CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C.

LOS DESAFÍOS DEL DERECHO INTERNACIONAL PÚBLICO EN LA ERA DIGITAL

T E S I N A

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN DERECHO

PRESENTA

ALESSANDRA BARZIZZA VIGNAU

DIRECTOR DE LA TESINA:

DR. JOSÉ ANTONIO CABALLERO JUÁREZ

CIUDAD DE MÉXICO **NOVIEMBRE, 2018**

A mi mamá Eugenia, a mi papá Massimo y a mi hermano Luca

por ser el principio, razón y fin de mi existencia.

AGRADECIMIENTOS

Quiero agradecer a todas las personas que han influenciado mi formación como ser humano, como estudiante y como profesionista. Sin duda su presencia y apoyo ha sido parte esencial en el proceso de cumplimiento de mis metas.

A mi mamá, por la formación diversa y humana que me has dado a lo largo de mi vida y enseñarme lo que implica ser, precisamente, humano.

A mi papá, porque a través de tu confianza aprendí a confiar en mí misma. Has sido, eres y serás siempre mi otra mitad.

A Luca, por tu amor incondicional, tu paciencia, interés, entusiasmo y apoyo en todos mis proyectos. No sé qué haría sin ti.

A mi Nonno y a mi Nonna Barzizza, por su apapacho y eterna ternura, por hacerme sentir siempre única.

A mi abuelo Armando Vignau, porque eres ejemplo y parámetro de ética y honestidad profesional.

A Gaby, por tu cariño, entusiasmo, apoyo y paciencia. Funges un rol muy importante.

A Lina, por las grandes oportunidades y el mundo profesional que me has abierto, por escuchar mis inquietudes.

A Moni, por tu paciencia y dedicación en mi formación profesional.

A Sebas, por las excelentes recomendaciones y libros, que sin duda contribuyeron en el planteamiento y culminación de este trabajo.

A Juan y Alan, por todo el cariño, aprendizaje, risas y buenos momentos. Con ustedes aprendí el valor y significado de hacer equipo.

A mis profesores José Antonio Caballero y Javier Cruz Angulo, por su constante apoyo y confianza y por dar las clases más interesantes y divertidas. Prometo seguir siempre cuestionándome dónde está la pared más dura del CIDE.

A mis profesoras María Solange Maqueo, Jimena Moreno y Mercedes Albornoz, por todo el apoyo que me han brindado durante y después de la carrera, por aconsejarme e impulsar y aplaudir mi pasión por la tecnología. Cada vez que visito el CIDE me siento como en casa.

A mis primas, primos, tíos y tías Vignau, porque junto a ustedes aprendí sobre el amor tan grande e incondicional que se puede encontrar en medio de la ironía y el sarcasmo. Son y seguirán siendo siempre un motor de avance en tiempos adversos.

A Quirarte, por toda la protección, cariño y compañía que me brindaste cuando más lo necesité. Te quiero eterna e incondicionalmente.

A mis amigos Millo, Gabriel, Diego, Billy, Iñigo y Lalo, por ser siempre la compañía más divertida. Por todas las carcajadas y su interminable cariño y lealtad.

A mis amigas, Pau, So, Vicky, Silvia, Alexa, Luisa, Ale Moreira, Anny, Jessy, Natalia y Anya, por todas las experiencias compartidas antes, durante y después de mi carrera. Por comprender mis ausencias.

A mi equipo Jessup, Raúl, Irene y Priscila, junto a ustedes viví las mejores experiencias de mi carrera.

A mi coach Ana, cuya toma de decisiones eventualmente conllevó al inicio de mi pasión por la tecnología. Por todo el apoyo y consejos que has seguido dándome durante todos estos años, a pesar de ya no ser mi coach. Te quiero mucho. ¡Gracias!

A mi equipo del Concurso Nacional de Derecho Constitucional, Claudia, Alejandro y Ricardo, porque la experiencia que vivimos "sí es de compas".

ÍNDICE

LISTA DE ABREVIATURAS

AEPD:	Agencia Española de Protección de Datos
CIJ:	Corte Internacional de Justicia
CNIL:	Comisión Nacional de Informática y Libertades
CJUE:	Corte de Justicia de la Unión Europea
CLOUD:	Clarifying Lawful Overseas Use of Data
GDPR:	General Data Protection Regulation
LICRA:	Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France
TIC:	Tecnologías de la Información y la Comunicación
TPIY:	Tribunal Penal Internacional para la Ex Yugoslavia
TJUE:	Tribunal de Justicia de la Unión Europea
UEJF:	L'union des Etudiants Juifs De France

INTRODUCCIÓN

En junio de 2010 un evento sin precedentes cambió para siempre la forma en la que percibimos el mundo: Estados Unidos e Israel destruyeron las centrifugas de enriquecimiento de uranio de una planta nuclear en Irán.

Después de leer estas primeras líneas, seguramente la primera duda que le surge al lector es: ¿por qué llamar a este suceso "un evento sin precedentes"? El hecho es lamentable, pero parece no ser novedad. Esto es verdad. Sin embargo, lo que resulta aterrador y al mismo tiempo intrigante es el medio a través del cual la planta nuclear fue destruida: un ciberataque actualmente denominado Stuxnet.

Stuxnet no solamente implicó un uso ilegal de la fuerza por parte de Estados Unidos e Israel en contra de Irán que pudo haber desatado un grave conflicto internacional entre, cuando menos, esas tres naciones, sino un cambio permanente en la forma en la que percibimos el mundo y los peligros que nos rodean. La trama de algunas series de televisión que anteriormente podría haber sido clasificada como ciencia ficción parece haberse convertido en realidad. Por ejemplo, en la serie de televisión *"The Good Wife"* cierto hacker encriptó los archivos de una firma de abogados y solicitó un pago de Bitcoins a cambio de liberar la información encriptada. En mayo de 2017 los archivos de más de 250,000

ordenadores alrededor del mundo, incluyendo los de grandes empresas de telefonía, bancos y hospitales fueron encriptados por medio de un ciberataque. Los hackers solicitaron un pago en Bitcoins a cambio de liberar esa información. En otro capítulo, los correos electrónicos privados de cierta candidata para ocupar un puesto público fueron robados por medio de un ciberataque y posteriormente publicados. En virtud de que dichos correos electrónicos contenían información sobre la vida privada de la candidata que contradecía los valores que promovía en su campaña, la publicación provocó que perdiera las elecciones. En 2016, durante el proceso de campaña de las elecciones de Estados Unidos, algunos correos electrónicos pertenecientes al Comité Democrático Nacional y a los miembros de campaña de la ex candidata a la presidencia Hilary Clinton fueron robados por medio de un ciberataque y posteriormente publicados. Los correos electrónicos, entre otras cosas, contenían información que puso en tela de juicio el correcto manejo de información clasificada por parte de la candidata mientras ocupó otros cargos públicos. Es probable que lo anterior haya provocado que Clinton perdiera las elecciones.

Sucesos como los anteriormente descritos han provocado que la ciberseguridad se convierta en una de las principales preocupaciones

de la comunidad internacional[1]. El constante aumento en el uso de las TIC y la dependencia que, en consecuencia, han desarrollado los Estados y sus ciudadanos respecto de éstas los ha vuelto más susceptibles a ser víctimas de un ciberataque. Sin embargo, aún no hay consenso respecto de la aplicabilidad del sistema jurídico internacional al ámbito del ciberespacio. Muchos autores se han mostrado escépticos y argumentan que, en virtud de que en el ciberespacio no existe una división territorial que permita distinguir entre la jurisdicción de un Estado y otro, la factibilidad de aplicar los principios de este sistema resulta dudosa[2]. Sin embargo, hay quienes defienden una postura contraria y argumentan que las normas

[1] Por ejemplo, desde 2010 Gran Bretaña estableció en su Estrategia de Seguridad Nacional que los ciberataques realizados por Estados y actores no estatales forman parte de los cuatro riesgos prioritarios para la seguridad nacional de ese Estado. "*A Strong Britain in an Agre of Uncertainty; The National Security Strategy* (October 2010), 29 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (consultada el 7 de julio de 2018).

