 2131 (XX) 1965, *Declaración sobre la Admisibilidad de la Intervención en los Asuntos Internos de los Estados y Protección de su Independencia y Soberanía.* A/RES/20/2131 (21 de diciembre de 1965). Corfu, p. 35. *Actividades Armadas en el Territorio del Congo*, para. 164.

[255] *Al-Skeini vs. Reino Unido*, Sentencia del 7 de julio de 2011. Aplicación No. 55711/07.

[256] ILA, Second Report, 6.

[257] *Caso "SS Lotus"* (Francia v. Turquía) 1927 CPJI (Serie. A) No.10. *"está determinado que un Estado está obligado a usar debida diligencia en prevenir la comisión dentro de su dominio de un acto criminal en contra de otra nación o de su gente"*. Traducción realizada por las autoras.

[258] *Reclamos de Alabama de los Estados Unidos de América v. Gran Bretaña.*, pp.125-134, 129.

beligerantes al no cumplir con su obligación de neutralidad[259]. Este caso fue también de gran importancia al determinar responsabilidad Estatal por actos privados ocurriendo en el territorio del Estado, en aplicación de la de debida diligencia.

La obligación de debida diligencia también ha sido desarrollada en el caso *Trail Smelter*, en donde el Tribunal determinó que:

> *[…] under the principles of international law, as well as of the law of the United States, 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*.[260]

A pesar de que el anterior caso refiere a daños ambientales, el principio de prevención del daño fue desarrollado también por la CIJ en el Caso de *Corfu*. La CIJ en su decisión en este caso determinó que: *"it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"*[261], así estableció una definición actualmente reconocida de la debida diligencia. Esta es una obligación que deriva del principio de soberanía, la cual requiere que los Estados protejan, dentro de su territorio, los derechos de otros Estados[262].

A partir de esta resolución, la debida diligencia ha evolucionado a cubrir obligaciones amplias de los Estados respecto a daños, en especial en el campo del Derecho ambiental. Los Estados tienen el derecho soberano de explotar sus recursos, según sus propias políticas ambientales y de desarrollo. Sin embargo, tienen igualmente la responsabilidad de asegurar cuáles actividades dentro de su jurisdicción o control no causen

---

[259] *Ibid*.
[260] *Trail Smelter*, 1965. *"bajo los principios de Derecho Internacional, al igual que bajo las leyes de Estados Unidos, ningún Estado tiene el derecho de usar o permitir el uso de su territorio de manera en que cause daño por gases en o hacia el territorio de otro o a las propiedades o personas en ello, cuando el caso es de serias consecuencias y el daño es establecido de manera clara y con evidencia convincente"*. Traducción realizada por las autoras.
[261] *Corfu*, at. 22. *"es la obligación de todos los Estados no permitir conscientemente que su territorio sea usado para actos contrarios a los derechos de otros Estados".* Traducción realizada por las autoras.
[262] *Caso Isla de Palmas*, 839.

daño a otros Estados. Esto se observa en el Principio 2 de la Declaración de Río sobre el Ambiente y Desarrollo, el cual indica: *"De conformidad con la Carta de las Naciones Unidas y los principios del Derecho Internacional, los Estados tienen el derecho soberano de aprovechar sus propios recursos según sus propias políticas ambientales y de desarrollo, y la responsabilidad de velar por que las actividades realizadas dentro de su jurisdicción o bajo su control no causen daños al medio ambiente de otros Estados o de zonas que estén fuera de los límites de la jurisdicción nacional"*[263].

La CIJ en su opinión consultiva sobre la Legalidad de la Amenaza o Uso de Armas Nucleares indicó:

> The Court recognizes that the environment is under daily threat and that the use of nuclear weapons could constitute a catastrophe for the environment. The Court also recognizes that the environment is not an abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn. The existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment[264].

Asimismo, la Corte reafirma este criterio en el caso *Gabcikovo-Nagymaros* en 1997, volviendo a hacer énfasis sobre la importancia del ambiente, no solo para los Estados, sino para toda la humanidad[265].

---

[263] Declaración de Río sobre el Ambiente y Desarrollo, A/CONF.151/26 (Vol. I) (12 de agosto de 1992), Principio 2.

[264] *Legalidad de la Amenaza o Uso de Armas Nucleares,* Opinión Consultiva, Reportes CIJ, 1996., para. 29. *"La Corte reconoce que el ambiente está bajo amenaza diaria y el uso de armas nucleares puede constituir una catástrofe para el ambiente. La Corte también reconoce que el ambiente no es una abstracción, pero representa el espacio viviente, la calidad de vida y la misma salud de los seres humanos, incluyendo generaciones futuras. La existencia de una obligación general de los Estados de asegurar cuáles actividades dentro de su jurisdicción y control respeten el ambiente de otros Estados o de áreas más allá del control nacional es ahora parte del cuerpo del Derecho Internacional relacionado al ambiente*". Traducción realizada por las autoras.

[265] *Gabcikovo*, para. 53

El efecto de la debida diligencia en ciertos contextos, diluye la rigurosidad de obligaciones Estatales. Un enfoque menos rígido en obligaciones puede alentar una amplia participación y con el tiempo puede fortalecerse, así se crea costumbre internacional en relación con práctica estatal y *opinio iuris*. Ejemplo de esto es la obligación de estudios de impacto ambiental, la cual ha sido considerada ahora por la CIJ y progresivamente reforzada[266].

A pesar de que el principal avance del concepto de debida diligencia se ha dado en el campo del Derecho Ambiental, este se ha desarrollado en otras áreas del derecho también. Lo anterior debido a que no es una norma específica aplicable al Derecho Ambiental, sino que ha evolucionado a ser costumbre en el Derecho Internacional.

La Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970[267], la cual fue determinada como una regla de costumbre internacional por la CIJ en el Caso de *Actividades Armadas en el Territorio del Congo*, hace referencia a la obligación de debida diligencia en el caso específico al indicar que: *"Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force"*[268].

Este principio ha sido reiterado en el caso de *Agentes Diplomáticos y Consulares Estadounidenses en Tehrán*, ante la CIJ. En esta situación la Corte determinó que el

[266] *Pulp Mills en el Río Uruguay (Argentina v. Uruguay), Juzgamiento, Reportes CIJ 2010, p. 14*, *Ciertas Actividades llevadas a cabo por Nicaragua en la Zona Fronteriza y Construcción a lo largo del Río San Juan (Nicargua v. Costa Rica)*, Juzgamiento del 16 de diciembre de 2015.
[267] Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 (XXV).
[268] Actividades Armadas en el Territorio del Congo, para. 162. *"Cada Estado tiene el deber de abstenerse de organizar, instigar, asistir o participar en actos de guerra civil o actos terroristas en otro Estado o consentir en actividades organizadas dentro de su territorio dirigidas hacia la comisión de dichos actos, cuando los actos referidos en el presente párrafo implican amenaza o uso de la fuerza"*. Traducción realizada por las autoras.

Gobierno de Irán falló en tomar todas las *"medidas apropiadas"* para proteger la misión estadounidense[269].

Por tanto, se concibe de manera flexible el concepto de debida diligencia, el cual varía según las circunstancias y el ámbito del derecho en el cual es aplicable. Esto permite que los estados con capacidades económicas limitadas puedan participar del sistema de Derecho Internacional sin tener la carga de obligaciones normativas no razonables[270]. A pesar de esto, existen ciertas obligaciones de protección y debida diligencia donde el Estado está en la obligación de cumplir, independientemente de sus capacidades económicas. Tal es el caso de las obligaciones respecto a la protección de misiones diplomáticas e inmunidades[271], donde los Estados deben cumplir con el mismo estándar independiente de sus capacidades.

La debida diligencia se enfoca no en la pregunta violatoria a la obligación internacional, pero se pregunta si los Estados tomaron todas las medidas razonables y apropiadas para evitar y mitigar el daño a otros Estados[272]. Así es como un estándar razonable de juzgamiento, cuidado, prudencia y determinación se puede esperar de un Estado en circunstancias. Un Estado debe usar su infraestructura con un grado de diligencia conforme a la situación. Factores como la efectividad del control territorial, la capacidad y los medios disponibles para un Estado y la naturaleza de las actividades pueden determinar el grado de diligencia que deben tomar. Estados en desarrollo con administraciones inefectivas pueden no ser requeridos a actuar de la misma manera que un Estado con la posibilidad de incrementar y ejercer control[273].

a. Estándar de la obligación de Debida Diligencia

Usualmente, las reglas primarias establecen elementos para determinar si un Estado cumplió o no con su obligación de debida diligencia. Ejemplo de esto son la Convención

[269] *Agentes Diplomáticos y Consulares Estadounidenses en Teherán*, para. 63.
[270] ILA, Second Report, 3.
[271] Convención de Viena sobre Relaciones Diplomáticas. Viena 18 de abril de 1961, entrada en vigor 24 de abril de 1964, Art. 22(2).
[272] ILA, Second Report, 3.
[273] Flemme, Maria. "Due Diligence in International Law." Master's thesis, Faculty of Law-University of Lund, 2004. 2005. Consultado en noviembre de 2016. http://lup.lub.lu.se/student-papers/record/1557482 , 14.

Internacional para la Represión de la Financiación del Terrorismo[274] y la Convención de la Organización de las Naciones Unidas contra la Delincuencia Organizada Trasnacional[275]. Ambos cuerpos normativos establecen parámetros claros para determinar si los Estados cumplieron o no con su obligación.

Sin embargo, el estándar no siempre está claramente determinado por un cuerpo normativo específico. Como lo indicó el Tribunal Internacional sobre Derecho del Mar en la opinión consultiva sobre la Explotación Minera de los Fondos Marinos:

> The content of "due diligence" obligations may not easily be described in precise terms. Among the factors that make such a description difficult is the fact that "due diligence" is a variable concept. It may change over time as measures considered sufficiently diligent at a certain moment may become not diligent enough in light, for instance, of a new scientific or technological knowledge. […][276].

A pesar de que hay dificultad en determinar el estándar, esto no implica que la obligación de debida diligencia no tiene contenido. Los Estados mantienen la posibilidad de decidir los medios con los cuales utilizarán para cumplir con las medidas que se esperan de ellos. Sin embargo, esta discreción puede ser limitada en virtud de: (i) que la norma principal explícitamente indica los medios, como por ejemplo medidas legislativas específicas para prevenir y reprimir ciertas conductas; o, (ii) una medida específica es indispensable para evitar el daño[277].

Por tanto, la debida diligencia es un estándar flexible y razonable, el cual se adapta a hechos y circunstancias particulares. Si bien es difícil determinar en términos precisos los

[274] Asamblea General, Resolución A/RE/54/109, Convenio Internacional para la Represión de la Financiación del Terrorismo, Aprobado por la Asamblea General de Naciones Unidas el 9 de diciembre de 1999, entrada en vigor 10 de abril de 2002, Art. 18.
[275] Asamblea General, Resolución A/RES/55/25, Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, (8 de enero de 2001), Art. 7.
[276] Cámara de Disputas del Suelo Marino de Tribunal Internacional de Derecho del Mar, *Responsabilidades y Obligaciones de los Estados Patrocinando Personas y Entidades Respecto a las Actividades en el Área*, Opinión Consultiva, 1 de febrero de 2011, para. 117.
[277] ILA, Second Report, 7-8.

elementos, varios pueden ser derivados de casos y tratados para identificar las características fundamentales de la debida diligencia como concepto y principio. A continuación, se mencionarán estos elementos:

a) Razonabilidad

En debida diligencia el Estado debe llevar a cabo todas las medidas razonables que se espere tome. Incluso en graves violaciones de Derecho Internacional, como la comisión de genocidio, la CIJ estableció que el estándar para determinar responsabilidad al Estado es cuando manifiestamente falló en tomar todas las medidas necesarias que estaban bajo su poder[278].

Este estándar de razonabilidad también se ha incluido en los Lineamientos de las Naciones Unidas sobre Negocios y Derechos Humanos[279]. La Oficina de Derechos Humanos del Alto Comisionado ha indicado respecto a este estándar que:

> Such measure of prudence, activity, or assiduity, as is property to be expected from, and ordinarily exercised by, a reasonable and prudent [person] under the particular circumstances; not measured by an absolute standard, but depending on the relative facts of the special case […].[280]

Asimismo, el Proyecto de los Artículos de Daño Transfronterizo de Actividades Peligrosas también se refiere a este elemento[281].

---

[278] *Genocidio,* Sentencia, para. 430.

[279] Reporte del Representante Especial del Secretario General en el tema de Derechos Humanos y corporaciones transnacionales y otras empresas, John Ruggie, *Principios Guía en Negocios y Derechos Humanos, Implementando el Marco de las Naciones Unidas "Proteger, Respetar y Remedios",* UN DOC A/HRC/17/31, 21 de marzo de 2011.

[280] Alto Comisionado de los Derechos Humanos, *La Responsabilidad Corporativa para respetar Derechos Humanos, una guía interpretativa*, 6.

[281] Comisión de Derecho Internacional, @Draft articles on Prevention of Transboundary Harm from Hazardous Activities@, UN GOAR 56th Sess. Supp. No.10, UN Doc A/56/10 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf. Commentary to Article 3, para 10.

El criterio para determinar qué es razonable, debe depender, entre otros, del nivel de desarrollo del Estado. En ciberataques, debe considerarse entonces la complejidad de la infraestructura del Estado, las herramientas de seguridad disponible y las capacidades tecnológicas del mismo.

b) Buen gobierno

En relación con el elemento de buen gobierno, se debe considerar que la debida diligencia requiere del Estado no menos de una medida de prevención que un gobierno bien administrado pueda ejercer[282].

El Tribunal del Centro Internacional de Arreglo de Diferencias relativas a Inversiones (CIADI) en el caso de ILAA v. Sri Lanka, indicó:

> A number of other contemporary International law authorities noticed the "sliding scale", from the old "subjective" criteria that takes into consideration the relatively limited existing possibilities of local authorities in a given context, towards an "objective" standard of vigilance in assessing the required degree of protection and security with regard to what should be legitimately expected to be secured for foreign investors by a reasonably well organized modern state[283].

Dicho enfoque está, asimismo, implícito en la Opinión Consultiva sobre Explotación Minera de los Fondos Marinos[284]. Este elemento de buen gobierno, implica en el contexto de ciberataques, que se aplique un estándar distinto de exigencia, en relación con Estados que se encuentran en su funcionamiento efectivo, *versus* un Estado que no tenga la posibilidad real de administrarse según los estándares establecidos previamente.

---

[282] ILA, Second Report, 10.
[283] CIADI, *Asian Agricultural Products LTD. (AAPL) v. República de Sri Lanka*, Caso No. ARB/87/3, Laudo Final, 27 de junio de 1990, para. 77.
[284] Cámara de Disputas del Suelo Marino de Tribunal Internacional de Derecho del Mar, Opinión Consultiva, para. 158.

c) Control sobre el territorio y actores no estatales

Esta obligación de debida diligencia ha sido desarrollada principalmente en el campo del Derecho Internacional Humanitario. En este sentido, la CIJ en el caso de *Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro)* determinó en relación con la obligación de debida diligencia lo siguiente:

> […] In this area, the notion of "due diligence", which calls for an assessment in concreto, is of critical importance. Various parameters operate when assessing whether a State has duly discharged the obligation concerned. The first, which varies greatly from one State to another, is clearly the capacity to influence effectively the action of persons likely to commit, or already committing, genocide. This capacity itself depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events. The State's capacity to influence must also be assessed by legal criteria, since it is clear that every State may only act within the limits permitted by international law; seen thus, a State's capacity to influence may vary depending on its particular legal position vis-à-vis the situations and persons facing the danger, or the reality, of genocide. On the other hand, it is irrelevant whether the State whose responsibility is in issue claims, or even proves, that even if it had employed all means reasonably at its disposal, they would not have sufficed to prevent the commission of genocide. As well as being generally difficult to prove, this is irrelevant to the breach of the obligation of conduct in question, the more so since the possibility remains that the combined efforts of several States, each complying with its obligation to prevent, might have achieved the

result — averting the commission of genocide — which the efforts of only one State were insufficient to produce".[285]

Este estándar se refiere a que al Estado se le exigirá la aplicación de la debida diligencia, en el tanto tenga capacidad de influenciar y controlar los actos dentro de su territorio, todo en el marco de lo legalmente posible, en el ejercicio de las potestades soberanas del Estado. El mismo no puede alegar, en la determinación de si ejerció su obligatoriedad, que aun actuando de manera diligente, el ilícito se hubiera cometido. Por tanto, en el contexto de infraestructura cibernética de un Estado y actores no estatales que actúan en la comisión de un ilícito, serían aplicables los mencionados estándares.

d) Grado de riesgo

La Opinión Consultiva sobre la *Explotación Minera de los Fondos Marinos* indica que la obligación de debida diligencia cambia en virtud del riesgo de la actividad[286]. Este estándar también se refleja en el Proyecto de Artículos de la Comisión de Derecho Internacional sobre la Prevención de Daño Transfronterizo. El artículo 3 de este proyecto

[285] *Genocidio* (Bosnia y Herzegovina v. Serbia y Montenegro), para. 430. *"[…] En esta área la noción de "debida diligencia", la cual llama a una evaluación en concreto, es de importancia crítica. Varios parámetros operan cuando se evalúa si un Estado ha debidamente cumplido con la obligación. La primera, la cual varía grandemente de un Estado a otro, es la capacidad de influir en forma efectiva en la acción de las personas que posiblemente cometan, o ya estén cometiendo, genocidio. Esta capacidad por sí misma depende, entre otras cosas, en la distancia geográfica del Estado en cuestión de la escena de los eventos y de la fuerza de los vínculos políticos, al igual que vínculos de otra naturaleza, entre las autoridades del Estado y los actores principales en los eventos. La capacidad del Estado de influir debe ser evaluada por un criterio legal; pues es claro que los Estados solo pueden actuar dentro de lo permitido por el Derecho Internacional: por lo tanto, la capacidad de un Estado de influir puede variar según su posición legal vis-à-vis de la situación y las personas en peligro, de la realidad de genocidio. Por el otro lado, es irrelevante si el Estado cuya responsabilidad está en cuestión, alega o incluso prueba, que, utilizando todos los medios razonables a su disposición, no hubiera sido suficiente para prevenir la comisión de genocidio. No solo esto es generalmente difícil de probar, sino que es irrelevante a la violación de la obligación de la conducta en cuestión, más aún que las posibilidades existen de esfuerzos combinados entre varios Estados, cada uno cumpliendo con su obligación de prevenir, pudiendo alcanzar el resultado –previniendo la comisión de genocidio– cuando los esfuerzos de solo un Estado fueran insuficientes".* Traducción realizada por las autoras.
[286] Cámara de Disputas del Suelo Marino de Tribunal Internacional de Derecho del Mar, Opinión Consultiva, para. 117.

explica que el estándar de debida diligencia debe ser apropiado y proporcional al grado de riesgo del daño transfronterizo[287].

La Guía de la ONU sobre Principios de Derechos Humanos y Negocios acepta, igualmente, que la debida diligencia requerida incrementa en situaciones en donde el riesgo de daño conocido es significativo[288].

El Estado debe entonces tomar las medidas necesarias para evitar la comisión de actividades en el ciberespacio, las cuales signifiquen un grado de riesgo, tomando en cuenta el nivel de riesgo para el tipo de medida a tomar.

e) Conocimiento de la actividad y riesgo potencial

Usualmente, a los Estados solo se les puede exigir que actúen de manera diligente para prevenir daños de los cuales tienen conocimiento. Sin embargo, en algunas circunstancias un Estado puede estar en una obligación de usar sus mejores esfuerzos para adquirir conocimiento de la actividad que se está llevando a cabo dentro de su jurisdicción o territorio.

Lo anterior se refleja en la sentencia por la CIJ en *Corfu,* donde se concluyó que la colocación de las minas no pudo haberse realizado sin el conocimiento del gobierno de Albania[289]. Por tanto, Albania fue declarado responsable, porque sabía o debió haber sabido de la actividad.

A pesar de que a un Estado no se le exige que actué según ilícitos de los cuales no tiene conocimiento, en ciertas actividades cometidas por medio de su infraestructura cibernética, el Estado debe tomar todas las medidas razonables para evitar su ejecución; pues en ciertas circunstancias, no podría alegar que no tenía conocimiento de que su infraestructura estaba

[287] Comisión de Derecho Internacional. "Draft articles on Prevention of Transboundary Harm from Hazardous Activities". UN GOAR 56th Sess. Supp. No.10, UN Doc A/56/10 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf., comentario al Artículo 2, para 11.
[288] *Principios Guía en Negocios y Derechos Humanos*, Principio 17 (b).
[289] *Corfu*, 22.

siendo utilizada para la comisión de un hecho internacionalmente ilícito. Asimismo, respecto al riesgo potencial propio del ciberespacio, no se podría alegar desconocimiento y, por ende, la falta de medidas o actuación no se justificaría.

f) Mala fe y ausencia de medidas

No se puede considerar que un Estado ha actuado de manera diligente cuando actuó de mala fe o conscientemente se negó a tomar medidas en contra de la realización del ilícito.

El Tribunal en el Laudo Arbitral indicó este criterio en el caso *Wena Hotels Ltd. v. República Árabe de Egipto*[290]. En este caso el Tribunal determinó que el Estado falló en tomar acción legal en contra de aquellos responsables por la confiscación forzosa de bienes de Wena[291].

Por tanto, una acción consciente y de mala fe de no actuar de manera diligente por un ciberataque cometido por medio de su infraestructura, causaría la atribulación de responsabilidad del Estado.

b. Estándares de Debida Diligencia

A pesar de la existencia de los mencionados elementos, los cuales se deben tomar en cuenta en la obligación de debida diligencia, es relevante referirse también a los estándares objetivos y subjetivos que pueden aplicarse. Dichos estándares establecen criterios para determinar el cumplimiento del Estado de la obligación. El estándar objetivo dispone que el mismo debe aplicarse a todos los Estados, independientemente de sus características individuales. Mientras que el subjetivo permite expectativas distintas de los Estados, según su desarrollo, el grado de control o cualquier otra característica que pueda poner al Estado en una posición especial. A continuación, se mencionará en forma breve ambos estándares.

[290] CIADI, *Wena Hotels Ltd. v. República Árabe de Egipto*, Caso No. ARB/98/4, Laudo, 8 de diciembre de 2000.
[291] CIADI, *Wena Hotels*, paras. 82, 84 y 94.

a) Subjetivo

El nivel de desarrollo de los Estados puede tener inherencia en la operación de obligaciones de debida diligencia en ciertas circunstancias. La Organización Mundial del Comercio (OMC) permite a los estados identificarse como países *"en desarrollo"*[292], pero reserva la categoría de *"países menos desarrollados"* a los admitidos a la División de Políticas y Análisis de Desarrollo de las Naciones Unidas[293].

En el Derecho Ambiental Internacional el concepto de *"obligaciones diferenciadas pero comunes"* deriva de la Conferencia de Río sobre el Medio Ambiente y el Desarrollo de 1992 y los tratados que se produjeron como consecuencia[294].

En el ámbito de los Derechos Humanos, los Estados tienen estándares diferentes respecto a ciertos derechos. Tal es el caso de los derechos referidos en la Convención Internacional sobre Derechos Económicos Sociales y Culturales, en la cual se indica que los Estados deben tomar todas las medias apropiadas para alcanzar, de manera progresiva, ciertos derechos[295]. Naciones en desarrollo están permitidas a limitar ciertos derechos económicos, culturales y sociales a nacionales y ejercer un nivel más bajo de debida diligencia con respecto a no nacionales[296].

El Derecho Internacional Humanitario, también tiene normas de debida diligencia, ambos como parte de la costumbre internacional y los tratados. Sin embargo, el grado de control que las partes tengan sobre su territorio, ya sea efectivo o general, al igual que el rol de entes no estatales, lo cual incluye contratistas militares privados y organizaciones

[292] "World Trade Organization." WTO | Development - Who are the developing countries in the WTO? Consultado el 21 de enero de 2017. https://www.wto.org/english/tratop_e/devel_e/d1who_e.htm.
[293]"World Trade Organization" WTO | Understanding the WTO - least-developed countries. Consultado el 21 de enero de 2017. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org7_e.htm.
[294] Declaración de Río sobre el Ambiente y Desarrollo, Principio 7. Convenio sobre la Diversidad Biológica, 22 de mayo de 1992, entrada en vigor 29 de diciembre de 1993, Art. 6. Convención Marco de las Naciones Unidas sobre el Cambio Climático, GE.05-62220, 9 de Mayo 1992, Art. 3.1. Convención de las Naciones Unidas de Lucha contra la Desertificación, A/AC.241/27, 12 de diciembre de 1994, Art. 6.
[295] Pacto Internacional de Derechos Económicos, Sociales y Culturales, Asamblea General Resolución 2200 A (XXI), de 16 de diciembre de 1966, Art. 2.1. Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, Resolución 34/180 18 de diciembre de 1979, entrada en vigor 3 de setiembre de 1981, Art. 2
[296] Pacto Internacional de Derechos Económicos, Sociales y Culturales, Art. 2.3.

internacionales, crea estándares distintos respecto a la obligación de debida diligencia según las circunstancias específicas[297]. Estados ocupados también tienen la obligación de debida diligencia en el territorio que ocupan y el grado de sus obligaciones dependerá del grado de control[298].

Otros factores subjetivos también han sido considerados en establecer el grado de debida diligencia requerido por los Estados. En el caso entre Bosnia y Herzegovina v. Serbia y Montenegro, la CIJ determinó que la proximidad geográfica y las relaciones políticas militares y financieras entre los órganos del Estado de Serbia y los genocidas en Bosnia, crea una obligación distinta a la de otros Estados para tomar medidas preventivas[299].

b) Objetivo

Por otro lado, existen obligaciones de debida diligencia en la cuales el mismo estándar es requerido por todos los Estados, independientemente de sus recursos económicos, grado de control y otras características especiales.

En este sentido, surgen ciertas provisiones en la base de derechos económicos, sociales y culturales[300], la prevención del terrorismo[301], DIH[302] y ciertas obligaciones para la protección del ambiente de áreas fuera de la jurisdicción nacional[303].

En el acuerdo consultivo sobre la Explotación Minera de los Fondos Marinos, el Tribunal determinó que no podía establecerse un estándar más bajo en el tema de

[297] Geneva Conventions I-IV 1949, art 1 y 3, TPIR, Fiscalía v. Jean Paul Akayesu, 2 de setiembre de 1998, Caso número ICTR-96-4-T, *Nicaragua*, *Tadić*, *Genocidio* (Bosnia y Herzegovina v. Serbia y Montenegro), Yeager v. Islamic Republic of Iran, Laudo No. 324-10199-, 2 de noviembre de 1987.
[298] Actividades Armadas en el Territorio del Congo, para. 102-113.
[299] *Genocidio* (Bosnia y Herzegovina v. Serbia y Montenegro), para. 430-434.
[300] Comentario General N. 3, Pacto Internacional de Derechos Económicos, Sociales y Culturales, E/1991/23, 14 de diciembre de 1990, para 10.
[301] Resolución del Consejo de Seguridad, S/RES/1373 (2001), 28 de setiembre de 2001. Resolución del Consejo de Seguridad, S/RES/1540 (2004), 28 de abril de 2004.
[302] TPIR, Fiscalía v. Jean Paul Akayesu, para. 432-445. Convenios Ginebra 1949. Protocolo Adicional II a los Convenios de Ginebra de 12 de agosto de 1949, 8 de junio de 1977.
[303] Cámara de Disputas del Suelo Marino de Tribunal Internacional de Derecho del Mar, Opinión Consultiva, para. 158.

gobernanza de contratistas involucrados con la explotación y exploración del suelo marino[304]. El Tribunal Internacional del Derecho del Mar acogió el estándar indicado por el Tribunal, en este caso en su opinión consultiva sobre la pesca ilegal, no reportada y no regulada, donde no contempló que no hubiera obligaciones comunes pero diferenciadas entre los Estados[305].

Otra área en donde no existen obligaciones diferidas, es en el caso de recursos jurídicos efectivos. La obligación de los Estados de mantener un cuerpo judicial competente, servicios policiales, cortes penales y tribunales para resolver disputas privadas es una obligación de resultado y la debida diligencia no tiene injerencia. Sin embargo, el hecho de que la investigación sea efectiva es una obligación de debida diligencia y los órganos del Estado deben ejercer sus responsabilidades de manera oportuna[306].