[2] Eric Talbot Jensen, "Cyber Sovereignty: The Way Ahead" *Texas International Law Journal* 50:2 (2015), 275 -304 [en adelante "Eric Talbot Jensen, "*Cyber Sovereignty: The Way Ahead*"]; Wolf Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyber Space", *International Law Studies,* 89 (2013) [en adelante Wolf Heintschel von Heinegg, "*Territorial Sovereignty and Neutrality in Cyber Space"*]; David R. Johnson & David Post, "Law and Borders — The Rise of Law in Cyberspace", *Stanford Law Review* 48:1367 (1996) [en adelante "David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*"]; Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review* 76:3 (1998) [en adelante "Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*"]; Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law" *Texas Law Review* 88:7 (2010), 1573 [en adelante "Sean Kanuck, *Sovereign Discourse on Cyber Conflict*"].

vigentes del derecho internacional público sí son aplicables al ciberespacio[3]. Hasta ahora ningún tribunal internacional se ha pronunciado al respecto, sin embargo en los últimos años diversos académicos alrededor del mundo se han dado a la tarea de publicar propuestas en este sentido. Particularmente, estas publicaciones se relacionan con la aplicación de las normas que regulan el uso de la fuerza en el ciberespacio[4]. De igual manera, un grupo de académicos expertos independientes en Derecho Internacional Público crearon, en 2013 y 2017, el Manual de Tallinn 1.0 y 2.0, respectivamente. Estos manuales, basados en las fuentes del Derecho Internacional Público, constituyen una propuesta no vinculante de normas adaptadas a la actividad cibernética en tiempos de guerra y de paz.

Las obras anteriormente mencionadas junto con otros trabajos académicos, jurisprudencia de tribunales internacionales y nacionales, y los Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos, que de ahora en adelante llamaré

[3] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Estados Unidos, OUP, 2014) [en lo sucesivo "Roscini, *Cyber Operations and the Use of Force in International Law*"]; Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* (Nueva York, CUP, 2014) [en adelante "J. Shackelford, *Managing Cyber Attacks in International Law*"];

[4] Roscini, *Cyber Operations and the Use of Force in International Law*; Michael N. Schmitt. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Gran Bretaña, CUP, 2013) [en adelante "Tallinn Manual 1.0]*;* Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to be Launched* (Gran Bretaña, CUP, 2017) [en adelante "Tallinn Manual 2.0)].

los Artículos de Responsabilidad Estatal, conforman el marco de análisis de este trabajo, en el que defenderé que la aplicabilidad y eficacia de las normas y principios del Derecho Internacional Público no debe partir de un análisis abstracto y generalizado de la naturaleza del ciberespacio. Más bien, debe analizarse tomando en cuenta los elementos y particularidades de cada uno de los debates actuales en materia digital. De esta manera, encontraremos que su aplicabilidad y eficacia tratándose del debate que versa sobre la remoción o desindexación de contenido que han tenido que realizar algunas empresas resulta dudosa. Sin embargo, sí son eficaces y pueden aplicarse con la finalidad de atribuir responsabilidad a los Estados por ciberataques realizados por sus propios órganos o por una persona o grupo de personas y tienen efectos adversos en el territorio de otro Estado.

Para probar la hipótesis de este trabajo, en el primer apartado expondré a grandes rasgos la manera en la que se conforma y funciona el sistema de Derecho Internacional Público y las razones por las que considero que es relevante estudiar su aplicación y eficacia en materia digital. Lo anterior con la finalidad de ejemplificar y señalar, en forma explícita, los motivos por los cuales estimo que un análisis sobre la aplicabilidad de las normas del Derecho Internacional Público al ciberespacio no debe partir de una visión generalizada de la naturaleza del ciberespacio.

En el segundo apartado expondré de manera general en qué consiste el debate en materia de remoción o desindexación de contenido y la manera en la que éste se relaciona con el Derecho Internacional Público. Encontraremos que los principios de este sistema normativo son aplicables. Sin embargo, existen dudas respecto de la eficacia de las normas del Derecho Internacional Público.

Posteriormente, en el tercer apartado expondré los hechos de algunos de los ciberataques que han sucedido en los últimos años y relacionaré algunos de sus componentes con los Artículos de Responsabilidad Estatal. En este capítulo abordaré cuestiones sobre los elementos y condiciones de aplicación de dichos artículos, así como la problemática que se ha generado en torno a los mismos.

Finalmente, en el cuarto apartado analizaré los elementos y condiciones de aplicación de algunas normas primarias del sistema jurídico internacional con la finalidad de evaluar su aplicabilidad a los hechos de los casos que se describen en el segundo apartado. Asimismo, explicaré las razones por las que considero que los ciberataques que se describen en los casos son un hecho internacionalmente ilícito.

Aunque reconozco que algunos de los ciberataques y fuentes jurisprudenciales que voy a analizar en este trabajo pueden relacionarse o tener implicaciones en el ámbito del derecho internacional de los derechos humanos y del derecho internacional privado, me enfocaré únicamente en cuestiones correspondientes al Derecho Internacional Público general. Es decir, me limitaré a hablar solamente de los principios del Derecho Internacional Público establecidos en la Carta de las Naciones Unidas y los Artículos de Responsabilidad Estatal, tocando únicamente de manera tangencial y a manera de ejemplo otras normas.

El Derecho Internacional Público y la disputa por la Gobernanza del Internet

El Derecho Internacional Público es el cuerpo de normas y principios que regulan las relaciones entre los Estados.[5] Sin embargo, a diferencia de lo que sucede en los ordenamientos jurídicos nacionales, el sistema jurídico internacional no cuenta con un mecanismo de implementación coercitiva por medio del cual puede obligarse a los Estados a actuar de una determinada manera. Tampoco existe un cuerpo legislativo facultado para emitir normas obligatorias para los Estados.[6] Por lo tanto, las obligaciones estatales provienen de las fuentes del Derecho Internacional Público, que por referencia se encuentran establecidas en el artículo 38 del Estatuto de la Corte Internacional de Justicia, a saber: a) tratados internacionales; b) costumbre internacional; c) principios generales del derecho; y, d) fuentes subsidiarias, como doctrina o jurisprudencia de tribunales locales o internacionales.[7] Lo anterior implica que aquello que resulta obligatorio para los Estados es aquello que éstos mismos aceptan, tácita o explícitamente, como obligatorio. Dicho en otros términos, en virtud del ejercicio de su

[5] Roland R. Foulke, "Definition and Nature of International Law*", Columbia Law Review,* 19:6 (1919): 429-466

[6] Malcolm N. Shaw, *"International Law"* Sixth Edition (Cambridge, CUP, 2008), [en adelante "Malcolm N. Shaw, *International Law"*], 2-5.

[7] Ian Brownlie, *Principles of Public International Law,* Seventh Edition, (Oxford, OUP, 2008), 5 [en adelante "Brownlie, *Principles of Public International Law*"]; Estatuto de la Corte Internacional de Justicia (North Sea Continental Shelf Cases 1969), art. 38.

soberanía, los Estados pueden, por ejemplo, obligarse mediante la firma y ratificación de un tratado internacional a cumplir con ciertas obligaciones. En otras ocasiones, cierta práctica estatal reiterada considerada obligatoria por los mismos Estados (*inveterata consuetudo et opinio iuris seu necessitatis)* puede llegar a constituirse como una norma dentro del sistema jurídico internacional[8]. O bien, puede suceder que la aplicación uniforme y reiterada de alguna norma contenida en un tratado se cristalice y se convierta en una norma obligatoria para todos los Estados que forman parte de la comunidad internacional.[9] Sin embargo, bajo ninguna circunstancia pueden verse obligados, en forma coercitiva, por un órgano internacional a actuar de una determinada forma. Lo anterior implica que la implementación y cumplimiento de las obligaciones internacionales depende más bien de los mecanismos internos que cada Estado estructure en su sistema jurídico.

Ahora bien, a pesar de que el sistema jurídico internacional no cuenta con un cuerpo legislativo ni un mecanismo de implementación coercitiva, sí está conformado por un cuerpo de normas de naturaleza adjetiva cuya función es determinar los criterios bajo los cuales se considera que un determinado hecho, cuya naturaleza es considerada

[8] Ian Brownlie, *Principles of Public International Law*, 7-9; *North Sea Continental Shelf Cases (Germany v Denmark/Germany v Netherlands*) [1969] (Judgment) ICJ Rep 3 § 77 [en adelante "*North Sea Continental Shelf Cases"*]

[9] Ian Brownlie, *Principles of Public International Law*, 13; *North Sea Continental Shelf Cases,* § 61, 62.

contraria a las normas de derecho internacional, es atribuible a uno o varios Estados. Este cuerpo de normas se encuentra codificado en un documento denominado Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos y son obligatorias para los Estados en virtud de haber sido conformadas y redactadas con base en costumbre internacional. De esta manera, por un lado, los criterios con base en los cuales se atribuye responsabilidad estatal por la comisión de hechos internacionalmente ilícitos pertenecen al sistema jurídico internacional, y por otro lado el cumplimiento de las obligaciones provenientes del sistema jurídico internacional y la implementación de las decisiones emitidas por órganos jurídicos internacionales son facultad soberana de cada Estado.

La principal característica de las normas que actualmente conforman el sistema jurídico internacional es que se encuentran estrechamente vinculadas a la existencia de un espacio físico determinado dentro del cual un Estado ejerce su soberanía, entendida ésta como "*la facultad exclusiva que tienen los Estados de ejercer sus funciones dentro de su territorio*"[10]. Esto se debe a que el ámbito de aplicación de dichas normas es, en la mayoría de los casos, el territorio de los Estados. Por ejemplo, la obligación de debida diligencia aplica únicamente respecto de las actividades que se llevan a cabo dentro

[10] *The Island of Palmas Arbitration (Netherlands v United States)* (1928) 2 RIAA 829, 838 (traducción propia) [en adelante "*Island of Palmas Arbitration*"].

del territorio de éstos mismos.[11] Esto también sucede con el principio de no intervención, ya que abarca todas aquellas actividades o acontecimientos de carácter doméstico que suceden dentro del territorio de un Estado y que, en virtud de su soberanía, le competen exclusivamente a éste[12].

La característica de las normas anteriormente mencionada cobra especial relevancia tratándose de la factibilidad de aplicarlas al ciberespacio. Esto se debe a que algunos autores afirman que, en virtud de que el ciberespacio es intangible y ubicuo (por lo que no existe una distribución territorial clara sobre la cual un Estado pueda ejercer su soberanía), la aplicación de dichas normas a este ámbito resulta imposible[13]. A mi parecer esta es una afirmación basada en una premisa abstracta y generalizada que no considera los componentes de los diversos debates actuales en materia digital y la manera en la que éstos se relacionan con el derecho internacional púbico. Debido a la información que controlan y las funciones que

[11] *Corfu Channel Case (UK v Albania)* [1949] (Judgment) ICJ Rep 4, 22 [en adelante "*Corfu Channel Case*"].

[12] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1984] (Judgment) ICJ Rep 14, § 205 [en adelante "*Nicaragua Case*"].

[13] David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*; Sean Kanuck, *Sovereign Discourse on Cyber Conflict*, 1557; Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*; Wolf Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyber Space*

cumplen dentro de la sociedad, las empresas de tecnología se encuentran íntimamente relacionadas con el ejercicio de los derechos fundamentales de los individuos y la seguridad y economía de los Estados. En virtud de lo anterior, los debates sobre neutralidad de la red, la responsabilidad de los intermediarios en internet (que a su vez se traduce en un problema de remoción o desindexación de contenido), la ciberseguridad y la economía y educación digitales se han convertido en los principales componentes de la disputa entre el sector privado y los Estados por la gobernanza del Internet[14].

Las particularidades y alcances de cada una de estas disputas constituyen un tema amplio y multidisciplinario que excede los límites de este trabajo. Sin embargo, considero que una afirmación general y tajante respecto de la inaplicabilidad del derecho internacional al ciberespacio en el fondo implica aceptar que los Estados han perdido esta disputa y, por ende, la gobernanza de internet se encuentra en manos del sector privado. Lo anterior podría tener grandes implicaciones, ¿cómo podrían los Estados garantizar la seguridad y ejercicio de los derechos de sus ciudadanos si no tienen control sobre los elementos u objetos que se relacionan con esos derechos? ¿Cuál sería el incentivo del sector privado para continuar cumpliendo con la regulación existente en materia de

[14]Laura Denardis, *The Global War for Internet Governance* (Estados Unidos, YUP, 2014), 1-2 [en adelante "Laura Denardis, *The Global War for Internet Governance*"].

competencia económica, propiedad intelectual o protección de datos personales? ¿Cómo se conducirían las relaciones de los Estados en caso de suscitarse un conflicto internacional que resulte de una operación cibernética maliciosa? Considerando que estamos viviendo un momento histórico en el que las TIC se encuentran íntimamente relacionadas con los intereses primordiales del Estado, al grado de ser interdependientes, y al mismo tiempo se afirma que ha habido una pérdida de control por parte del Estado respecto de estas áreas de interés público[15], no es menor hablar sobre la aplicabilidad de las normas del derecho internacional en el ámbito digital.

En palabras de Jeremy Wright, el Fiscal General de Gran Bretaña "*si nos quedamos callados* [los Estados], *si aceptamos que los retos que impone la tecnología cibernética son mayores que aquellos que el marco jurídico internacional puede soportar […] entonces no podemos esperar otra cosa más que el ciberespacio se convierta en un lugar todavía más peligroso. […] el ciberespacio no es y no debe ser nunca un lugar sin Ley […] la cuestión no es si el derecho internacional aplica o no en el ciberespacio, sino la manera en la que debe ser aplicado y si nuestro entendimiento actual sobre éste es suficiente. […]*".

[15] Laura Denardis, "*The Global War For Internet Governance*", 1-6

Google, Yahoo! y otros v. El Derecho Internacional Público. Un resultado esquizofrénico.

Si nos referimos al debate sobre la remoción o desindexación de contenido que, por ordenes de diversos tribunales nacionales, han tenido que realizar algunas empresas con la finalidad de cumplir con diversos ordenamientos jurídicos nacionales o regionales, encontraremos que existe un problema de eficacia del derecho internacional. Esto podría deberse a que la naturaleza ubicua del internet y algunas de sus características técnicas (como la factibilidad de evadir mecanismos de geolocalización) ha traído como consecuencia que, en un intento de implementar los ordenamientos jurídicos anteriormente mencionados, algunas de esas decisiones judiciales resulten ser violatorias de los principios que rigen al propio sistema jurídico internacional, causando un resultado esquizofrénico: con la finalidad de asegurar la eficacia de sus sistemas jurídicos nacionales, los Estados provocan una pérdida de eficacia del sistema jurídico internacional.

Existen tres casos con base en los cuales puede entenderse el contenido y alcance de este debate y la problemática que representa en el ámbito del Derecho Internacional Público. Uno de estos casos es *Licra y UEJF v. Yahoo! Inc. y Yahoo! Francia (2000)*, que en adelante llamaré el Caso *Yahoo Inc.*. En este caso, una ONG en Francia denominada *Ligue contre le racisme et l'antisémitisme et*

Union des étudiants juifs de France (LICRA), junto con un grupo de estudiantes judíos que residen en Francia *L'union des Etudiants Juifs De France* (UEJF), demandaron a Yahoo! Francia y Yahoo! Inc. frente a un tribunal francés argumentando que la venta de productos Nazis en la página de Yahoo! Estados Unidos implicaba una violación al Código Penal de Francia, ya que a pesar de que los productos no estaban siendo promocionados directamente en la página de Yahoo! Francia, era posible accesar a la página de Estados Unidos desde territorio francés.[16]

Tomando en consideración que, basándose en la dirección IP del usuario, Yahoo! Inc. tenía la posibilidad de rastrear el origen geográfico de los usuarios que acceden a la página de Yahoo! Estados Unidos, el juez francés ordenó la implementación de una herramienta de geolocalización para bloquear el acceso de los nacionales franceses al contenido de la página de Yahoo! Estados Unidos. El juez también consideró la posibilidad de que algunos usuarios intentasen entrar a la página a través de portales que les permiten anonimizar su navegación y, por lo tanto, no revelar la localización geográfica desde donde buscan accesar. Sin embargo, declaró que esta no era una razón suficiente para no implementar la medida, ya que Yahoo! Inc. podría limitar el acceso a la página

[16] *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme (LICRA)*, 433 F.3d 1199 (9th Cir. 2006) [en adelante "Caso *Yahoo! Inc*"] El caso completo se puede consultar en https://caselaw.findlaw.com/us-9th-circuit/1144098.html.