Derivado de lo antes expuesto, en el ámbito del ciberespacio se aplicaría un criterio subjetivo, en tanto las condiciones y las complejidades de los sistemas de los Estados exigirán un estándar diferenciado según sus capacidades. Esto, a su vez, se analizaría caso por caso en conjunto con los estándares anteriormente mencionados.

b) Aplicación de la obligación de debida diligencia en ciberataques

1. Consideraciones generales

En el ciberespacio deriva de la obligación general del Derecho Internacional de debida diligencia desarrollado en la sección anterior. Dicho concepto estipula que un Estado debe hacer todo lo necesario para prevenir cuáles acciones que emanen de su territorio, puedan vulnerar los derechos de otros[307], lo cual es de aplicación en el ciberespacio. En el contexto de la ciberseguridad ha sido definida como la revisión de la

[304] Ídem, paras. 158-159 y 161.
[305] Tribunal Internacional de Derecho del Mar, *Solicitud de Opinión Consultiva presentado por la Comisión Sub Regional de Pesqueros,* Opinión Consultiva, 2 de abril de 2015, paras. 125-129.
[306] *Kelly and others vs. Reino Unido,* Sentencia del 4 de agosto de 2001, Aplicación No. 30054/96, para 96.
[307] Annegret Bendiek, "Due Dilligence in Cyberspace", *Stiftung Wissenscharft und Politik German Institute for International and Security Affairs,* (2016):5, consultado el 19 de setiembre de 2016. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf.

gobernanza, los procesos y los controles usados para asegurar información, identificar y entender los riesgos posibles[308].

Las posibles reglas que regulen el ciberespacio siempre quedarán atrás, frente a los constantes desarrollos tecnológicos. Por tanto, resulta necesario recurrir a obligaciones como la debida diligencia, con el fin de evitar la perpetuación de actuaciones ilícitas y, en caso de que ocurran, determinar si existe o no responsabilidad de un Estado. Asimismo, la debida diligencia, como un estándar o concepto abierto, evita las dificultades que derivan de un acuerdo con reglas taxativas. Desarrollar un tratado o reglas específicas de aplicación requeriría consenso de los Estados, lo cual es extremadamente difícil o imposible de alcanzar[309], en especial en el contexto del ciberespacio.

La CIJ ha enfatizado en la importancia de aplicación de las reglas existentes de Derecho Internacional en la ausencia de reglas específicas, especialmente en razón del avance de las tecnologías[310].

Puesto que la debida diligencia deriva en forma directa del principio de soberanía, las obligaciones generales indicadas anteriormente son de aplicación al contexto del ciberespacio. El Grupo de Expertos Gubernamentales de las Naciones Unidas, ha reconocido que principios de Derecho Internacional emanados del principio de soberanía, resultan vinculantes en el contexto cibernético[311].

A pesar de que no existe un único estándar de debida diligencia, tal como se indicó supra, el mismo dependerá de la regla primaria en cuestión. Existen obligaciones que requieren un estándar más exigente, como por ejemplo la obligación de prevenir el crimen de genocidio[312]. De igual forma, surgen estándares más altos para obligaciones en actividades inherentemente peligrosas, así varía el estándar según el nivel de riesgo[313]. Esta

[308] Bendiek, 7.
[309] ILA, Second Report, 3.
[310] *Legalidad de la Amenaza o Uso de Armas Nucleares*, Opinión Consultiva, Reportes CIJ, 1996, para 39.
[311] Asamblea General, Resolución A/70/174, *Grupo de Expertos Gubernamentales en Desarrollo den el Campo de la Información y Tecnologías en el Contexto de Seguridad Internacional* (2015): para 27.
[312] Genocidio *(Bosnia y Herzegovina v. Serbia y Montenegro).*
[313] Cámara de Disputas del Suelo Marino de Tribunal Internacional de Derecho del Mar, Opinión Consultiva, para 117.

evaluación se aplica en el ámbito de las ciberoperaciones y los ciberataques; pues no todas las actuaciones son de la misma gravedad.

Un aspecto importante a considerar en el ámbito de la debida diligencia en el ciberespacio, es que la obligatoriedad cubre la participación de al menos tres partes: (i) el Estado objetivo de la ciberoperación; (ii) el Estado obligado a cumplir con la debida diligencia; (iii) un tercero que sea el autor de la ciberoperación[314]. Por lo tanto, la obligación aplica a cualquier tercero en una ciberoperación independientemente de si es llevado a cabo por una persona privada, corporación, agente no estatal o un Estado.

Asimismo, la obligación en el contexto de las ciberoperaciones y ciberataques aplica por medio del territorio soberano. La obligación incluye cualquier infraestructura cibernética usada para llevar a cabo la actividad, al igual que cualquier persona involucrada. En este sentido, es importante tomar en cuenta que la parte que lanza el ciberataque puede operar de manera remota por medio de un tercer Estado[315]. Por ejemplo, un *hacker* localizado en Estado A, el cuall lleva a cabo una operación destructiva contra el Estado B y usa la infraestructura del Estado C. Si el Estado C tiene conocimiento de la utilización de su infraestructura y omite tomar medidas razonables para darle fin a la operación, dicho Estado estaría violando la obligación de debida diligencia. Esta interpretación también se aplica extraterritorial en el tanto el Estado puede estar en control de un territorio en el exterior sobre el cual no ejerce soberanía, como es el caso de ocupación militar[316].

La obligación debe considerarse de igual forma bajo el supuesto de que la infraestructura de un Estado sea utilizada únicamente de tránsito para la operación, por ejemplo, información a través de un cable de fibra óptica. El Grupo Internacional de Expertos que desarrollaron el Manual de Tallin 2.0, consideran que el estado de tránsito, debe acoplarse a las mismas obligaciones de debida diligencia en tanto (i) tenga

[314] Tallinn 2.0, 32.
[315] Ídem.
[316] Comisión de Derecho Internacional, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, UN GOAR 56th Sess. Supp. No.10, UN Doc A/56/10 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf. Comentario al Art. 1, para 12.

conocimiento de una operación que se desarrolle el nivel requerido de daño potencial a otro; y, (ii) pueda tomar medidas viables para darle fin de manera efectiva[317].

A pesar de los criterios mencionados, dado el estado de los sistemas de comunicación en la actualidad, es poco probable que los Estados tengan conocimiento y puedan identificar tráfico malicioso transitando en su infraestructura. La firma del *malware* puede ser desconocida y no ser detectada por software antivirus o el *malware* puede estar encriptado[318]. Adicionalmente, el tráfico de internet por lo general pasa a través de infraestructura privada de proveedores de servicios de internet. La dificultad entonces es sobre el conocimiento que pueda tener el Estado, no sobre la existencia o no de la obligación de debida diligencia.

El conocimiento es un elemento constitutivo de la obligación, en el contexto del ciberataque se requerirá únicamente lo razonable en determinar responsabilidad. Como fue desarrollado en la sección anterior, el Estado debe actuar como un Estado razonable actuaría en esas circunstancias[319]. No es razonable exigirle a un Estado detectar una operación realizada a través de un *malware* desconocido. El estándar es más bien si la actuación de otro Estado equipado en forma similar, en el curso normal de eventos, hubiera detectado la operación. Asimismo, la obligación de debida diligencia no solo incluye omisión o inacción, sino que incluye no haber tomado las medidas suficientes razonables disponibles y practicables[320].

En relación con el daño, el artículo 2 de los AREHII, no requiere la comprobación de un daño para determinar la responsabilidad internacional del Estado. Por tanto, en el contexto de ciberataques, no resulta necesario que exista un daño físico a objetos o lesiones a individuos. Ejemplo de esto sería un ciberataque cuyo objetivo es la perturbación de banca en línea, medios de comunicación, funciones gubernamentales y del sector privado. El daño constituye violación a obligaciones de Derecho Internacional y aunque no haya daño físico, constituye una obligación del Estado y, por tanto, responsabilidad.

[317] Tallinn 2.0, 33.
[318] Ídem, 43.
[319] Ídem, 42.
[320] Tallinn 2.0, 43.

2. Otras consideraciones

Adicionalmente, resulta esencial aplicar la obligación de debida diligencia como medio para responsabilizar a los Estados por las consecuencias que puede traer optar por otro tipo de respuesta. Responder a ciberataques con contraataques automáticos y represalias por medio de actos digitales, sería extremadamente problemático. Primero, cualquier intención para atribuir responsabilidad en forma directa a un Estado por un ciberataque con la intención de responder con contra medidas, despierta una serie de preguntas técnicas, legales y políticas. Ciberdefensa activa puede provocar una carrera de armamento con riesgos incalculables para infraestructura crítica. Por eso, desde una perspectiva de debida diligencia, la estrategia debe ser una de disuasión. Por ejemplo, Alemania y la Unión Europea lideran con sus leyes de seguridad en tecnologías de la información y directiva de Red y Seguridad de Información (NIS, por sus siglas en inglés), creando infraestructura de comunicación e información resistente y en determinar estándares mínimos de seguridad en tecnologías de la información[321].

Los gobiernos deben resistir la tentación de reaccionar al incremento en ataques digitales y más bien deben construir nuevas armas digitales y de ofensiva. Varios Estados han tomado esta iniciativa de disuasión y defensiva sobre ofensiva, construyendo costumbre internacional en relación con la debida diligencia en el ciberespacio. Alemania es un ejemplo de un país que ha incorporado normas de debida diligencia en áreas estratégicas de su política cibernética internacional y políticas de ciberseguridad. La Unión Europea junto con la OTAN, conjuntamente han perseguido una estrategia defensiva en estas áreas[322].

Como fue mencionado supra, las obligaciones de debida diligencia deben esperarse de Estados que han sido atacados, al igual que aquellos en cuyo territorio los servidores o cables de datos utilizados están localizados. La exigencia de estos estándares depende entonces de la habilidad de los Estados en cuestión de ejercer influencia y sus capacidades en Tecnologías de Información y Comunicación.

[321] Bendiek, 10.
[322] Bendiek, 19.

La debida diligencia requiere que los Estados actúen de manera responsable, no solo entre sí, sino también en sus actividades internas. Los Estados deben procurar evitar caer en políticas de ofensiva en el ámbito cibernético. Una política de ofensiva no solo iría en contra de la obligación de debida diligencia, sino causaría la posibilidad de que los conflictos escalen sin medida y contribuiría a la proliferación de ciberataques.

El Gobierno Federal de Alemania, Estados Miembros de la Unión Europea y la Unión Europea misma, se adhieren en principio a la idea de debida diligencia, derivada de los estándares anteriormente mencionados de jurisprudencia de la CIJ. Esta norma obliga a los Estados a asegurar que ninguna acción originada de su territorio en tiempo de paz, viole los derechos de otros Estados[323].

La debida diligencia permite a la comunidad internacional usar el Derecho Internacional para que los Estados rindan cuentas por omisiones en hacer su infraestructura segura; por violar una obligación por negligencia al actuar, o por una falta de cooperación en proteger contra y solucionar ciberataques[324].

La Asamblea General de las Naciones Unidas ha llamado a los Estados a asegurar que sus leyes y prácticas eliminen puertos seguros para quienes utilicen, de manera criminal, las tecnologías de la información[325]. El Grupo de Expertos Gubernamentales de las Naciones Unidas, ha estudiado esta idea en su reporte final en el 2015 sobre el "Desarrollo en el Campo de la Información y Tecnologías en el Contexto de Seguridad Internacional" e indican que todos los Estados deben asegurar que sus territorios y, especialmente, sus sistemas de computadoras e infraestructura localizada en sus territorios o se encuentre bajo su control, no sea mal utilizado para ataques a infraestructura de otros Estados[326].

[323] Ídem, 7.
[324] Christian Shaller, *Internacional sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014 Berlin Stiftung Wissenschaft und Politik, (2014):* 25.
[325] Asamblea General, Resolución 55/63 *Combatiendo el uso Criminal de las Tecnologías de la Información,* A/RES/55/63 (22 de enero de 2001), art. 1(a).
[326] Asamblea General, Resolución A/70/174, *Grupo de Expertos Gubernamentales en Desarrollo den el Campo de la Información y Tecnologías en el Contexto de Seguridad Internacional* (22 de julio de 2015).

Capítulo III

Formas de exclusión de responsabilidad de los Estados por ciberataques

Sección I: eximentes de responsabilidad internacional de los Estados por ciberataques

Los supuestos de eximentes de responsabilidad son situaciones bajo las cuales un hecho internacionalmente ilícito da pie a un Estado atacado para que tome medidas en reacción al ataque que está recibiendo, sin tener responsabilidad internacional por ello. Ahora bien, cabe aclarar que un Estado que recurre a cualquier tipo de medida al considerar que entra en una de las eximentes de responsabilidad y se basa, para tomar la decisión, en su evaluación unilateral del contexto, lo hace bajo su propio riesgo y puede incurrir en responsabilidad por su propia conducta ilícita en caso de una evaluación incorrecta[327].

Seguidamente se analizarán algunos de los supuestos que corresponden a eximentes de responsabilidad.

i. Legítima defensa

La figura de legítima defensa se deriva de la obligación de los Estados al no uso de la fuerza, el cual es un principio que se encuentra contemplado en el artículo 2(4) de la Carta de Naciones Unidas, el cual establece que *"[l]os Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas"*.

Este artículo tiene como precedente el Tratado General de Renuncia a la Guerra, denominado Pacto de París o Pacto Briand-Kellog, de 27 de agosto de 1928, el cual fue firmado y ratificado una vez finalizada la Primera Guerra Mundial. Por medio de este Pacto, los Estados condenan el recurso a la guerra para solucionar controversias internacionales y

[327] Recopilación de Laudos Arbitrales. Acuerdo de servicios aéreos de 27 de marzo de 1946 entre los Estados Unidos de América y Francia. 16 de abril de 1938 y 11 de marzo de 1941. VOLUMEN III, 443.

renuncian a ella como instrumento de política internacional[328]. No obstante, este Pacto solo prohibió la guerra y dejó un vacío legal en cuanto a la ilicitud de otras formas de uso de la fuerza que no constituyeran propiamente una guerra y, entonces, es cuando en 1945 con la Carta de Naciones Unidas se establece la prohibición formal del uso de la fuerza, lo cual la volvió la piedra angular de esta obligación[329].

No obstante, la Carta no solo ofreció avance en el tema, pues contempló el derecho a la legítima defensa, uno de los derechos que se dejaron por fuera del Pacto mencionado. Es así como en el artículo 51 de la Carta se establece:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.

Según lo que dispone el artículo 2(4) de la Carta de Naciones Unidas, un ciberataque podría constituir un uso de la fuerza; pues si bien no puede comprometer la integridad territorial del Estado atacado, si afecta su independencia política, como se evidenció en el ejemplo antes mencionado de los ataques de Rusia a los Estados Unidos. Por lo tanto, si un ciberataque constituye un hecho internacionalmente ilícito, se puede encontrar en ambas partes del conflicto; por lo tanto, el ataque cometido desencadena una respuesta como legítima defensa, o bien, como la respuesta en legítima defensa que realizó el Estado, siempre que se dé bajo las circunstancias requeridas para considerarlo como tal.

---

328 James Crawford, *op. cit.* 745.

329 Actividades Armadas en el Territorio del Congo (*República Democrática del Congo v. Uganda*) Sentencia, Reportes CIJ 2005, para. 148.

Asimismo, al igual que en las demás situaciones eximentes de responsabilidad, un Estado no puede ir en contra de otras normativas que no acepten limitaciones o restricciones contenidas en Convenciones Internacionales, de las cuales los Estados formen parte, por ejemplo los Convenios de Ginebra o el Pacto de Derechos Civiles y Políticos, que no aceptan restricciones en todos los derecho y ha de cuidarse de violentar ninguno de estos al ejecutar un ciberataque; pues le podría generar responsabilidad internacional.

El artículo 51 tiene la particularidad de que se considera costumbre internacional el no comunicarle al Consejo de Seguridad la toma de las medidas que se ejecuta como legítima defensa[330], por lo tanto, un ciberataque realizado de manera inesperada en respuesta de un ataque y siempre que resulte necesario y proporcional[331], si podría perfectamente encajar como una medida de legítima defensa.

ii. Contramedidas en razón de un hecho internacionalmente ilícito

La CIJ estableció que una contramedida es justificada si tiene que cumplir ciertos requisitos. En primer lugar, una contramedida solo debe tomarse en respuesta a un hecho ilícito internacional anterior de otro Estado y, segundo, debe dirigirse contra el Estado atacante[332]. Esta posibilidad de tomar contramedidas y sus respectivas regulaciones se hallan en los artículos del 49 al 54 de AREHII.

Por su parte el artículo 49, es el numeral que establece objetivo y límites al indicar que:

> 1. El Estado lesionado solamente podrá tomar contramedidas contra el Estado responsable del hecho internacionalmente ilícito con el objeto de inducirlo a cumplir las obligaciones que le incumban en virtud de lo dispuesto en la

[330] *Nicaragua*, Sentencia, 200.
[331] *Legalidad de la Amenaza o Uso de Armas Nucleares*, 41. *Nicaragua*, Sentencia, 176.
[332] Gabcíkovo, 55.

segunda parte.

2. Las contramedidas se limitarán al incumplimiento temporario de obligaciones internacionales que el Estado que toma tales medidas tiene con el Estado responsable.

3. En lo posible, las contramedidas serán tomadas en forma que permitan la reanudación del cumplimiento de dichas obligaciones.

La Comisión de Derecho Internacional explica que, al tomar contramedidas, el Estado lesionado retiene por el momento el cumplimiento de una o más obligaciones internacionales que debe al Estado responsable y, por otro lado, el párrafo 2 del artículo 49 refleja este elemento. Aunque las contramedidas normalmente tomarán la forma del incumplimiento de una obligación única, es posible que una medida particular pueda afectar al cumplimiento de varias obligaciones en forma simultánea.

Por este motivo, el párrafo 2 se refiere a *"obligaciones"* en plural. Diferentes obligaciones coexistentes podrían verse afectadas por el mismo hecho. La prueba es siempre la de la proporcionalidad, exigida en el artículo 51 de AREHII; pues no se trata de que el Estado, el cual ha cometido un hecho internacionalmente ilícito, se convierta en el blanco de ninguna forma o combinación de contramedidas, de manera independiente de su gravedad o consecuencias. Además, en cuanto cese el hecho ilícito la contramedida debe acabar, no puede mantenerse ninguna medida más allá del tiempo necesario. La palabra *"temporario"* del párrafo 2, indica el carácter temporal o provisional de las contramedidas. Su objetivo es el restablecimiento de una condición de legalidad entre el Estado lesionado y el responsable[333].

Asimismo, al igual que en las demás situaciones eximentes de responsabilidad, como ya se mencionó con anterioridad, un Estado no puede ir en contra de otras normativas que no acepten limitaciones o restricciones; pues hay convenciones

[333] Comisión de Derecho Internacional, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*"*, 130.

internacionales que no aceptan restricciones en todos los derechos. Ejemplo de esto se encuentra en el artículo 50 de AREHII, el cual establece:

> 1. Las contramedidas no afectarán:
>
> > a) La obligación de abstenerse de recurrir a la amenaza o al uso de la fuerza, como está enunciada en la Carta de las Naciones Unidas;
> >
> > b) Las obligaciones establecidas para la protección de los derechos humanos fundamentales;
> >
> > c) Las obligaciones de carácter humanitario que prohíben las represalias;
> >
> > d) Otras obligaciones que emanan de normas imperativas del derecho internacional general.
>
> 2. El Estado que tome contramedidas no quedará exento del cumplimiento de las obligaciones que le incumban:
>
> > a) En virtud de cualquier procedimiento de solución de controversias aplicable entre dicho Estado y el Estado responsable;
> >
> > b) De respetar la inviolabilidad de los agentes, locales, archivos y documentos diplomáticos o consulares.

Es importante mencionar que los artículos de AREHII establecen el requerimiento de que el Estado lesionado, debe solicitar al Estado responsable de acuerdo con el artículo 43, cumpla las obligaciones que le incumben en virtud de la segunda parte, esto de previo a tomar contramedidas, así como notificar al Estado de la decisión de tomar contramedidas y ofrecerse a negociar con el mismo previo a iniciar con la toma de las medidas.

Ahora bien, para determinar si un ciberataque puede no generarle responsabilidad a un Estado por ser considerado contramedida, tiene que haber cumplido todo lo antes mencionado. Esto requiere que el ciberataque haya sido planeado para ser ejecutado en forma específica como una contramedida; pues se requieren pasos previos a su comisión con el Estado atacante para que cumpla a cabalidad con lo exigido por los AREHII y, solo en este supuesto, un ciberataque podría entrar como una contramedida, en caso contrario podría

verse como un hecho internacionalmente ilícito, como por ejemplo por la prohibición del uso de la fuerza.

iii. Fuerza mayor

Fuerza mayor es una de las posibles excluyentes de responsabilidad internacional y se trata de una situación en la cual el Estado en cuestión está obligado a actuar de manera no conforme con los requisitos de una obligación internacional que le incumbe[334].

Para estar en presencia de una situación de fuerza mayor, se deben cumplir tres supuestos: A) el acto de que se trate debe ser provocado por una fuerza irresistible o por un hecho imprevisto[335]; B) fuera del control del Estado interesado; y C) que hace que sea materialmente imposible realizar la obligación en las circunstancias de análisis[336].

La imposibilidad material de ejecución que dé lugar a un caso de fuerza mayor, puede derivarse de un suceso natural o físico (por ejemplo, cambios meteorológicos que puede desviar las aeronaves del Estado al territorio de otro Estado, los terremotos, las inundaciones o la sequía) o bien, de la intervención humana (como por ejemplo la pérdida del control sobre una parte del territorio del Estado como resultado de una insurrección o devastación de una zona por operaciones militares llevadas a cabo por un tercer Estado), o una combinación de ambas. Ciertas situaciones de coacción o coerción que impliquen la fuerza impuesta al Estado, también pueden constituir un caso de fuerza mayor si cumplen los diversos requisitos del artículo 23.

En particular, la situación debe ser irresistible, de modo que el Estado interesado no tiene posibilidad real de escapar de sus efectos. La fuerza mayor no incluye las circunstancias en las cuales el cumplimiento de una obligación se ha vuelto más difícil, por ejemplo, debido a alguna crisis política o económica. Tampoco cubre situaciones

[334] James Crawford, *op. cit., 205.*
[335] Cfr. Corte Permanente de Arbitraje, Concesión de los faros del imperio otomano (Francia vs. Grecia) 12 R.I.A.A. 155; 23 I.L.R. 659 (1956), 219-220.
[336] James Crawford, *op. cit.*, 295-297.

provocadas por el descuido o el incumplimiento del Estado de que se trate, aun cuando el perjuicio resultante sea accidental y no intencional[337].

Entonces, en un supuesto en donde hay dos Estados con una responsabilidad derivada de un tratado bilateral, en donde uno de los Estados le permite al otro que utilice ciertos servidores del país, pero estos son destruidos por un huracán, lo cual obliga al Estado afectado a no cumplir con su obligación, la fuerza mayor precluiría la responsabilidad del Estado afectado por el incumplimiento. No obstante, el Estado podría resultar responsable por no tomar las medidas necesarias para resguardar y hacer un respaldo de la información, bajo el conocimiento del peligro o las potenciales consecuencias del huracán anunciado, por ejemplo.

[337] Comisión de Derecho Internacional, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", 76 y 77.

Capítulo IV

Obligaciones derivadas de la Comisión de un hecho internacionalmente ilícito y su aplicación en ciberataques

Derivado de la comisión de un hecho internacionalmente ilícito, el Estado objeto de la violación está facultado para solicitar cesación o reparación del Estado responsable[338]. Dichas reglas derivan no solo de tratados, sino de la costumbre internacional[339]; por lo tanto, cualquier obligación en el Derecho Internacional está sujeto a los mismos parámetros. A continuación, se desarrollarán las obligaciones consecuencia de una violación al Derecho Internacional atribuible a un Estado y su aplicación en el ámbito de los ciberataques.

Sección I: cesación y no repetición

El artículo 30 de los AREHII determina, en virtud con la comisión de un hecho internacionalmente ilícito, dos elementos vinculados: cesación de una conducta ilícita y la garantía de no repetición por el Estado responsable[340]. Ambos resultan aspectos vinculados a restaurar o reparar la relación legal afectada por el ilícito. Por otro lado, la cesación se refiere a la obligatoriedad básica de cumplimiento con el Derecho Internacional[341], asegurarse el fin de que una conducta ilícita continúe, cesación es una obligación independiente requerida no como medio de reparación[342]. Por su lado, las garantías de no repetición, tienen una tarea preventiva y pueden ser descritas como un refuerzo positivo de acciones futuras[343].

[338] AREHII, Art. 28.
[339] Ejemplo es el caso de la obligación de permitir pasaje inocente de la Convención sobre Derecho del Mar. Para un Estado parte la obligación deriva directamente del tratado, pero para un Estado como los Estados Unidos de América, como no parte, la obligación deriva del derecho internacional en general.
[340] AREHII, Art. 30.
[341] James Crawford, *op. cit.*, 567.
[342] Ídem.
[343] Recopilación de Laudos Arbitrales. Caso relativo a las diferencias entre Nueva Zelanda y Francia, en relación con la interpretación y la aplicación de dos acuerdos, concluido el 9 de julio de 1986 entre los dos Estados y el cual está relacionado con el problema derivado del asunto *Rainbow Warrior*. 30 de abril de 1990 VOLUMEN XX pp. 215-284, p. 266. *Gabcikovo-Nagymaros,* paras. 125–127.

La referencia a *"actos"* incluye acciones y omisiones, por lo tanto, cesación es relevante para todos los hechos internacionalmente ilícitos independiente si la conducta del Estado es una acción o una omisión; pues puede haber acciones de abstenerse[344].

El tema de cesación usualmente se relaciona con el de reparación, en especial en temas de restitución. Muchas veces la cesación puede no ser distinguible de la restitución, como por ejemplo en el caso de liberar rehenes o devolver objetos confiscados. Sin embargo, ambos deben ser distinguidos. Contrario a restitución, cesación no está sujeto a límites de proporcionalidad. La dificultad de distinguir entre cesación y restitución está ejemplificada en el laudo arbitral de *Rainbow Warriror*[345].

La obligación respecto a la garantía de no repetición, se relaciona con restaurar la confianza en un vínculo continuo, no son necesarios en todos los casos y es un concepto más flexible que el de cesación. Usualmente, se solicitan cuando el Estado lesionado tiene razón para creer que la mera restauración de la situación anterior no los protege de manera satisfactoria[346].

Dichas garantías usualmente son verbales, o bien, pueden involucrar algo más, por ejemplo, medidas preventivas adoptadas por el Estado responsable, con el fin de evitar la repetición de la violatoria. La práctica internacional no es uniforme de acuerdo con la clase de garantías que pueden solicitar. El Estado dañado por lo general puede solicitar salvaguardias contra la repetición, sin especificar la forma en que deben de implementarse. En el caso *LaGrand,* la CIJ indicó: *"this obligation can be carried out in various ways. The choice of means must be left to the United States"*[347]. Asimismo, indicó que un Estado puede no estar en postura de asegurar no repetición, o garantía de que sea efectivo; sin embargo, esto depende de la obligación en específico.

---

[344] *Rainbow Warrior*, para.113.
[345] Ídem, para. 105.
[346] Comisión de Derecho Internacional. "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". Naciones Unidas Copyright, 2001. Consultado el 17 de febrero de 2016. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
[347] *LaGrand (Alemania v. Estados Unidos),* Reportes 2001, p.466, para. 125. *"Esta obligación puede ser llevada a cabo de varias maneras. La opción de los medios debe ser dejada a los Estados Unidos".* La traducción fue realizada por las autoras.

En el ámbito del ciberespacio, un Estado está obligado a cesar la actividad cibernética que esté causando un ilícito y evitar que el mismo continúe sucediendo en virtud de las consideraciones mencionadas supra. En este contexto, puede ser insuficiente que el Estado meramente asegure que cumplirá con obligaciones de, por ejemplo, debida diligencia en el futuro. Este Estado puede entonces estar en la necesidad de adoptar medios técnicos, operacionales y legislativos para asegurar que sus actividades maliciosas no vuelvan a ocurrir, como el valorar las vulnerabilidades en infraestructura explotada con anterioridad[348].

La obligación de asegurar no repetición no aplica en todas las circunstancias, únicamente en aquellas en donde el Estado perjudicado tiene preocupaciones razonables de que no será protegido. Como ejemplo, si un Estado utiliza de manera repetida ciberataques para violar la soberanía de otro Estado, el Estado perjudicado puede solicitar no solo cesación de la actividad, sino también garantías de que el Estado responsable respete de ahora en adelante la soberanía del Estado.

Sección II: reparaciones

La función de reparar el daño es, en la medida de lo posible, restablecer relaciones reflejadas en el *status quo ante.* La CPJI, en el caso de la *Fábrica de Chórzow*, declaró que:

> The essential principle contained in the actual notion of an illegal act-a principle which seems to be established by inter- national practice and in particular by the decisions of arbitral tribunals-is that reparation must, as far as possible, wipe out al1 the consequences of the illegal act and reestablish the situation which would, in al1 probability, have existed if that act had not been committed. Restitution in kind, or, if this is not possible, payment of a sum corresponding to the value which a restitution in kind would bear; the award, if need be, of damages for loss sustained which would not be covered

[348] Tallinn 2.0, 143.