únicamente a aquellos usuarios que revelen su localización geográfica.[17]

En respuesta a esta orden, Yahoo! Inc. argumentó la imposibilidad técnica de determinar, de manera precisa, la nacionalidad de los usuarios que acceden a su página en Estados Unidos, por lo que, para poder cumplirla, la empresa se vería obligada a remover el contenido de la página de Yahoo! Estados Unidos (lo que implicaría que un tribunal nacional, el tribunal francés que conoció de este caso, en realidad estaría determinando el contenido al que pueden tener acceso el resto de los usuarios de los servicios de Yahoo! Inc. alrededor de todo el mundo). Tomando en cuenta este argumento, el juez ordenó la conformación de un panel de tres expertos, quienes deberían emitir pronto una opinión técnica sobre la factibilidad, desde una perspectiva tecnológica, de que Yahoo! Inc. cumpliese con dicha orden.[18]

El panel de expertos concluyó que el 70% de los usuarios franceses pueden ser identificados mediante el rastreo de sus direcciones IP, y el acceso de estos usuarios a la página de *Yahoo!* Estados Unidos se puede impedir mediante la implementación de un software de filtrado de geolocalización, el cual puede cargarse en los servidores

[17] Caso *Yahoo! Inc.*
[18] Caso *Yahoo! Inc.*

de Yahoo! Inc. en California, Estados Unidos. Finalmente, los expertos también determinaron que una solicitud de revelación de la nacionalidad del usuario como requisito para acceder a la página aumentaría en un 20% la precisión de la información con base en la cual se puede filtrar el acceso de los usuarios a la página de *Yahoo!* Estados Unidos. Es decir, la implementación del software junto con el requisito de revelación de nacionalidad permite una precisión del 90% al momento de filtrar el acceso al contenido de la página. Conforme con la respuesta de los expertos, el juez ordenó la implementación de ambas medidas dentro de los 90 días siguientes a la emisión de la sentencia. De lo contrario, la empresa debería pagar una multa de $13,000 dólares por cada día que no acatase la orden establecida en la sentencia.[19]

Este caso generó una gran polémica a nivel internacional y surgieron grandes debates alrededor de las implicaciones que podría tener en materia de competencia económica, libertad de expresión y derecho

[19] Marc H. Greenberg, "A Return to Lilliput: The LICRA v. Yahoo! Case and The Regulation of Online Content In The World Market" *Berkeley Technology Law Journal* 18:1191 (2003) [en adelante "Marc H. Greenberg, *A Return to Lilliput: The LICRA v. Yahoo! Case and The Regulation of Online Content In The World Market*"], 1213, 1214; Yahoo! Inc. no impugnó la sentencia del tribunal francés. Sin embargo, decidió llevar el caso al Noveno Tribunal de Distrito de California del Norte, en San José. Este tribunal determinó que la orden del tribunal francés es contraria a la Primera Enmienda de la Constitución de Estados Unidos, por lo que no podía hacerse efectiva. Sin embargo, LICRA y UEJF apelaron esta decisión en el Tribunal de Alzada del Noveno Circuito de Estados Unidos, quien revirtió la decisión del Tribunal de Distrito argumentando que no tenía jurisdicción sobre LICRA y UEJF y, por lo tanto, carecía de competencia para determinar sobre la aplicabilidad de la sentencia.

a la privacidad. Por un lado, se consideró que el requisito de revelación de nacionalidad podría resultar violatorio de las normas de privacidad de otros Estados y que, en general, la sentencia atentaba en contra del carácter libre y abierto del internet, ya que la decisión de bloquear el acceso de los usuarios a la página de *Yahoo!* Estados Unidos implica establecer fronteras en el internet. Por otro lado, surge la preocupación de que el contenido de una página esté sujeta a la jurisdicción de todos los tribunales nacionales alrededor del mundo. Lo anterior se debe a que existe el riesgo de que un solo tribunal sea capaz de determinar, únicamente con base en las leyes del Estado en el que ejerce su jurisdicción, cuál es el contenido al que pueden acceder todos los usuarios alrededor del mundo, y no solamente aquellos que son ciudadanos o nacionales de dicho Estado. Sin embargo, el hecho de que un Estado no pudiese ejercer su jurisdicción sobre dicho contenido implicaría que las leyes del Estado en el que se encuentran establecida la plataforma que presta estos servicios serían las que determinan el contenido al que pueden tener acceso los usuarios de todo el mundo.[20]

Esta no fue la primera vez que un tribunal nacional se pronunció sobre el contenido al que pueden tener acceso los ciudadanos o nacionales de un Estado a través del internet. En 1986 un tribunal en

[20] Marc H. Greenberg, "*A Return to Lilliput: The LICRA v. Yahoo! Case and The Regulation of Online Content In The World Market*", 1210-1222.

Estados Unidos ordenó a Tattilo Editrice S.p.A. no aceptar las suscripciones de ciudadanos estadounidenses a su página web (que se encontraba albergada en un servidor en Italia), y contenía una versión digitalizada de la revista "Playmen", cuya circulación dentro del territorio estadounidense había sido prohibida en 1981 por medio de un mandato judicial. La orden de no aceptar las suscripciones de los ciudadanos de Estados Unidos se debió a que el tribunal consideró que permitir a los ciudadanos estadounidenses acceso a la página web equivalía a continuar circulando la revista dentro de Estados Unidos, lo que implicaba una violación al mandato judicial.[21]

Al igual que en el Caso Yahoo!, el tribunal estadounidense se pronunció respecto del contenido al que pueden tener acceso los ciudadanos estadounidenses desde el territorio del Estado en el que el tribunal ejerce su jurisdicción. El razonamiento de este tribunal para pronunciarse en este sentido fue el siguiente:

> "*El internet es un fenómeno mundial, accesible desde cualquier parte del mundo. No puede impedirse que Tattilo opere su sitio web solamente porque el mismo es*

[21] 511 F. Supp 486 (1981) *Playboy Enterprises, Inc., v. Chuckleberry Publishing, Inc,Tattilo Editrice SPA, Publishers Distributing Corporation, Arcata Publications Group, Inc.*, United States District Court, S. D. New York. No. 79 Civ. 3525 (1 de abril de 1981) [en adelante "*Playboy Enterprises Inc. v. Chucleberry Publishing Inc*.)

> *accesible desde un Estado en el que su contenido está prohibido. […] Una decisión en este sentido tendría un efecto devastador sobre todos los demás usuarios* [fuera de Estados Unidos] *que utilizan este servicio[…]. Por lo tanto, si bien es cierto que esta Corte no tiene la competencia para prohibir la creación de sitios de internet alrededor del mundo, sí la tiene para prohibir el acceso a esos sitios en este país."*[22]

Dejando a un lado las injerencias que el Caso *Yahoo!* podría tener en materia de privacidad y protección de datos personales por el requisito de declaración de privacidad, considero que el fondo de ambas sentencias va de acuerdo con los principios del Derecho Internacional Público. De acuerdo con una sentencia emitida por la Corte Permanente Internacional de Justicia en 1938, no existe ninguna norma en el Derecho Internacional Público que prohiba que los Estados ejerzan su jurisdicción sobre actos que, a pesar de no haber sido cometidos dentro de su territorio, tengan efectos dentro del mismo.[23] Esta forma de ejercer jurisdicción se conoce doctrinalmente como "la teoría de los efectos"[24] y se ha utilizado en

[22] *Playboy Enterprises, Inc. v. Chucleberry Publishing, Inc.*
[23] *SS Lotus Case (France v Turkey)* [1927] (Judgment) PCIJ Rep Series A No 10, 18 -23. [en adelante "*SS Lotus Case*"].
[24]Thomas Schultz, "Carving up the Internet: "Jurisdiction, Legal Orders, and the Private/Public International Law Interferface" *European Journal of International Law,* 19:4 (2008), 812.

las últimas décadas como base para el ejercicio de jurisdicción de los Estados y sus tribunales en aspectos relacionados con la materia digital.[25] Además, en ambos casos los tribunales se abstuvieron *prima facie* de ejercer su jurisdicción en otros territorios, ya que únicamente prohibieron el acceso a ese contenido desde el territorio al que pertenecen. Una decisión en otro sentido hubiera implicado una violación al principio de no intervención, que como veremos más adelante implica *inter alia* que cada Estado tiene la libertad de decidir, con total independencia de otros Estados, el contenido al que pueden acceder sus ciudadanos[26].

[25]Por ejemplo, la aplicación extraterritorial del GDPR está basada en esta teoría. Considerando 23 del GDPR: "*[…]el tratamiento de datos personales de interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. […]*." Asimismo, el pasado 21 de junio la Suprema Corte de Estados Unidos decidió que en materia de comercio interestatal el "nexo sustancial" que debe existir entre la actividad que se grava y el Estado para que éste último pueda gravar las compraventas que realizan las empresas de comercio electrónico se define con base en la cantidad de dinero o transacciones que realice la empresa dentro del territorio del Estado, independientemente de que se encuentre físicamente establecido en otro Estado *South Dakota, Petitioner v. Wayfair, Inc., et al.*, Suprema Corte de Estados Unidos (Judgment), [21 de junio de 2018], la opinión completa de la Suprema Corte de Estados Unidos puede consultarse en https://www.supremecourt.gov/opinions/17pdf/17-494_j4el.pdf.

[26] Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 1571.