> by restitution in kind or payment in place of it-such are the principles which should serve to determine the amount of compensation due for an act contrary to international law[349].

En este mismo sentido, el Tribunal Internacional de Derecho del Mar en el caso M/V Saiga indicó al citar el caso de Chorzow:

> It is a well-established rule of international law that a State which suffers damage as a result of an internationally wrongful act by another State is entitled to obtain reparation for the damage suffered from the State which committed the wrongful act and that "reparation must, as far as possible, wipe out all the consequences of the illegal act and reestablish the situation which would, in all probability, have existed if that act had not been committed" (Factory at Chorzów, Merits, Judgment No.13, 1928, P.C.I.J., Series A, No. 17, p. 47). [350]

Asimismo, en el caso de Mavrommatis, donde el daño fue sufrido por un nacional, la CPJI indicó: *"By taking up the case of one of its subjects and by resorting to diplomatic action or international judicial proceedings on his behalf, a State is in reality asserting its own rights - its right to ensure, in the person of its subjects, respect for the rules of*

---

[349] *Fábrica de Chórzow (Alemania vs. Polonia),* Demanda de Indemnización, Fondo, (1928) CPJI (Serie. A) No 17. 47. *"El principio esencial contenido en la noción actual de un acto ilegal -un principio que parece establecerse por costumbre internacional y en particular por las decisiones de tribunales arbitrales- es que la reparación debe, en la medida de lo posible, eliminar todas las consecuencias del acto ilegal y restablecer la situación que, en toda probabilidad, existiría si el acto no hubiera sido cometido. Restitución en especie, o, si no es posible, el pago de una suma correspondiente al valor que una restitución en especie tendría, el monto, de ser necesario, de daños por la pérdida sufrida que no estaría cubierta por la restitución en especie ni por pago en su lugar, son tales los principios que deberían servir para determinar el monto de compensación debido por un acto contrario al Derecho Internacional".* La traducción fue realizada por las autoras.

[350] Tribunal Internacional de Derecho del Mar, El Caso M/V "Saiga" (No. 2) (San Vicente y las Granadinas v. Guinea), Sentencia, 1 de julio de 1999, para. 170. *"Es una bien establecida regla de Derecho Internacional que un Estado que sufre de un daño como resultado de un hecho internacionalmente ilícito por otro Estado, está facultado para obtener reparación de los daños sufridos del Estado que cometió el acto ilícito y que 'la reparación debe, en la medida de lo posible, eliminar todas las consecuencias del hecho ilícito y restablecer la situación que, en toda probabilidad, hubiera existido si el acto no hubiera sido cometido'" (Factory at Chorzów, Merits, Judgment No.13, 1928, P.C.I.J., Series A, No. 17, p. 47)".* La traducción fue realizada por las autoras.

international law.[351]*"* De tal manera, se refuerza la posibilidad de los Estados de solicitar reparaciones, no solo por daños a sí mismo, sino representar las de sus nacionales por medio de protección diplomática.

La CIJ en el caso de *Barcelona Traction,* hizo referencia a la posibilidad de reparación en el caso de Estados que busquen vindicar intereses colectivos, como el caso de Derechos Humanos o el ambiente al definir: *"In view of the importance of the rights involved, al1 States can be held to have a legal interest in their protection; they are obligations erga omnes.*[352]*"*

El *"daño"* puede referirse a cualquier daño moral o físico causado por una operación cibernética ilícita[353]. Daño moral incluye daño a propiedad, o que afecte los intereses del Estado, el cual se pueda valorar en términos monetarios. La naturaleza y la extensión del daño resultan en especial relevantes para el tipo y monto de las reparaciones. La interferencia con ciberoperaciones o la pérdida de datos o información que resulte en pérdidas financieras, constituye un daño material[354]. La mera inconveniencia de acceso temporalmente perdido al internet, o pérdida de correspondencia personal que no tiene un impacto pecuniario, no es un daño material[355].

Daño moral se refiere a otras formas de daños relacionados con la dignidad o prestigio del Estado perjudicado[356]. Por ejemplo, un ciberataque que manipule información publicada por una página gubernamental que menoscabe la confianza en el gobierno, sería causal de daño moral.

---

[351] *Las concesiones Palestinas de Mavrommatis (Grecia vs. Reino Unido),* CPJI (Serie. A) No 2, 12.
[352] *Caso de Barcelona Traction, Light and Power Company, Limited (Bélgica v. España),* Reportes 1970, p.3, 33. *"En vista de la importancia de los derechos involucrados, se podría sostener que todos los Estados tienen un interés legal en su protección; son obligaciones erga omnes".* La traducción fue realizada por las autoras.
[353] AREHII, Art. 31.
[354] Tallinn 2.0, 144.
[355] Ídem, 145.
[356] AREHII, Art. 31, comentario paras. 5 y 7.

El daño que da pie a la reparación, no necesariamente puede ser determinado o cuantificado con facilidad. Esto es relevante, en especial en las operaciones cibernéticas; pues las consecuencias pueden ser difíciles de cuantificar. Por ejemplo, un DDoS contra el sistema de un banco del Estado puede perjudicar transacciones financieras que resulten en la pérdida de confianza del sector financiero del Estado[357]. A pesar de que la cuantificación del daño es difícil, el derecho de recibir reparación persiste.

Lo anterior es especialmente relevante en el contexto del ciberespacio, en virtud de que las consecuencias imprevisibles y remotas son muy probables[358]. La naturaleza interconectada de la infraestructura y actividades cibernéticas, pueden hacer difícil anticipar el impacto de un ciberataque. Por ejemplo, aunque ciertos *malware* pueden ser muy específicos para determinada ciberinfraestructura, otros tipos de *malware* son muy contagiosos y pueden extenderse con rapidez a otros sistemas[359].

Por tanto, derivado de los casos anteriores y en referencia a los artículos 28 y 34 de los AREHII, el Estado objeto de un ilícito internacional puede solicitar reparaciones. Estas deben ser íntegras del perjuicio causado por el hecho internacionalmente ilícito y pueden tener la forma de restitución, indemnización y satisfacción[360], ya sea de manera única o combinada. De continúo, se detallará cada una de estas formas de reparación.

i. Restitución

El artículo 35 de los AREHII, indican que un Estado responsable de un hecho internacionalmente ilícito está obligado a la restitución; es decir, a restablecer la situación que existía antes de la comisión del hecho ilícito, siempre y en la medida en que esa restitución: a) no sea materialmente imposible; b) No entrañe una carga desproporcionada en relación con el beneficio que derivaría de la restitución en vez de la indemnización[361].

[357] Tallinn 2.0, 145.
[358] Tallinn 2.0, 146.
[359] Tallinn 2.0, 146.
[360] AREHII, Art. 34.
[361] Ídem, Art. 35.

Solo si la restitución no es suficiente para remediar la situación causada por el Estado responsable del ilícito, se considerarán otras formas de reparación[362].

A pesar de lo establecido en el artículo, la aplicación práctica tiene gran dificultad, en especial en relación con el hecho de que restablecer la situación anterior al hecho ilícito resulta prácticamente imposible. Asimismo, la disposición de que las medidas no sean desproporcionales al beneficio derivado de la restitución en la práctica resultan dificultosas, máxime cuando por lo general implican la aplicación de medidas a nivel interno de los gobiernos.

Esta dificultad se ejemplifica en los casos de la CIJ de la *Orden de arresto del 11 de abril del 2000 (República Democrática del Congo v. Bélgica)* y *Avena.* En el caso de la *Orden de Arresto,* la Corte reconoció que una mera declaración de un ilícito bajo el Derecho Internacional es insuficiente y consideró que Bélgica estaba bajo la obligación de cancelar la orden de arresto emitida de manera ilegal[363]. Por otro lado, en el caso de *Avena* la Corte rechazó la solicitud de cancelación de la sentencia de muerte emitidas sin notificación o asistencia consular. Solo estableció que los Estados Unidos estaba bajo la obligatoriedad de proveer medidas de revisión y reconsideración de las sentencias emitidas en violación de la Convención de Viena de Relaciones Consulares[364].

En el caso de una ciberoperación, la restitución puede incluir proveer datos respecto al *malware* utilizado, para que el Estado perjudicado pueda neutralizar los efectos del *malware* en sus sistemas. Sin embargo, si la restitución es materialmente imposible, como el caso donde el daño causado por el ciberataque no pueda revertirse o si la ciberinfraestructura objeto de la operación fue destruida y no puede ser reemplazada, la compensación y la satisfacción serían los métodos apropiados[365].

---

[362] AREHII, Art. 25, comentario para 3.
[363] *Orden de arresto del 11 de abril del 2000 (República Democrática del Congo v. Bélgica),* Reportes CIJ 2002, p.3, 32.
[364] *Avena y otros Nacionales Mexicanos (México v. Estados Unidos de América), Sentencia, Reportes CIJ 2004, p. 12,* 60, 72.
[365] AREHII, Art. 35.a.

ii. Indemnización

De conformidad con el artículo 36 de los AREHII, el Estado responsable de un hecho ilícito a nivel internacional, está obligado a indemnizar el daño causado por ese hecho en la medida en que dicho daño no sea reparado por la restitución[366]. En ese sentido, la indemnización pecuniaria es por lo general la medida más apropiada y comúnmente utilizada para remediar el ilícito. La indemnización debe cubrir todo daño susceptible de evaluación financiera, incluido el lucro cesante en la medida en que este sea comprobado[367].

En el caso *Gabcikovo*, la CIJ reafirmó esta regla al determinar que el Estado perjudicado está facultado para recibir indemnización por parte del Estado que cometió el ilícito[368]. A pesar de que la Corte, en pocas ocasiones ha otorgado daños y perjuicios[369], ha sentado las bases para que se den este tipo de reparación en tribunales, tales como el Tribunal de Reclamos Irán-Estados Unidos, la Comisión de Compensación de la ONU y la Comisión de Reclamos Eritrea-Etiopía, al igual que tribunales de inversiones.

Ciertas dificultades se presentan en el cálculo de daños indirectos o daño moral, por lo tanto, los AREHII no lo regulan y se deja para análisis de cada caso.

En relación con el pago, los AREHII también mencionan la obligación de pagar intereses. El artículo 38 indica:

> Artículo 38
>
> 1. Se debe pagar intereses sobre toda suma principal adeudada en virtud del presente capítulo, en la medida necesaria para asegurar la reparación íntegra. La tasa de interés y el modo de cálculo se fijarán de manera que se alcance ese resultado.
>
> 2. Los intereses se devengarán desde la fecha en que debería haberse pagado

[366] AREHII, Art. 36.1.
[367] Ídem, Art. 36.2.
[368] *Gabcikovo*, 81.
[369] *Caso de Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo),* Méritos, Juzgamiento, Reportes CIJ 2012, p.324., para 56.

la suma principal hasta la fecha en que se haya cumplido la obligación de pago[370].

Para la determinación de la tasa de interés y el momento en el cual los mismos empiezan a correr, puede variar según la obligación. Esto puede estar determinado por medio de un tratado o contrato, o algunos tribunales han utilizado los parámetros del Derecho Internacional Privado y seleccionar tasas nacionales[371]. Recientemente, los tribunales han estado más dispuestos a otorgar intereses, incluso intereses compuestos[372].

La idea de indemnización es amplia y no solo incluye los daños al Estado; sin embargo, también a sus nacionales y compañías. Un DDoS contra un comercio que resulte en pérdidas es relativamente fácil de evaluar. Por tanto, cualquier daño resultado de una actividad ilícita por medio de un ciberataque o ciberoperación, puede ser cuantificable para efectos de establecer el monto de indemnización debido al Estado lesionado.

iii. Satisfacción

La satisfacción puede definirse como cualquier medida, la cual el Estado responsable está obligado por la comisión de un ilícito de conformidad con la costumbre internacional o por acuerdo entre las partes, además de restitución o indemnización cuando estas no sean posibles. Usualmente, corresponden a una muestra de arrepentimiento o reconocimiento del acto ilícito. Esta medida consigue tomar varias formas, las cuales pueden ser cumulativas[373].

El Artículo 37 de los AREHII indica:

1. El Estado responsable de un hecho internacionalmente ilícito está obligado a dar satisfacción por el perjuicio causado por ese hecho en la medida en que ese perjuicio no pueda ser reparado mediante restitución o indemnización.

[370] AREHII, Art. 38.
[371] James Crawford, *op. cit.*, 577.
[372] Diallo, para 56.
[373] James Crawford, *op. cit.*, 574.

2. La satisfacción puede consistir en un reconocimiento de la violación, una expresión de pesar, una disculpa formal o cualquier otra modalidad adecuada.
3. La satisfacción no será desproporcionada con relación al perjuicio y no podrá adoptar una forma humillante para el Estado responsable[374].

Los ejemplos indicados en el inciso segundo, son solo algunas posibilidades, la forma apropiada dependerá de las circunstancias, entre algunos ejemplos se puede incluir: la debida investigación sobre las causas del hecho que causó los daños, o acción penal o disciplinaria a los individuos encargados de la conducta que causó el ilícito[375]

Una de las formas más comunes de satisfacción es por medio de una declaración de ilicitud del acto por el tribunal o corte competente[376]. Este tipo de satisfacción fue afirmado por la CIJ en el caso de *Corfu*, donde la Corte, luego de determinar la ilegalidad de la operación de limpieza de minas llevado a cabo por el Reino Unido, indicó: *"To ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty. This declaration is in accordance with the request made by Albania through her Counsel, and is in itself appropriate satisfaction"*[377].

Existe práctica estatal en reclamos para solicitar satisfacción que pueden ser aplicables al contexto cibernético; por ejemplo, reclamos se han hecho en relación con insultos a la bandera, violaciones de soberanía y violación a instalaciones diplomáticas[378]. Por analogía un Estado podría reclamar por la deformación de un sitio de internet del Estado, violación a la soberanía por medio de un ciberataque o usar medios cibernéticos dirigidos a correspondencia diplomática[379].

---

[374] AREHII, Art. 37.
[375] Ídem, comentario para. 5.
[376] James Crawford, *op. Cit.*, 575.
[377] *Corfu*, 35. *"Para asegurar respeto por el derecho internacional, del cual este es un órgano, la Corte debe declarar que la acción de la Naviera Británica constituyó una violación a la soberanía de Albania. Esta declaración es de acuerdo con la solicitud hecha por Albania a través de su representación y es en sí misma satisfacción apropiada".* Traducción realizada por las autoras.
[378] AREHII, Art. 37, comentario para 4.
[379] Tallinn 2.0, 352.