Sin embargo, este debate sigue vigente y ha cobrado aún más relevancia en los últimos años por el denominado "derecho al olvido"[27]. El primer antecedente judicial del derecho al olvido fue el caso de Google España e Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, al que en adelante me referiré como el Caso Costeja. En este caso, Mario Costeja Gonzáles, un ciudadano español, solicitó ante la AEPD la desindexación por parte del buscador Google Inc., del vínculo a una publicación del periódico español *El Vanguardista*, misma que aparecía en la página de dicho buscador cuando se ingresaba el nombre del señor Costeja. En dicha publicación se establecía que en 1998 una propiedad del señor Mario Costeja González había sido subastada, debido a que incumplió con sus obligaciones de pago respecto de algunas deudas adquiridas con anterioridad a la subasta. Sin embargo, en 2014 el señor Costeja ya había cumplido con el pago de sus deudas, por lo que solicitó a la autoridad española que ordenase la desindexación de dicho artículo. La Agencia Española de Protección de Datos, con base en la Directiva 95/46/CE, que entre otras cosas establece el derecho del titular de datos personales a ejercer el derecho de

[27]En realidad se trata de los derechos de cancelación u oposición al tratamiento de datos personales. Sin embargo, por diversas cuestiones se ha denominado públicamente como "derecho al olvido".

cancelación de los mismos, ordenó a Google Inc. la remoción de dicho resultado de búsqueda.[28]

Google Inc. y Google España decidieron apelar la decisión de la AEPD ante la Audiencia Nacional Española, misma que, a su vez, decidió hacer una consulta prejudicial al Tribunal de Justicia de la Unión Europea (TJUE). El TJUE determinó, entre otras cosas, que Google está obligado a desindexar contenido ante la petición del titular de los datos, independientemente de que el contenido de la página que vincula sea legal o no. Específicamente, ordenó desvincular el nombre del titular de los datos con la noticia que le causa perjuicio, no eliminar el acceso a la noticia misma. Es decir, la noticia continúa siendo accesible bajo otros criterios de búsqueda, simplemente ésta no se encontrará relacionada con el nombre de la persona que ejerce su derecho de cancelación frente al buscador[29]

El TJUE también estableció que, en principio, el derecho a la protección de datos personales de los individuos prevalece sobre el interés económico del motor de búsqueda y sobre el interés público de encontrar la información que busca desindexarse, salvo en aquellas circunstancias en las que, "*por razones concretas, como el*

[28]Asunto C-131/12, Sentencia del Tribunal de Justicia Europeo (Gran Sala), *Google Spain, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, 13 de mayo de 2014. [en adelante "*Caso Costeja*"].
[29] *Caso Costeja.*

papel desempeñado por el titular de los datos personales en la vida pública, la injerencia en este derecho fundamental esté justificada por el interés preponderante del público en tener acceso a la información de que se trate"[30].

Independientemente de las controversias y cuestionamientos que pueden suscitarse por el llamado "derecho al olvido" debido a los incentivos e implicaciones que genera[31], en este trabajo la que nos concierne es que en el Caso Costeja anteriormente planteado el TJUE no se pronunció respecto del alcance de la desindexación del nombre del titular de los datos con el contenido en cuestión—territorial o global— que tiene que realizar Google al momento de cumplir con solicitudes de cancelación de datos personales.

Años después, mientras enfrentaba un procedimiento sancionatorio frente a la CNIL por haber incumplido con una medida cautelar de desindexación en todos sus portales y no solamente los de la Unión Europea, incluido el dominio de Google.com, en febrero de 2016 Google anunció la implementación en sus servidores del mismo

[30] *Ibidem.*

[31] Esta discusión se aborda con mayor amplitud y detalle en Keller, Daphne, "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation" (22 de marzo de 2017). Disponible en SSRN: https://ssrn.com/abstract=2914684 or http://dx.doi.org/10.2139/ssrn.2914684.

software de geolocalización que el juez francés ordenó en el Caso *Yahoo! Inc.* Es decir, la desindexación no aplicaría respecto de todos los portales de Google, sino únicamente desde el territorio del Estado en el que se interpuso la solicitud de cancelación de datos.[32] Sin embargo, a pesar de los esfuerzos de Google, en marzo de 2016 la CNIL determinó lo siguiente:

> "[…] *si bien la implementación del mecanismo de geolocalización constituye un avance [..] esta medida puede ser eludida por el usuario interesado […], ya que existen soluciones técnicas para burlar las medidas de filtrado implementadas por la empresa que permiten al usuario elegir la procedencia geográfica de la dirección IP (usando una VPN, por ejemplo). Asimismo, la información continúa siendo accesible desde fuera de Francia […] por lo que esta medida no logra el objetivo fijado por la Directiva europea en materia de protección de datos personales. Para permitir que los ciudadanos europeos se beneficien de una protección eficaz e integral de sus derechos fundamentales, es necesario un acto de aplicación que no distinga la extensión y origen*

[32]Google to scrub web search results more widely to soothe EU objections https://uk.reuters.com/article/us-google-eu-privacy-idUKKCN0VJ29U;https://www.zdnet.com/article/google-extends-block-on-right-to-be-forgotten-search-results/ (consultada el 22 de junio de 2018)

geográfico del internet y que, por ende, sea capaz de responder a los requisitos de protección de datos previamente dictados por el TJUE."[33]

Tras haber sido multado por no haber desindexado globalmente (de los dominios de todos los países del mundo, incluido Google.com) el contenido relacionado con la persona que solicitó esta acción, Google LLC. apeló la decisión de la CNIL ante la Corte Suprema Administrativa de Francia, la cual a su vez remitió el asunto al TJUE. Éste último aún no ha emitido su decisión.[34]

Para poder analizar la problemática que gira en torno a las sentencias anteriormente planteadas, deben considerarse algunas de las implicaciones que la sentencia emitida por la CNIL y aquella que, en caso de ser resuelta en el mismo sentido por el TJUE, podrían tener en el sistema jurídico internacional.

Por un lado, existe un principio de Derecho Internacional Público que establece que los Estados únicamente pueden ejercer su

---

[33]Resolución de la CNIL, *"Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X"* https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032291946&fastReqId=273825503&fastPos=1 (consultada el 26 de mayo de 2018) (traducción propia) [en adelante "*Resolución de la CNIL*"]

[34]Google "right to be forgotten" case goes to top EU court https://www.zdnet.com/article/google-right-to-be-forgotten-case-goes-to-top-eu-court/ (consultada el 26 de junio de 2018).

jurisdicción dentro del territorio de otros Estados cuando existe un tratado internacional que así lo establece, o bien se ha conformado una norma de costumbre internacional en este sentido.[35] Actualmente se considera que la infraestructura cibernética localizada dentro del territorio de los Estados (lo cual incluye los servidores que se encuentren dentro del territorio de los mismos) se entiende protegida por la soberanía de ese Estado. Por lo tanto, la sentencia emitida por el CNIL tendría efectos en el territorio de todos aquellos Estados en los que Google tendrá que llevar a cabo la desindexación del nombre del titular que ejerce sus derechos respecto del contenido en disputa. Dicho en otras palabras, dado que no existe un tratado internacional que permita expresamente a Francia ejercer su jurisdicción en otros Estados, la decisión de la CNIL constituye una violación a la soberanía de todos los Estados en los que su decisión podría tener efectos.

Por otro lado, los Estados conservan una facultad soberana de interpretar e implementar las obligaciones que contraen en materia de derechos humanos de acuerdo con su propio sistema jurídico nacional y sus valores culturales. Por lo tanto, éstos gozan de un amplio margen de apreciación respecto de las medidas y métodos que desean implementar con la finalidad de garantizar los derechos establecidos en los tratados de los que forman parte. Lo anterior

[35] *SS Lotus Case*, 49.

siempre y cuando no actúen en forma contraria al objeto y propósito de las obligaciones ahí establecidas.[36] En virtud de lo anterior, la decisión de la CNIL podría implicar una injerencia en el margen de apreciación de los Estados en materia de derechos humanos. Dicho de otra manera, la decisión del TJUE en el Caso Costeja respecto de delegar a Google la responsabilidad de realizar un ejercicio de ponderación entre el derecho a la libertad de expresión y el derecho a la protección de datos personales, así como la regla general de prevalencia del derecho a la protección de datos personales sobre el derecho a la libertad de expresión, tendría efectos en todos los Estados en los que dicha empresa responda solicitudes de desindexación de contenido. Es decir, la decisión del TJUE sumada a la decisión de la CNIL serían quienes determinan cómo es que deben garantizarse estos derechos dentro del territorio de dichos Estados.

No obstante, la CNIL estableció que, aún cuando su decisión tiene efectos extraterritoriales, la eficacia de los derechos de cancelación u oposición al tratamiento de datos personales depende de que puedan ser aplicados respecto de la totalidad de ese tratamiento y no solamente de aquel que se efectúa en el portal del Estado donde se interpone la acción. "*Esto debe ser así aún cuando el criterio*

[36] *De Cubber v. Belgium*, no. 9186/80 § 35 ECHR (1984); VgT Verein Gegen Tierfabriken v. Switzerland, no. 24699/94, §78 ECHR (2001); Malcolm N. Shaw, *International Law*, 357.

adoptado pueda entrar en conflicto con los derechos de otros Estados"[37].

Los casos y criterios anteriormente planteados sin duda ponen en tela de juicio la eficacia del sistema jurídico internacional en el ámbito de la gobernanza que se plantea. Si bien no me atrevería a decir que dichas normas son inaplicables, considero que valdría la pena explorar la posibilidad de establecer un tratado que, tomando en consideración la naturaleza ubicua del internet, regule la jurisdicción de los Estados, cuando menos en materia de protección de datos personales. De esta manera, los Estados podrían acordar los términos y alcances del ejercicio de jurisdicción por parte de otros Estados dentro de su territorio y así asegurar la eficacia de su sistema jurídico en materia de protección de datos personales. Es decir, si lo que realmente se busca es una homogeneización en la forma en la que se reglamentan, garantizan e implementan las obligaciones en materia de protección de datos personales, resultaría conveniente que los Estados, en pleno ejercicio de su soberanía y en igualdad de condiciones, acuerden el modo en el que deben implementarse este tipo de obligaciones.

Ahora bien, el dilema anteriormente planteado no se presenta cuando consideramos la posibilidad de aplicar los principios del Derecho

[37] *Resolución de la CNIL*.

Internacional Público para efectos de establecer que la realización de un ciberataque por parte de un Estado o de una persona o grupo de personas desde el territorio de un Estado puede ser considerada un hecho internacionalmente ilícito y, por lo tanto, generar la responsabilidad internacional de dicho Estado. La ciberseguridad es uno de los debates actuales más importantes en materia digital por encontrarse íntimamente relacionada con la protección de las funciones básicas de los Estados. Las vulneraciones de seguridad de la infraestructura de los Estados tanto como la de los sectores financiero o industrial pueden derivar en grandes pérdidas económicas para los Estados o, incluso, en la destrucción de objetos físicos que podría, eventualmente, dañar a los ciudadanos.[38] En virtud de lo anterior, no es de menor importancia hablar acerca de la aplicabilidad de las normas del Derecho Internacional Público a este aspecto de la gobernanza de internet. Específicamente sobre la posibilidad de establecer la responsabilidad internacional de los Estados por la comisión de ciberataques que emanan de su territorio y tienen efectos adversos en el territorio de otro Estado.

[38] Laura Denardis, *The Global War for Internet Governance*, 86.

Atribución de los ciberataques a los Estados con base en los Artículos de Responsabilidad Estatal. El primer elemento.

El artículo 1 de los Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (en lo sucesivo, los "Artículos de Responsabilidad Estatal") establece que "*todo hecho internacionalmente ilícito del Estado genera su responsabilidad internacional*".

El artículo 2 de los Artículos de Responsabilidad Estatal establece que "*un hecho puede ser considerado como internacionalmente ilícito cuando un comportamiento consistente en una acción u omisión: (i) es atribuible a un Estado según el derecho internacional;* y (ii) *constituye una violación a una obligación internacional del Estado*".

De los dos artículos expuestos en los párrafos anteriores se desprende que, para poder probar que los ciberataques son un hecho internacionalmente ilícito que genera responsabilidad a los Estados, es necesario que se acrediten los siguientes elementos: (i) que los ciberataques son una conducta atribuible a los Estados; y (ii) que los ciberataques constituyen una violación a las obligaciones internacionales de los Estados.

El primer elemento del artículo 2 de los Artículos de Responsabilidad Estatal establece claramente que la atribución a un Estado de una determinada conducta, independientemente de que dicha conducta consista en una acción u omisión, debe realizarse de conformidad con el derecho internacional.

Con la finalidad de probar que los ciberataques son una conducta atribuible a los Estados de conformidad con el derecho internacional, utilizaré algunas de las normas establecidas en el Capítulo Segundo de los Artículos de Responsabilidad Estatal y tomaré como ejemplo dos de los ciberataques que, por sus características, considero ejemplificativos y altamente ilustrativos en cuanto al alcance y consecuencias que pueden tener este tipo de conductas y la forma en la que usualmente se planean, coordinan y realizan.

Exposición de los hechos de los casos que serán materia de estudio en el presente apartado.

Caso Stuxnet

En 2010 "VirusBlokAda", una agencia de seguridad en Bielorrusia, descubrió "Stuxnet", un malware que fue utilizado por Estados Unidos e Israel para atacar y destruir un alto porcentaje de las centrifugas de enriquecimiento de uranio de una planta nuclear localizada en Natanz, Irán[39]. Mientras analizaban Stuxnet, los

[39]Stuxnet Worm Attack on Iranian Nuclear Facilities, Michael Holloway http://large.stanford.edu/courses/2015/ph241/holloway1/ (consultada el 2 de noviembre de 2017).

miembros de VirusBlokAda descubrieron que su objetivo principal era atacar el Programmable Logic Controler (PLC) de la planta nuclear de Natanz. Un PLC es un tipo de computadora pequeña de uso común que se conecta a la infraestructura física que se utiliza para apagar, prender o controlar en forma genérica la velocidad de las válvulas o motores de plantas de energía, sistemas financieros, de salud, o de transporte de los Estados, o bien sistemas industriales. Además, Stuxnet estaba conformado por varios códigos conocidos como "Zero-Day Code".[40] Un código como este es excepcionalmente difícil de configurar, ya que permite que el malware se expanda automáticamente por el ciberespacio sin que su creador tenga que hacer absolutamente nada.[41]

En virtud del nivel de sofisticación de Stuxnet, algunos miembros de la agencia de seguridad en Bielorrusia comenzaron a sospechar que no podía haber sido creado sin el apoyo logístico y financiero de, cuando menos, un Estado.[42]

[40]Last minute paper: An indepth look into Stuxnet https://www.virusbulletin.com/conference/vb2010/abstracts/indepth-look-stuxnet (consultada el 2 de noviembre de 2017).

[41]El virus que tomó el control de mil máquinas y les ordenó autodestruirse http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet (consultada el 5 de septiembre de 2017);

[42] Documental "Zero Days"; Virus infecta planta nuclear iraní http://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw.shtml (visto el 15 de mayo de 2016)

Las sospechas de los miembros de VirusBlokAda se confirmaron en junio de 2012. David E. Singer, un reconocido periodista del *New York Times*, publicó un artículo revelando los hechos detrás de la destrucción de la planta nuclear de Natanz[43]. La información contenida en dicho artículo proviene de entrevistas realizadas a ex agentes americanos, europeos e israelíes de las agencias de seguridad de Irán y Estados Unidos que estuvieron directamente involucrados en la planificación y configuración de Stuxnet, así como de varios miembros del equipo de seguridad nacional que laboraron en la Casa Blanca durante la administración del ex Presidente de Estados Unidos Barack Obama.[44] De acuerdo con los hechos narrados por dichas personas en las entrevistas, Stuxnet fue una operación secreta ordenada por George W. Bush en 2006. El nombre clasificado de dicha operación era "Juegos Olímpicos" y su objetivo primordial era retrasar el programa nuclear de Irán[45]. Aunque la idea de realizar un ciberataque a la planta nuclear de Irán fue de los agentes de la Agencia de Seguridad Nacional de Estados Unidos, la programación,

[43]Obama ordered wave of cyber attacks against Iran http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (consultada el 15 de diciembre de 2015); Revela *Times* que Obama incrementó los ciberataques contra el programa nuclear iraní http://www.jornada.unam.mx/2012/06/02/mundo/023n2mun (consultada el 16 de diciembre de 2015)

[44]Stuxnet: la filtración de un ciberataque http://www.proceso.com.mx/346707/stuxnet-la-filtracion-de-un-ciberataque (consultada el 5 de noviembre de 2017)

[45]Las armas de Estados Unidos para evitar la guerra con Irán http://www.jornada.unam.mx/2012/06/02/mundo/023n2mun (consultada el 7 de noviembre de 2017)

las pruebas y la operación de Stuxnet fueron el resultado de un trabajo conjunto entre la Agencia de Seguridad Nacional de Estados Unidos y algunos agentes del Mossad, la agencia de seguridad nacional de Israel.[46]

Aunque la planeación y creación de Stuxnet sucedió durante la administración de George W. Bush, el ciberataque estaba planeado para después de 2010. Sin embargo, en esta fecha, durante el mandato del Presidente Barack Obama, un ingeniero que trabajaba en la planta nuclear de Irán, cuya computadora se encontraba infectada con dicho malware, conectó su computadora al internet fuera de Natanz. Stuxnet no pudo reconocer que su ambiente había cambiado y comenzó a auto-replicarse por todo el mundo, lo que puso la secrecía de la operación en grave peligro. En consecuencia, el entonces Presidente de Estados Unidos, Barack Obama, dio la orden de acelerar el momento de la destrucción de las centrífugas de enriquecimiento de uranio de la planta nuclear de Natanz.[47]

---

[46]Obama ordered wave of cyber attacks against Iran http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (consultada el 9 de noviembre de 2017); Obama ordenó personalmente un ataque cibernético contra Irán http://www.elmundo.es/elmundo/2012/06/01/internacional/1338585021.html (consultada el 9 de noviembre de 2017); Israeli Test on Warm Called Crucial in Iran Nuclear Delay http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1 (consultada el 9 de noviembre de 2017).