VII. Conclusiones

Los ciberataques en la actualidad, representan un problema con el cual se enfrentan gobiernos, empresas e incluso individuos. La tecnología se ha vuelto la base de una gran cantidad de interacciones en la sociedad; negocios, medios sociales y de comunicación, e incluso plataformas estatales de servicios públicos. Por lo tanto, como consecuencia natural, la regulación del ciberespacio y las interacciones que en él se dan, resulta una necesidad.

Sin embargo, el Derecho, que se supone debe ofrecer respuesta a las necesidades actuales de la sociedad, no avanza lo suficientemente rápido o de manera efectiva para brindar respuesta a las interrogantes que surgen de las actividades lícitas e ilícitas llevadas a cabo en el ciberespacio. Por el contrario, la evolución en el mismo se dificulta por la divergencia de opiniones y concepciones que existen en la materia. Esta problemática tiene aún más presencia en el Derecho Internacional, pues una de las bases del mismo es el consentimiento de los Estados, requiriendo así, en muchos aspectos, cooperación en la elaboración y cumplimiento de la regulación pertinente. Es así, como el desarrollo de la normativa por concepto de responsabilidad internacional de los Estados, continúa evolucionando a la luz de nuevos campos de aplicación, como lo son el ciberespacio e incluso el espacio exterior.

El ámbito del ciberespacio por mucho tiempo se concibió como un área no regulable. Sin embargo, por medio de esfuerzos doctrinarios, se ha avanzado en el estudio de la normativa existente y su consecuente aplicación. A partir de esto, se han desarrollado interpretaciones que permiten aplicar la normativa existente a este campo y proporcionar alternativas a los Estados.

Como se mencionó anteriormente, un ciberataque corresponde al aprovechamiento de una deficiencia de un sistema, con el fin de interrumpir, alterar o destruir un anfitrión. Es esencial aclarar que, aunque los ciberataques normalmente se concebirían en contextos de conflictos armados, en donde el DIH resultaría aplicable, existen ciberataques en otros marcos o situaciones, que hacen necesario identificar las normas aplicables en estos escenarios.

Tal como se deriva de la hipótesis del presente trabajo, en el Derecho Internacional actualmente cuenta con las bases necesarias, en diferentes áreas, para establecer la responsabilidad internacional de un Estado por un ciberataque. Esto en virtud de los siguientes puntos conclusivos, los cuales derivan de los capítulos y las secciones esbozadas con anterioridad.

Uno de los ejes centrales de la normativa aplicable a la responsabilidad internacional de los Estados, es el análisis de la atribución del hecho internacionalmente ilícito. En el contexto de los ciberataques, la complejidad de los sistemas imposibilita la atribución directa a un Estado por la comisión del ilícito en contra de un sujeto de Derecho Internacional. En una operación cibernética, el origen, los autores, y los medios son extremadamente complejos, y en ocasiones imposibles, de identificar de manera certera, debido a todas las posibilidades existentes para burlar los sistemas de identificación y rastreo.

Sin embargo, por medio del análisis anteriormente realizado de la jurisprudencia de la CIJ, se llega a la conclusión de que es posible que la Corte determine, a través de medios indirectos, la responsabilidad internacional de un Estado por situaciones relacionadas al ciberespacio. Dicho análisis evidencia como, a través de los amplios estándares de admisibilidad y evaluación de la prueba, la CIJ ha analizado situaciones complejas en las cuales la atribución no es fácilmente asequible. Por tanto, se deriva la posibilidad de que los Estados recurran a la CIJ para el estudio de situaciones violatorias de obligaciones internacionales llevadas a cabo a través de un ciberataque. Los Estados pueden presentar una gran variedad de elementos probatorios para el análisis de la Corte, la cual, a su vez, tiene la posibilidad de utilizar peritos y solicitar prueba adicional para mejor resolver, de conformidad con sus amplias facultades.

A pesar de la demostrada dificultad probatoria en temas cibernéticos, la aplicación práctica de los mencionados estándares de la prueba y los poderes de la Corte, así como el marco legal y la jurisprudencia de la misma, evidencian la capacidad que tiene para

resolver este tipo de disputas, esta Corte Internacional. El gran conocimiento y la experiencia de este organismo internacional le permiten recibir, analizar y dar una solución, basada en los hechos y la evidencia, a la controversia jurídica que pueda generar un ciberataque, siempre en observancia del Derecho Internacional, la igualdad entre los Estados y el arreglo pacífico de controversias. De lo contrario, muchas obligaciones de Derecho Internacional quebrantadas por un sujeto de Derecho Internacional por la comisión de uno o varios ciberataques, quedarían impunes.

En cuanto al análisis realizado sobre la atribución de un ciberataque llevado a cabo por terceros a un Estado, cabe concluir que la CIJ puede llegar a determinar que el mismo es responsable por un hecho internacionalmente ilícito, cometido por una empresa privada, semiprivada o transnacional, o bien, por colaborar en la comisión de un ciberataque realizado por un grupo terrorista o insurgente, siempre que se cumplan con los requisitos analizados en capítulo respectivo. No obstante, no se debe olvidar que el principio general aplicable es que el Estado no es responsable por actos de grupos insurgentes o terroristas, o de aquellos con quien no se logre establecer un vínculo suficiente que genere su atribución. Por tanto, la responsabilidad atribuible a un Estado por actos de terceros, se limita a aquellas actuaciones del cual el Estado tuvo control o conocimiento de conformidad con los estándares expuestos y desarrollados anteriormente.

Los Estados tienen obligaciones que deben respetar para el buen entendimiento y el funcionamiento de las relaciones entre los miembros del Sistema Internacional y para colaborar con el mantenimiento de la paz. Uno de estos pilares que deben ser respetados, es la soberanía de los Estados. Ahora bien, así como es importante probar la atribución de un hecho, resulta esencial determinar la violación que se constituye por medio del ciberataque, y el tipo de obligación internacional quebrantada para establecer la existencia de un hecho internacionalmente ilícito derivado de su comisión. Es por esto que, del análisis realizado, se puede concluir que cada Estado goza de una soberanía en términos de jurisdicción a lo interno del país, y otra, en términos de igualdad entre Estados, y tal como se estableció, ambas soberanías deben ser respetadas según el Derecho Internacional. Es así como un ciberataque que comprometa los elementos cibernéticos que se encuentran en el territorio

de un país, o bien que intervenga en los asuntos internos del Estado, tal como se dio en el caso de Rusia-Estados Unidos y las últimas elecciones presidenciales, violentan la soberanía del mismo.

Obligaciones internacionales, tales como el respeto a la soberanía o la prohibición del uso de la fuerza, pueden derivar de muchas fuentes del Derecho Internacional, así como quedó demostrado desde la introducción del presente trabajo. Ahora bien, otra obligación que deben acatar los Estados derivada de la Costumbre Internacional, es la obligación de debida diligencia. Esta requiere que los Estados empleen un estándar de cuidado razonable, para evitar la comisión de un hecho ilícito a nivel internacional. Como fue indicado ampliamente en secciones anteriores, los Estados tienen la obligación de no permitir, de manera consciente, que su territorio sea utilizado para actos contrarios a los derechos de otros Estados. A pesar de que esta obligación ha sido desarrollada en distintos ámbitos como el derecho ambiental, el derecho internacional humanitario, el derecho del mar e incluso en temas de inversiones, la norma es aplicable de manera general en razón de ser costumbre. Por tanto, los Estados deben tomar todas las medidas que resulten razonables, entre los parámetros de los estándares mencionados, para evitar la comisión de un ciberataque que violente las obligaciones del Estado con la comunidad internacional, y evitar que su infraestructura cibernética sea utilizada para la ejecución de ciberataques en perjuicio de otros Estados.

A pesar de que esta obligación puede ser percibida como una amenaza a la soberanía del Estado, por concebirse como una medida inalcanzable o excesiva, la flexibilidad de la norma es por el contrario una ventaja para asegurar que exista mayor observancia y prevención contra la comisión de ciberataques. Asimismo, se debe rescatar que los estándares no son de aplicación uniforme a todos los Estados, pues sus capacidades y características particulares, son las bases para determinar si cumplieron o no con la obligación requerida, lo cual será analizado siempre, en el marco de lo razonable.

Es relevante resaltar que, de la mano de las causales para la atribución de responsabilidad internacional, encontramos las figuras eximentes de la misma. Estas

establecen posibilidades bajo las cuales, un ciberataque o el incumplimiento de una obligación relacionada con el ciberespacio, no cause la responsabilidad internacional de un Estado. Dentro del presente trabajo, se analizan tres de estas figuras excluyentes de responsabilidad, de las cuales se logra concluir que, si bien existen posibilidades de que el Estado no sea responsable por la comisión de un ciberataque o el incumplimiento de una obligación en temas de ciberespacio, los requerimientos de la mayoría de las figuras, son muchos y muy específicos, lo que genera un grado de riesgo elevado para que la Corte considere que pueden ser aplicadas a la situación bajo análisis.

Por lo tanto, puede concluirse que, aunque exista la posibilidad de excusar el quebranto de una obligación internacional, existe el riesgo de que un Estado interprete o actúe conforme a estas medidas, por considerar que se encuentra dentro de una de las situaciones eximentes de responsabilidad. Los Estados podrían tomar esa decisión, mediante una evaluación unilateral de la situación bajo su propio riesgo, ya que, al actuar de esta manera podrían incurrir en responsabilidad internacional por su propia conducta ilícita, en caso de una evaluación incorrecta, o bien en responsabilidad internacional por violentar alguna obligación por medio del ciberataque, que no pueda ser justificada o cubierta por la figura eximente de responsabilidad aplicada.

Finalmente, tal y como lo señala la jurisprudencia de la CIJ y los AREHII, un Estado que sufre un hecho internacionalmente ilícito en su contra, se encuentra facultado para solicitar la cesación, la garantía de no repetición y la correspondiente reparación, de conformidad con las reglas generales de la responsabilidad internacional. Los estándares existentes en el tema de reparaciones, resultan aplicables en los supuestos de ciberataques, y proporcionan así la última garantía a los Estados de encontrar respuesta a las violaciones sufridas por la comisión de un ataque cibernético en su perjuicio.

Es en razón de todo lo anterior, que debe resaltarse que, aún y cuando en el Derecho Internacional se encuentran las bases necesarias para la determinación de un ciberataque como hecho internacionalmente ilícito generador de responsabilidad internacional, las características propias de esta rama del Derecho, al igual que las complejas y particulares

tipologías del ciberespacio, hacen que la aplicación de dichas normas en temas de ciberataques, en la práctica, resulte particularmente desafiante. En primer lugar, los Estados víctimas de este tipo de violaciones, pueden no tener los medios o capacidades tecnológicas para recopilar la evidencia suficiente para probar que el ataque provino de un Estado en específico, o en su defecto, que el Estado tenía conocimiento y control sobre el ciberataque cometido y que por ende le resulten atribuibles los actos de terceros.

Otro obstáculo, es la posibilidad de que la CIJ admita una situación de esta naturaleza dentro de su competencia. La Corte, a pesar de contar con las herramientas y la experiencia necesarias para conocer situaciones complejas y determinar la responsabilidad o no de un Estado por considerar un ciberataque como un hecho internacionalmente ilícito, carece de la eficacia necesaria al no poseer competencia jurisdiccional obligatoria. Los procesos ante la CIJ a su vez, pueden resultar lentos por los retrasos de las partes litigantes, así como por las dificultades propias de los procesos, y puede no proporcionar las medidas correctivas necesarias en casos de ciberataques que requieran toma de medidas inmediatas.

A pesar de que la CIJ ha sido criticada por ser politizada en sus decisiones, ya sea en razón de la influencia de los Estados por parte del Consejo de Seguridad de las Naciones Unidas o incluso, por las influencias en los nombramientos de los jueces, este es uno de los órganos internacionales idóneos para dar una solución pacífica a estos conflictos y así evitar el posible levantamiento en armas de los Estados, incluso las cibernéticas, para defender su soberanía o el respeto a las obligaciones internacionales que un ciberataque puede quebrantar.

Asimismo, es importante rescatar que tribunales arbitrales o tribunales ad-hoc, pueden cumplir la misma función, ya que las reglas de responsabilidad internacional, debida diligencia, de eximentes de responsabilidad, e incluso reparaciones, son aplicables al ámbito de los ciberataques y deben ser referencia de los Estados para la resolución pacífica de este tipo de controversias de modo que se evite utilizar medidas que causen mayor tensión o conflicto. Los Estados deben procurar entonces, mantener ciertos estándares razonables de cuidado y control sobre su infraestructura cibernética para poder evitar la

comisión de ataques o proporcionar hábil respuesta en caso de que ocurran, todo en observancia de las bases normativas existentes, y así asegurar la estabilidad de la comunidad internacional.

VIII. Bibliografía

1. Convenciones internacionales

- Convención de Viena sobre el Derecho de los Tratados. U.N. Doc A/CONF.39/27 (1969), 1155 U.N.T.S. 331, Viena, 23 de mayo de 1969, entrada en vigor 27 de 1980.
- Convención de Viena sobre Relaciones Diplomáticas. Viena 18 de abril de 1961, entrada en vigor 24 de abril de 1964.
- Convención sobre Derechos y Deberes de los Estados. Aprobada en la séptima Conferencia de la Organización de Estados Americanos en Montevideo en diciembre de 1933.
- Convención de las Naciones Unidas sobre el Derecho del Mar. Adoptada el 10 de diciembre de 1982 en Montego Bay. Entrada en vigor el 16 de noviembre de 1994.
- Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes. Adoptada y abierta a la firma, ratificación y adhesión por la Asamblea General de Naciones Unidas en su resolución 39/46, de 10 de diciembre de 1984.
- Convención Interamericana contra el Terrorismo. Aprobada en la primera sesión plenaria de la Asamblea General de la Organización de Estado Americanos, celebrada el 3 de junio de 2002.
- Convenio sobre la Diversidad Biológica, 22 de mayo de 1992, entrada en vigor 29 de diciembre de 1993.
- Convención Marco de las Naciones Unidas sobre el Cambio Climático, GE.05-62220, 9 de mayo 1992.
- Convención de las Naciones Unidas de Lucha contra la Desertificación, A/AC.241/27, 12 de diciembre de 1994.
- Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, Resolución 34/180 18, diciembre 1979, entrada en vigor 3 Setiembre 1981.
- Convenios de Ginebra, 12 de agosto 1949.
- Convenio Internacional para la Represión de la Financiación del Terrorismo. Aprobado por la Asamblea General de Naciones Unidas en su resolución

A/RES/54/109 de 9 de diciembre de 1999 y abierta a la firma el 10 de enero de 2000. Entrada en vigor: 10 de abril de 2002 de conformidad con el artículo 26 (1).