[47]Obama ordered wave of cyber attacks against Iran http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (consultada el 8 de noviembre de 2017).

Antes de Stuxnet ya era usual que se causara daño a otras computadoras o sistemas de información por medio de ciberataques. Sin embargo, lo que resulta excepcional de Stuxnet es que fue el primer malware capaz de destruir infraestructura física. En virtud de lo anterior, los sucesos de 2010 en la planta nuclear de Natanz, Irán también son conocidos por ser el primer ataque a una infraestructura física realizado con lo que se considera un arma cibernética de muy peligrosa potencia.[48]

Caso Sony Pictures

El 11 de junio de 2014 Corea del Norte envió una carta al Secretario General de las Naciones Unidas, Ban Ki-moon, denunciando la película "*The Interviene*", una sátira acerca del asesinato del líder de la nación asiática Kim-Gong, que dentro de unos meses sería lanzada al público por Sony Picures. En el comunicado, Corea del Norte prometió tomar serias medidas en caso de que el gobierno de Estados Unidos apoyara, tácita o explícitamente, el lanzamiento de la película. El Secretario General de las Naciones Unidas no apoyó la posición de Corea del Norte.[49]

[48] Iran "first victim of cyberwar" http://www.scotsman.com/news/iran-first-victim-of-cyberwar-1-811906 (consultada el 10 de noviembre de 2017).

[49] http://jnslp.com/wp content/uploads/2016/07/The_2014_Sony_Hack_and_International_Law.pdf

El 21 de noviembre de 2014, dos altos funcionarios de Sony Picures recibieron amenazas por parte de un grupo denominado "God'sApstls" diciendo que causarían daño a la compañía. Tres días después, las pantallas de las computadoras de los empleados de Sony Pictures en Culver City, California se tornaron negras y apareció una calavera en ellas con un mensaje que decía "este es solo el comienzo, hemos robado toda la información de la compañía". Los hackers se autodenominaron los "Guardianes de la Paz".[50]

En días posteriores, los Guardianes de la Paz comenzaron a difundir, en diversos medios de comunicación, datos personales de los ejecutivos de Sony Pictures (números de seguridad social, expedientes médicos, salarios, correos electrónicos personales) además de varias películas pertenecientes a dicha compañía que aún no habían sido estrenadas.[51] Los empleados de Sony Pictures sufrieron severos daños por la publicación de sus datos personales, incluyendo robo de identidad y fraudes bancarios. La información de las computadoras de Sony Pictures fue destruida y los hackers instalaron un malware dentro de las mismas para cubrir sus huellas,

[50] http://jnslp.com/wp-content/uploads/2016/07/The_2014_Sony_Hack_and_International_Law.pdf

[51] Sony Employee Report http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf (consultado el 12 de diciembre de 2015).

lo que provocó que la red de Sony Pictures se tornara inoperable durante días.[52]

En diciembre de 2014, mientras continuaban filtrando información confidencial, los Guardianes de la Paz exigieron a Sony suspender el estreno de la película "*The Interviewer*", y amenazaron con realizar ataques terroristas en las salas cinematográficas en las que se exhibiera la película. En respuesta a las amenazas, la empresa decidió no exhibir la película en salas públicas.[53] Corea del Norte negó responsabilidad por el ciberataque, sin embargo calificó los actos y amenazas de los Guardianes de la Paz como "actos de justicia".[54]

Unos días más tarde, el FBI, en un comunicado de prensa, anunció que tenía evidencia suficiente para concluir que el gobierno de Corea del Norte era responsable por el ciberataque. El FBI explicó que la evidencia que había encontrado era que (i) el Malware que fue utilizado para cometer el ciberataque es casi idéntico a uno que había sido utilizado previamente por el gobierno de Corea del Norte; (ii)

---

[52] http://jnslp.com/wp-content/uploads/2016/07/The_2014_Sony_Hack_and_International_Law.pdf

[53] BBC Mundo El FBI acusa al gobierno de Corea del Norte del Hackeo a Sony Pictures http://www.bbc.com/mundo/ultimas_noticias/2014/12/141219_ultnot_corea_norte (consultado el 16 de diciembre de 2015)

[54] http://jnslp.com/wp-content/uploads/2016/07/The_2014_Sony_Hack_and_International_Law.pdf

la infraestructura utilizada para el ciberataque coincide con la infraestructura del gobierno norcoreano.[55]

A pesar de que Corea del Norte negó ante las Naciones Unidas su vinculación con los ciberataques, el 2 de enero de 2015 el ex Presidente de Estados Unidos, Barack Obama, emitió una orden ejecutiva imponiendo sanciones económicas en contra de dicho Estado.[56]

[55]Update on Sony Investigation https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (consultada el 15 de diciembre de 2015)

[56]*The Guardian, Sony Cyber Attack linked to North Korean Government, FBI says* *http://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official* (consultada el 10 de diciembre de 2015)*;* Abc News, Sony Hack Believed to be Routed Through Infected Computers Overseas http://abcnews.go.com/Politics/sony-hack-believed-routed-infected-computers-overseas/story?id=27667840 (consultada el 16 de diciembre de 2015)*;CNBC, FBI Details North Korean Attack on Sony* *http://www.cnbc.com/2015/01/08/fbi-details-north-korean-attack-on-sony.html#* (consultada el 17 de diciembre de 2015); *New York Times, FBI Says Little Doubt North Korea Hit Sony* *http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?_r=0* (consultada el 18 de diciembre de 2015*); New York Times, U.S. said to find North Korea ordered attack on Sony* *http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0* (consultada el 18 de diciembre de 2015)*; BBC News, Sony hack: Obama vows response as FBI blames North Korea* *http://www.bbc.com/news/world-us-canada-30555997* (consultada el 18 de diciembre de 2015).

Aplicación de los Artículos de Responsabilidad del Estado por Hechos Internacionalmente Ilícitos a las operaciones cibernéticas.

Caso Stuxnet

En virtud de que los elementos del Caso Stuxnet anteriormente expuestos establecen claramente que quienes estuvieron directamente involucrados en el ciberataque fueron agentes estatales de Estados Unidos e Israel, los hechos de este caso se subsumen sin mayores complicaciones al artículo 4 de los Artículos de Responsabilidad Estatal. Este artículo establece que toda conducta realizada por un órgano del Estado se considera atribuible a dicho Estado, sin importar el orden de gobierno al que pertenezca el órgano que realiza la conducta, las funciones que realice, o que sea una persona física, moral o cualquier otro tipo de entidad conforme al ordenamiento jurídico interno de cada Estado[57].

De esta manera, de la lectura de este artículo y de los hechos del caso Stuxnet, es posible afirmar que, por haber sido el Presidente de Estados Unidos quien ordenó la realización del ciberataque y las agencias de seguridad nacional de Israel y Estados Unidos quienes

[57]Artículo 4. 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. 2. Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado."

lo realizaron, dicha conducta resultaría *per se* atribuible a cualquiera de esos dos Estados. Sin embargo, con la finalidad de determinar si efectivamente este ciberataque constituye un hecho internacionalmente ilícito, más adelante evaluaremos cuáles son las normas primarias del sistema jurídico internacional que fueron violadas mediante este acto Estatal.

Caso Sony Pictures

El artículo 8 de los Artículos de Responsabilidad Estatal establece que el comportamiento de cualquier persona o grupo de personas será considerado un acto del Estado cuando esa persona o grupo de personas actuén bajo las instrucciones o la dirección o control de ese Estado.[58]

Los hechos del caso Sony Pictures muestran que no fue ningún órgano estatal perteneciente a Corea del Norte quien realizó el ciberataque, sino los Guardianes de la Paz, un grupo de personas que, independientemente de que pudieran ser calificados como terroristas o activistas hackers, no forman parte del gobierno de Corea del Norte. Por lo tanto, para que Corea del Norte resulte responsable, bajo el citado artículo 8, por el ciberataque dirigido a Sony Pictures,

[58]Artículo 8. 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.

es necesario probar que los Guardianes de la Paz actuaron bajo las instrucciones o la dirección y control de Corea del Norte.