- Declaración de Río sobre el Medio Ambiente y el Desarrollo. UN DOC A/CONF.151/26 (Vol. I) (12 agosto 1992)
- Declaración sobre la concesión de la independencia a los países y pueblos coloniales. Aprobada por la resolución 1514 (XV) de la Asamblea General de las Naciones Unidas el 14 de diciembre de 1960.
- Estatuto de la Corte Internacional de Justicia. *Anexo a la Carta de Naciones Unidas*, 26 de junio de 1945.
- Naciones Unidas, *Carta de las Naciones Unidas*, 1 UNTS XVI (24 de octubre de 1945).
- Pacto Internacional de Derechos Económicos, Sociales y Culturales, Asamblea General Resolución 2200 A (XXI), de 16 de diciembre de 1966.
- Protocolo Adicional I y II a los Convenios de Ginebra de 12 de agosto de 1949, 8 junio de 1977.
- Reglas de la Corte. Adoptadas el 14 de abril y en entradas en rigor el 1 de Julio de 1978.

2. Documentos de las Naciones Unidas

- Asamblea General, Resolución, RES 2222 (XXI) (1996), Declaración de los Principios Jurídicos que deben regir las Actividades de los Estados en la Exploración y Utilización del Espacio.
- Asamblea General, Resolución 55/63 *Combatiendo el uso Criminal de las Tecnologías de la Información,* A/RES/55/63 (22 de enero de 2001)
- Asamblea General, Resolución A/70/174, *Grupo de Expertos Gubernamentales en Desarrollo den el Campo de la Información y Tecnologías en el Contexto de Seguridad Internacional* (22 Julio 2015)
- Asamblea General, Resolución A/RE/54/109, Convenio Internacional para la Represión de la Financiación del Terrorismo, Aprobado por la Asamblea General de Naciones Unidas el 9 de diciembre de 1999, entrada en vigor 10 de abril de 2002.

- Asamblea General, Resolución 56/83, *Responsabilidad del Estado por hechos internacionalmente ilícitos,* A/RES/56/83 (28 de enero de 2002)
- Asamblea General, Resolución A/RES/55/25, *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* (8 enero 2001)
- Asamblea General, Resolución A/CN.4/L.778 30 de mayo de 2011, *Responsabilidad de las organizaciones internacionales.*
- Asamblea General, Resolución 62/61, *Responsabilidad de los Estados por hechos internacionalmente ilícitos, A*/RES/62/61 (8 enero de 2008)
- Asamblea General, Resolución 3314 (XXIX), *Definición del Crimen de Agresión.*
- Alto Comisionado de los Derechos Humanos, *La Responsabilidad Corporativa para respetar Derechos Humanos, una guía interpretativa (2012)*
- Comentario General N. 3, Pacto Internacional de Derechos Económicos, Sociales y Culturales, E/1991/23, 14 de diciembre 1990.
- Consejo de Seguridad. Resolución número 9, La Corte Internacional de Justicia. 15 de octubre de 1946, disponible en: http://www.un.org/es/sc/documents/resolutions/1946.shtml.
- Declaración relativa a los Principios de Derecho Internacional sobre las Relaciones Amistosas de 1970 (GA Res. 2625 (XXV)).
- Reporte del Representante Especial del Secretario General en el tema de derechos humanos y corporaciones transnacionales y otras empresas, John Ruggie, *Principios Guía en Negocios y Derechos Humanos, Implementando el Marco de las Naciones Unidas "Proteger, Respetar y Remedios",* UN DOC A/HRC/17/31, 21 de marzo de 2011.
- Resolución 2131 (XX) 1965, *Declaración sobre la Admisibilidad de la Intervención en los Asuntos Internos de los Estados y Protección de su Independencia y Soberanía.* A/RES/20/2131 (21 de diciembre de 1965)
- Resolución del Consejo de Seguridad, S/RES/1373 (2001), 28 de Setiembre de 2001.
- Resolución del Consejo de Seguridad, S/RES/1540 (2004), 28 de abril de 2004.

3. Normativa nacional de Costa Rica

- Asamblea Legislativa, Ley 24222 del 20 de diciembre de 1994. Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. Publicada en la Gaceta número 14 del 19 de enero de 1995.
- Asamblea Legislativa, Ley 8968 del 7 de julio de 2011. Ley de Protección de la Persona frente al tratamiento de sus datos personales. Publicada en la Gaceta número 170 del 5 de septiembre de 2011.
- Asamblea Legislativa, Ley 9072 del 20 de septiembre de 2012. Reforma Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. Publicada en la Gaceta No. 193 del 5 de agosto de 2012.

4. Documentos electrónicos

- Asociación Internacional de Abogados. "International Bar Association Rules on the Taking of Evidence in International Commercial Arbitrations". *International Bar Association*. Consultado el 23 de enero de 2017. http://www.ibanet.org/Document/Default.aspx?DocumentUid=68336C49-4106-46BF-A1C6-A8F0880444DC.
- Cassese, Antonio. "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia". European Journal of International Law, segunda edición (2007):666, consultado el 20 de febrero de 2017, http://www.ejil.org/article.php?article=233&issue=9.
- Clark, David D. y Susan Landau. "Untangling Attribution". Harvard Law School National Security Journal, Vol. 2, (2016), consultado el 4 de febrero de 2017, http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf
- Confederación Suiza, Manual sobre la aceptación de la jurisdicción de la Corte Internacional de Justicia: Modelo de cláusulas y formulaciones tipo, (2014), consultado el 23 de febrero de 2017,

https://www.eda.admin.ch/dam/eda/es/documents/publications/Voelkerrecht/handbook-jurisdiction-international-court_es.

- Colmegna, Pablo Damián. “Impacto de las normas de soft law en el Desarrollo del Derecho Internacional de los Derechos Humanos”. Revista electrónica del Instituto de Investigaciones “Ambrioso L. Gloja”, No. 8 (invierno 2012), consultado 18 de setiembre de 2016, http://www.derecho.uba.ar/revistagioja/articulos/R0008A006_0004_investigacion.pdf
- Comité Internacional de la Cruz Roja, *¿Qué limites impone el derecho de la guerra a los ataques cibernéticos?* Página oficial del Comité Internacional de la Cruz Roja, (2013), consultado el 5 de febrero de 2017, https://www.icrc.org/spa/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
- Comisión de Derecho Internacional. “Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries”. Naciones Unidas Copyright, 2001. Consultado el 17 de febrero de 2016. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
- Comisión de Derecho Internacional. “Draft articles on Prevention of Transboundary Harm from Hazardous Activities”. UN GOAR 56th Sess. Supp. No.10, UN Doc A/56/10 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf.
- Corte Internacional de Justicia. "Corte Internacional de Justicia". *Corte Internacional de Justicia*, Documentos en español. Consultado el 21 junio, 2016. http://www.icj-cij.org/homepage/sp/icjstatute.php.
- Crawford, James. “Proyecto de Artículos Sobre la Responsabilidad del Estado”. *United Nations Audiovisual Library of International Law*, 2009, consultado el 28 de junio, 2016. http://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_ph_s.pdf.
- CICR, "Geneva Conventions and Commentaries". International Committee of the Red Cross. 2016, consultado el 3 de setiembre de 2016. https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions.

- Deeks, Ashlee. "Tallinn 2.0 and a Chinese View on the Tallinn Process". *Lawfare, Hard National Security Choices*. 31 de mayo de 2015. Consultado el 8 de julio, 2016. https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.
- Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations - UN Documents: Gathering a Body of Global Agreements." A/RES/25/2625 Consultado el 04 de setiembre de 2016. http://www.un-documents.net/a25r2625.htm.
- Flemme, Maria. "Due Diligence in International Law." Master's thesis, Faculty of Law-University of Lund, 2004. 2005. Consultado en noviembre de 2016. http://lup.lub.lu.se/student-papers/record/1557482.
- French, Duncan, and Tim Stephens. "ILA Study Group on Due Diligence in International Law". Reporte. Due Diligence in International Law, International Law Commission. Consultado 2 julio de 2016. http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045.
- Grant, John P., y J. Craig Baker. "The Harvard Research in International Law: Contemporary Analysis and Appraisal". Library of Congress Cataloging-in-Publication Data, (2007). Consultado el 10 de julio de 2016. http://s1.downloadmienphi.net/file/downloadfile4/206/1392182.pdf.
- Hessbruegge, Jan. "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law". New York University Journal of International Law and Politics (JILP), Vol. 36, No. 4, (2004): 79, consultado el 16 de febrero de 2017, https://ssrn.com/abstract=2408953.
- Higgins, Rosalyn. "Speech by H.E. Judge Rosalyn Higgins President of the International Court of Justice." Speech, November 2, 2007. Accessed January 2016. http://www.icj-cij.org/presscom/files/3/14123.pdf.
- ILA Comittee Due Dilligence in International Law. "Due Diligence in International Law First Report". Study Groups - International Law Association. (2015). Consultado el 13 de enero de 2017. http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045.

- ILA Comittee Due Dilligence in International Law "Due Diligence in International Law Second Report." Study Groups - International Law Association. Julio, 2016. Consultado el 13 de enero de 2017. http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045.
- Koh, Harold Hongju. "International Law in Cyberspace." U.S. Department of State. Septiembre 18, 2012. Consultado el 7 de julio de 2016. http://www.state.gov/s/l/releases/remarks/197924.htm.
- Rubio Moraga, Angel L. "Historia e Internet: Aproximación al Futuro de la Labor Investigadora". Departamento de Historia de la Comunicación, Facultad de Ciencias de la Información, Universidad Complutense de Madrid. Consultado el 9 de febrero de 2017, http://pendientedemigracion.ucm.es/info/hcs/angel/articulos/historiaeinternet.pdf.
- Naciones Unidas. "Desarme, Naciones Unidas, ONU, Armas, Nuclear, Química, Biológica, Comisión De Desarme." UN News Center. Consultado el 3 de setiembre de 2016. http://www.un.org/es/disarmament/instruments/geneva.shtml.
- NATO Cooperative Cyber Defense Center of Excellence, *Centre is the first International Military Organization hosted by Estonia,* página oficial de NATO CCDCOE, (2008) consultada el 5 de febrero de 2017, https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html
- Schmitt, Michael. "International Law and Cyber Attacks: Sony v. North Korea". *Just Security*. 17 de diciembre de 2014. Consultado el 7 de junio de 2016. https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/
- Schmitt, Michael, and Liss Vihul. "The Nature of International Law Cyber Norms". *NATO CCD COE*, (2014). Consultado el 10 de julio de 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf.
- Schmitt, Michael. "In Defense of Due Diligence in Cyberspace." *The Yale Law Journal Forum,* 22 Junio de 2015. Consultado 7 julio de 2016. http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.

- Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law". *Berkeley Journal of International Law* 27, No. 1 (2009), 192-251. 2009. Consultado 3 junio de 2016. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil.
- "Treaties, States Parties, and Commentaries - Convention on the Prevention and Punishment of Genocide, 1948." Treaties, States Parties, and Commentaries - Convention on the Prevention and Punishment of Genocide, 1948. Consultado el 3, de setiembre de 2016. https://ihl-databases.icrc.org/ihl/INTRO/357?OpenDocument.
- "Tallinn Manual. Process". CCDCOE. 2014. Consultado el 08 de julio de 2016. https://ccdcoe.org/tallinn-manual.html.
- "Tallinn Manual Research." NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2014. Consultado el 08 de Julio, 2016. https://ccdcoe.org/research.html.
- Tikk, Eneken; Kadri Kaska y Liis Vihul. "International Cyber Incidents: Legal Considerations". *Cooperative Cyber Defence Centre of Excellence (CCD COE)*, (2010), consultado el 9 de febrero de 2017, https://ccdcoe.org/publications/books/legalconsiderations.pdf.
- United Nations Office for Outer Space Affairs. The Outer Space Treaty. Consultado el 03 de setiembre de 2016 http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html.
- "World Trade Organization". *WTO | Development - Who are the developing countries in the WTO?* Consultado el 21 de enero de 2017. https://www.wto.org/english/tratop_e/devel_e/d1who_e.htm.
- "World Trade Organization". *WTO | Understanding the WTO - least-developed countries*. Consultado el 21 de enero de 2017. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org7_e.htm.

5. Libros

- Barberis, Julio A. *Formación del derecho internacional.* Buenos Aires, Argentina: Editorial Ábaco de Rodolfo Depalma, 1994.
- Becker, Tal. *Terrorism and the State: Rethinking the Rules of State Responsability.* Oregon, Oxford y Portland: Hart Publishing, 2006.
- Brownlie, Ian. *System of the Law of Nations: State Responsibility*, Parte I. Oxford, Inglaterra: Clarendon Press, 1983.
- Boebert, W. Earl. ***A*** *Survey of Challenges in Attibution, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C., Estados Unidos: The National Academies Press, 2010.
- Caron, David D. "The basis of responsibility: attribution and other trans-substantive rules", *The Iran-United States Claims Tribunal: Its Contribution to the Law of State Responsibility*, R. B. Lillich y D. B. Magraw, eds. Irvington-on-Hudson, Nueva York, Estados Unidos: Transnational, 1998.
- Crawford, James. *Brownlie's Principles of Principles of Public International Law*. Oxford, Reino Unido: Oxford University Press, 2012.
- Crawford, James. *State Responsibility: The General Part*. New York, Estados Unidos: Cambridge University Press, 2013.
- De la Cueva y de la Rosa, Marco. *Teoría General del Estado. Apuntes de las clases impartidas por ilustres juristas del siglo XX.* México: Suprema Corte de Justicia de la Nación, 2014.
- Hobbes, Thomas. *El Leviatán. O la materia, forma y poder de una república eclesiástica y civil.* México: Fondo de Cultura Económica, 2010.
- M, Shaw. *International Law.* Cambridge, Inglaterra: Cambridge University Press, 2008.
- Sáenz Carbonell, Jorge Francisco. *Elementos de la Historia del Derecho*. San José, Costa Rica: ISOLMA, 2009.
- Schmitt, Michael N. *Tallinn Manual 2.0 on the international law applicable to cyber operations.* Cambridge, United Kingdom: Cambridge University Press, 2017.

- Ross, Alec. *The Industries of the Future.* New York, Estados Unidos: Simon & Schuster, 2016.
- Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York, Estados Unidos: Cambridge University Press, 2013.
- Varela Quirós, Luis A. *Las Fuentes del Derecho Internacional.* Bogotá, Colombia: Temis, 1996.
- Vargas Carrero, Edmundo. *Introducción al derecho internacional.* San José, Costa Rica: Juricentro, 1979.

6. Artículos

- Apple, James G. "General Principles of International Law", *International Judicial Monitor* 2, No. 2 (julio/agosto 2007). Consultado 17 de setiembre de 2016. http://www.judicialmonitor.org/archive_0707/generalprinciples.html.
- Bendiek, Annegret. "Due Dilligence in Cyberspace", *Stiftung Wissenscharft und Politik German Institute for International and Security Affairs*, (2016), consultado el 19 de setiembre de 2016, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf.
- Clark, David D. y Susan Landau, "Untangling Attribution", Harvard Law School National Security Journal, Vol. 2, (2016), consultado el 4 de febrero de 2017, http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf.
- Finklea, Kristin, y Catherine A. Theohary. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement". *Congressional Research Service* (enero 2015).
- González Campos, Julio D; Sánchez Rodríguez Luis I; Sáenz de Santamaría, Paz Andrés, "Curso de Derecho Internacional Público", Segunda Edición Revisada, Editorial Civitas, (Madrid 2002).

- Reisman, Michael W, y Eric E. Freedman. “The Plaintiff’s Dilema: Illegally obtained Evidence and Admissibility in International Adjudication”. *Yale Law School Legal Scholarship Repository*. Paper 730. (1982). http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1722&context=fss_papers.
- Roscini, Marco. "Digital Evidence as a Means of Proof before the International Court of Justice". *Journal of Conflict & Security* 21, No. 3 (2016), 541-554, consultado 11 enero de 2017. doi:10.1093/jcsl/krw016.
- Sharf, Michael P. y Margaux Day. “The International Corurt of Justice’s Treatment of Circumnstantial Evidence and Adverese Inferences” *Chicago Journal of International Law*. Vol. 13. No 1. Artículo 6. 1º de junio de 2012. http://chicagounbound.uchicago.edu/cjil/vol13/iss1/6.
- Shaller, Christian. “Internacional sicherheit und Völkerrecht im Cyberspace”. *SWP-Studie 18/2014, Berlin Stiftung Wissenschaft und Politik. (2014).*
- Tomka, Peter, y Vincent-Joel Proulx. "The Evidentiary Practice of the World Court". *NUS Law Working Paper Series*, Working Paper 2015/010, (2015). http://law.nus.edu.sg/wps/pdfs/010_2015%20_Vincent-Joel%20Proulx_Tomka.pdf
- Valencia-Ospina, Eduardo. "Evidence before the International Court of Justice". *International Law FORUM du droit international* 1, No. 4 (November 1999).

7. Artículos periodísticos

- BBC Mundo, “Alertan sobre virus que puede apagar fábricas”. *BBC Mundo*, 24 de septiembre de 2010, sección Tecnología, versión en línea, consultado el 10 de junio de 2016, http://www.bbc.com/mundo/ciencia_tecnologia/2010/09/100924_1043_virus_gusano_malware_stuxnet_iran_dc.shtml.
- BBC Mundo, “Virus infecta planta nuclear iraní”. *BBC Mundo*, 26 de septiembre de 2010, sección Internacional, versión en línea, consultado el 10 de julio de 2016, http://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw.shtml.

- David E. Sanger, "Obama order sped up wave of cyberattacks against Iran". *New York Times*, Middle East, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
- Esther Mucientes, "Asi se gestó el ataque más grave de los últimos 10 años", El Mundo, Tecnología, 22 de octubre de 2016, Madrid, versión en línea, consultado el 9 de febrero de 2017, http://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html.
- Guillén, Beatriz; Joan Faus y Rosa Jiménez Cano, "Varios ciberataques masivos inutilizan las webs de grandes compañías". *El País*, Tecnología, 22 de octubre de 2016, Madrid, Washington, San Francisco, versión en línea, consultado el 9 de febrero de 2017, http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html
- John Markoff, "Before the gunfire, Cyberattacks". *New York Times*, 12 de agosto de 2008, Tecnología, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
- Steven Lee Mayers, "Cyberattack on Estonia stirs fear of 'virtual war'". *New York Times*, 18 de mayo de 2007, Europa, versión en línea, consultado el 10 de julio de 2016, http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html.

8. Jurisprudencia

a. Sentencias y opiniones consultivas de la Corte Internacional de Justicia

- *Actividades Armadas en el Territorio del Congo (República Democrática del Congo v. Uganda),* Sentencia, Reportes CIJ 2005.
- *Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos de América),* Sentencia, Reportes CIJ, 1986.

- *Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. Estados Unidos de América),* Jurisdicción y Admisibilidad, Reportes CIJ, 1984.
- *Agentes Diplomáticos y Consulares Estadounidenses en Teherán (Estados Unidos v. Irán),* Sentencia, Reportes CIJ, 1980.
- *Aplicación de los Acuerdos Interinos del 13 de Setiembre de* 1995 (La Antigua República Yugoslava de Macedonia v. Grecia), Sentencia, 5 diciembre 2011. Reportes CIJ 2011.
- *Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina v. Serbia y Montenegro),* Sentencia, Reportes CIJ, 2007.
- *Avena y otros Nacionales Mexicanos (México v. Estados Unidos de América), Sentencia, Reportes CIJ 2004, p. 12.*
- *Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo),* Sentencia, Reportes CIJ 2012, p.324.
- *Ahmadou Sadio Diallo (República de Guinea v. República Democrática del Congo),* Compensación, Sentencia, Reportes CIJ 2010.
- *Barcelona Traction, Light and Power Company, Limited (Bélgica v. España),* Reportes 1970.
- *Canal de Corfu (Reino Unido v. Albania),* Méritos, (1949) CIJ.
- *Caso en relación a la soberanía sobre Pedra Branca/Pulau Batu Puteh, Rocas Medias y Borde del Sur (Malasia v. Singapur), Juzgamiento del 23 de mayo de 2008. Reportes CIJ, 2008.*
- *Caso de Pruebas Nucleares (Nueva Zelandia v. Francia),* Juzgamiento, Reportes CIJ, 1974.
- *Caza de Ballenas en la Antártida (Australia v. Japón: interviniendo Nueva Zelanda),* Juzgamiento, Reportes CIJ, 2014.
- *Caso África Sur-Oeste (Ethiopia v. Africa del Sur)*, Segunda Fase, Sentencia, Reportes CIJ, 1966.
- *Caso Relacionado a la Soberanía sobre Palau Ligitan y Palau Sipadan (Indonesia v. Malasia),* Sentencia, Reportes CIJ 2002.

- *Ciertas Actividades llevadas a cabo por Nicaragua en la Zona Fronteriza y Construcción a lo largo del Río San Juan (Nicargua v. Costa Rica)*, Juzgamiento del 16 de diciembre 2015.
- *Conformidad de la Declaración Unilateral de Independencia de Kosovo con el Derecho Internacional*, Opinión Consultiva. Reportes CIJ, 2010, p. 403.
- *Derechos de los Nacionales de los Estados Unidos de América en Marruecos*, Sentencia, 27 de agosto de 1952, Reportes CIJ 1952.
- *Delimitación Marítima del Mar Negro (Romania v. Ukrania)* Juzgamiento. Reportes CIJ.
- *LaGrand (Alemania v. Estados Unidos)*, Reportes CIJ, 2001, p. 466.
- *Legalidad de la Amenaza o Uso de Armas Nucleares*, Opinión Consultiva, Reportes CIJ, 1996.
- *Reparaciones por daños sufridos al servicio de Naciones Unidas*, Opinión Consultiva, Reportes CIJ, 1949.
- *Orden de arresto del 11 de abril del 2000 (República Democrática del Congo v. Bélgica)*, Reportes CIJ 2002.
- *Oro Monetario Removido de Roma en 1943 (Italia v. Francia, Reino Unido de Gran Bretaña y el Norte de Irlanda, y Estados Unidos de América)*, Orden del 3 de noviembre, 1953, Reportes CIJ 1953.
- *Proyecto Gabcikovo-Nagymaros (Hungría/Slovakia)*, Juzgamiento, Reportes CIJ, 1997.
- *Pulp Mills en el Río Uruguay (Argentina v. Uruguay), Juzgamiento, Reportes CIJ 2010.*
- *Fisheries (Reino Unido v. Noruega)* Reportes CIJ, 1951. Opinión disidente Juez Read.
- *Templo de Preah Vihear (Camboya v. Tailandia)*. Excepciones Preliminares, Reportes CIJ, 1961.

b. Sentencias de la Corte Permanente de Justicia Internacional

- *Concesiones Palestinas de Mavrommatis (Grecia vs. Reino Unido),* Sentencia, CPJI (Serie. A) No 2.
- *Fábrica de Chórzow (Alemania vs. Polonia),* Demanda de Indemnización, Fondo, (1928) CPJI (Serie. A) No 17.
- *Fábrica de Chórzow (Alemania vs. Polonia),* Competencia, (1927) CPJI (Serie. A) No 9.
- *Fosfato en Marruecos*, objeciones preliminares, (1938) CPJI (ser A/B) No. 74.
- *SS Lotus* (Francia v. Turquía) (1927) CPJI (Serie. A) No 10.

c. Laudos arbitrales

- Tribunal Arbitral, Caso de Reclamos Británicos en la Zona Española de Marruecos, Laudo Arbitral (1925).
- Recopilación de Laudos Arbitrales. Caso *Trail Smelter* (Estados Unidos Vs. Canadá). 16 de abril de 1938 y 11 de marzo de 1941. VOLUMEN III pp. 1905-1982.
- Recopilación de Laudos Arbitrales, Comisión de Reclamos Eritrea-Ethiopia – Laudo Parcial: Frente Principal –Reclamos de Eritrea 2, 4, 6, 7, 8 & 22. 28 de abril 2004 VOLUMEN XXVI pp. 115-153.
- Recopilación de Laudos Arbitrales. Reclamos de Alabama de los Estados Unidos de América v. Gran Bretaña. Laudo Arbitral del 14 de Setiembre de 1872. VOLUMEN XXIX, pp.125-134.
- Recopilación de Laudos Arbitrales. Caso Isla de Palmas (Países Bajos, Estados Unidos). 4 de abril 1928. VOLUMEN II pp. 829-871.
- Recopilación de Laudos Arbitrales. Caso relativo a las diferencias entre Nueva Zelanda y Francia en relación a la interpretación y aplicación de dos acuerdos, concluido el 9 de Julio de 1986 entre los dos Estados y el cual está relacionado con el problema derivado del asunto *Rainbow Warrior.* 30 de abril de 1990 VOLUMEN XX pp. 215-284.

d. Corte Interamericana de Derechos Humanos

- *Albán Cornejo y otros. vs. Ecuador*. Fondo, Reparaciones y Costas. Sentencia del 22 de noviembre de 2007. Serie C No. 171.
- *Cantoral Huamaní y García Santa Cruz vs. Perú*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia del 10 de julio de 2007. Serie C No. 167.
- *Espinoza Gonzáles Vs. Perú*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 20 de noviembre de 2014. Serie C No. 289.
- *Masacre de Mapiripán vs. Colombia*. Fondo, Reparaciones y Costas. Sentencia del 15 de septiembre de 2005. Serie C No. 134.
- *Masacre de Pueblo Bello vs. Colombia.* Fondo, Reparaciones y Costas. Sentencia del 31 de enero de 2006. Serie C No. 140.
- *Velásquez Paiz y otros Vs. Guatemala*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 19 de noviembre de 2015. Serie C No. 307.
- *Velásquez Rodríguez vs. Honduras*. Fondo. Sentencia del 29 de julio de 1988. Serie C No. 4.
- *Yvon Neptune vs. Haití*. Fondo, Reparaciones y Costas. Sentencia del 6 de mayo 2008. Serie C No. 180.

e. Corte Europea de Derechos Humanos

- *Adali vs. Turquía*, Sentencia del 31 de marzo de 2005, Aplicación No. 38187/97.
- *Al-Skeini vs. Reino Unido*, Sentencia del 7 de julio de 2011. Aplicación No. 55711/07.
- *Kiliç vs. Turquía*, Sentencia del 28 de marzo de 2000, Aplicación No. 22492/93.
- *Osman vs. Reino Unido*, Sentencia del 28 de octubre de 1998, Reportes de sentencias y Decisiones 1998-VIII.
- *Kelly y otros vs. Reino Unido*, Sentencia del 4 de agosto de 2001, Aplicación No. 30054/96.

f. Tribunal Penal Internacional para la Antigua Yugoslavia

- TPIY, Sala de Apelaciones, *Tadić*, 15 de julio de 1999 (Caso no. IT-94-1-A).

g. Tribunal Penal Internacional para Ruanda

- TPIR, Fiscalía v. Jean Paul Akayesu, 2 de setiembre de 1998 (Caso número ICTR-96-4-T).

h. Tribunal de Reclamos Irán-Estados Unidos

- *Petrolane, Inc. Vs. el Gobierno de la República de Irán*, Irán- Estados Unidos. C.T.R., vol. 27.
- Yeager v. Islamic Republic of Iran, Laudo No. 324-10199-, 2 de noviembre, 1987.

i. Tribunal Internacional de Derecho del Mar

- Cámara de Disputas del Suelo Marino del Tribunal Internacional de Derecho del Mar, *Responsabilidades y Obligaciones de los Estados Patrocinando Personas y Entidades Respecto a las Actividades en el Área,* Opinión Consultiva, 1 febrero 2011.
- Tribunal Internacional de Derecho del Mar, *Solicitud de Opinión Consultiva presentado por la Comisión Sub Regional de Pesqueros,* Opinión Consultiva, 2 de abril de 2015.
- Tribunal Internacional de Derecho del Mar, El Caso M/V "Saiga" (No. 2) (San Vicente y las Granadinas v. Guinea), Sentencia, 1 de julio de 1999.

j. Centro Internacional para de Arreglo de Diferencias Relativas a Inversiones (CIADI)

- CIADI, *Asian Agricultural Products LTD. (AAPL) v. República de Sri Lanka*, Caso No. ARB/87/3, Laudo Final, 27 de junio de 1990.
- CIADI, *Wena Hotels Ltd. v. República Árabe de Egipto*, Caso No. ARB/98/4, Laudo, 8 de diciembre de 2000. http://www.italaw.com/sites/default/files/case-documents/ita0902.pdf.

9. Otros

- Restatement (Third) of Foreign Relations Law of the United States §442(2)(c)2009.
- Comisión de Derecho Internacional, Principios rectores de las declaraciones unilaterales de los Estados, 2006.

IX. Anexos

Anexo 1- Resolución 1373 del Consejo de Seguridad de Naciones Unidas