La aplicabilidad del artículo 8 a conductas realizadas por una o varias personas que fueron instruidas por el Estado resulta clara en casos en los que sujetos privados son, por ejemplo, enviados como voluntarios o son empleados como auxiliares en diversos organismos del Estado sin ser oficialmente servidores públicos[59]. La determinación de cuándo una persona o grupo de personas actuaron bajo la dirección o control de un Estado también es un punto controversial. Se han sostenido diversas discusiones en torno al estándar que debe utilizarse para determinar cuándo una persona o grupo de personas actuaron bajo la dirección o control de un Estado, y el estándar de prueba que cada criterio implica.

El *Caso Relativo a las Actividades Militares y Paramilitares en Nicaragua y Contra Nicaragua (Nicaragua v. Estados Unidos)* de la CIJ, al que a partir de ahora me referiré como el Caso Nicaragua, el caso Dusko Tadic resuelto por Tribunal Penal Internacional para la ex Yugoslavia (TPIY), al que de ahora en adelante me referiré como el Caso Tadic y el Caso sobre la *Aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y*

[59] International Law Commission, "*Report of the International Law Commission on the Work of its 53rd Session*" (23 de abril–1 de junio y 2 de julio–10 de agosto de 2001) UN Doc A/45/10 (Draft Articles on State Responsibility with Commentaries), artículo 8(2) [en adelante "DARSIWA"].

Herzegovina v. Serbia y Montenegro) de la CIJ[60], resultan paradigmáticos para comprender el debate que gira en torno a la aplicabilidad del artículo 8 de los Artículos de Responsabilidad Estatal. A continuación expondré los hechos de los tres casos y el razonamiento de la CIJ y del TPIY respecto de cada uno de ellos y posteriormente daré a conocer mi punto de vista respecto de los criterios ahí establecidos.

En el Caso Nicaragua, Estados Unidos fue demandado por Nicaragua frente a la CIJ por haber brindado apoyo financiero y logístico a un grupo de oposición, conformado por guerrilleros, conocido públicamente como los "*Contras"* en varios atentados en contra del gobierno Sandinista.[61] Entre las demandas hechas por Nicaragua se encontraba la atribución de responsabilidad a Estados Unidos por los actos de los "*Contras"*.[62] La CIJ determinó que, aún cuando las pruebas que le fueron presentadas demostraban que la participación de Estados Unidos en las acciones de los *"Contras"* fue preponderante en virtud del financiamiento, entrenamiento, organización y planeación de las operaciones proveídos a los *"Contras"*, lo anterior no era suficiente para atribuir sus actos a

[60] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] (Judgment), ICJ Rep 43 § 210 [en lo sucesivo "*Genocide Convention Case*"].
[61] *Nicaragua Case*, § 81.
[62] *Nicaragua Case*, §114.

dicho Estado, pues los *"Contras"* bien podrían haber realizado estas acciones sin el apoyo y control de Estados Unidos[63], ya que incluso continuaron sus operaciones aún después de que Estados Unidos cesó su apoyo financiero[64]. Por lo tanto, para que los actos de los *"Contras"* pudieran ser atribuidos a Estados Unidos con base en el artículo 8, Nicaragua tendría que haber probado que: a) Estados Unidos tenía *control efectivo* sobre los "*Contras"* durante el curso de todas y cada una de sus operaciones militares y paramilitares[65]. Es decir, que instruyó todas las acciones y operaciones de dicho grupo; y b) que los *Contras* eran un grupo completamente dependiente respecto de los Estados Unidos. Es decir, que todos los actos que cometieron lo hicieron a nombre y cuenta de Estados Unidos y su sola existencia como grupo está basada en actuar a nombre de dicha nación. [66]

Posteriormente, en 1999 el TPIY en el Caso Tadic contradijo lo que estableció la CIJ en la sentencia del Caso Nicaragua. En este caso, el Tribunal Penal Internacional se vio en la necesidad de determinar, entre otras cosas, el grado de control que debe tener un Estado sobre un grupo armado que se encuentra dentro del territorio de otro Estado

[63] *Nicaragua Case*, §115.
[64] *Nicaragua Case*, §110.
[65] *Nicaragua Case*, §115,116.
[66] *Nicaragua Case*, §115; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1984] (Separate Opinion of Judge Ago) ICJ Rep 14 § 16

para efectos de atribuirle los actos de dicho grupo y entonces clasificar el conflicto en cuestión como un conflicto de carácter internacional[67]. En virtud de que ni la Tercera Convención de Ginebra ni el Derecho Internacional Humanitario proveen criterios para resolver esta pregunta, el Tribunal Penal Internacional recurrió al artículo 8 de los Artículos de Responsabilidad Estatal.[68] A diferencia de la CIJ, el Tribunal Penal Internacional determinó que no es necesario que el Estado tenga *control efectivo* sobre el grupo armado para que sus actos resulten atribuibles a dicho Estado, sino que basta con probar la existencia de un *control general* por parte del Estado sobre dicho grupo.[69] De acuerdo con lo establecido por el Tribunal Penal Internacional, tener un *control general* sobre un grupo de personas implica que, en virtud de que dicho grupo recibió financiamiento, entrenamiento, equipo, y apoyo en general por parte de un Estado para realizar sus operaciones, todas las acciones de dicho grupo resultan atribuibles al Estado que les brindó dicho apoyo, a pesar de que no todas sus operaciones y acciones hayan sido impuestas, solicitadas o dirigidas por dicho Estado.[70]

Posteriormente, en el Caso Genocidio Bosnia y Herzegovina alegaron frente a la CIJ que, entre otras cosas, Serbia y Montenegro

[67] *Prosecutor v. Dusko Tadic* [1999] (Appeal Judgement) ICTY § 97 [en lo sucesivo, "*Dusko Tadic*"].
[68] *Dusko Tadic*, § 98.
[69] *Dusko Tadic* §120.
[70] *DuscoTadic*, §122.

violaron su obligación de prevenir que el crimen de Genocidio se cometiera dentro de su territorio y de posteriormente extraditar a las personas que habían sido acusadas de cometer dicho crimen.[71]

A lo largo de su argumentación en este caso, la CIJ no solamente enfatizó la necesidad de aplicar el estándar de *control efectivo* establecido en el Caso Nicaragua cuando se trate de atribuir responsabilidad a un Estado con base en el artículo 8 de los Artículos de Responsabilidad Estatal[72], sino que expresamente citó la decisión del Tribunal Penal Internacional en el Caso Tadic y contradijo su interpretación. Lo anterior con base en los siguientes argumentos: i) el Tribunal Penal Internacional se había excedido en sus facultades en el Caso Tadic, al ser su jurisdicción exclusivamente criminal, el Tribunal Penal Internacional no tenía la competencia para decidir sobre cuestiones de responsabilidad estatal[73]; ii) el hecho de que el estándar de *control general* pueda ser utilizada para fines de determinar que un conflicto armado es de carácter de internacional, no quiere decir que dicha prueba pueda ser utilizada para responsabilizar al Estado por los actos de un grupo armado, pues son cuestiones de naturaleza distinta[74]; iii) debido a que existe un principio que establece que los Estados únicamente pueden ser internacionalmente responsables por sus propios actos, al haber

[71] *Genocide Convention Case* § 210
[72] *Genocide Convention Case*, § 401.
[73] *Genocide Convention Case* § 403.
[74] *Genocide Convention Case* § 405.

aplicado el estándar de *control general* el Tribunal Penal Internacional aumentó a niveles inaceptables la posibilidad de establecer la responsabilidad del Estado respecto de conductas que no fueron realizadas por sus propios órganos[75].

Como se aprecia de los casos anteriormente expuestos, la CIJ ha sido clara y consistente en cuanto al estándar que debe ser aplicado para acreditar que una persona o grupo de personas actuaron bajo la dirección o control de un Estado conforme al artículo 8 de los Artículos de Responsabilidad Estatal –el estándar de *control efectivo*–. Sin embargo, aún después de que fue emitido el fallo del Caso de Genocidio en 2007, algunos autores han establecido que, en virtud del anonimato y velocidad que caracterizan al ciberespacio, el estándar que debe aplicarse para atribuir responsabilidad a los Estados por ciberataques cometidos por una persona o grupo de personas que no sean órganos estatales *de jure*, debería de ser el de *control general* y no el de *control efectivo*.[76] Desde mi perspectiva, dicha propuesta carece de sustento al ir en contra de un principio fundamental del derecho de la responsabilidad internacional. Tal

[75] *Genocide Convention Case* §406.

[76] David E. Graham, "Cyber Threats and the Law of War", *Journal of National Security, Law & Policy*, 4:87 (2010), 87, 93; Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", *Georgetown Journal of International Law*, 42 (2010), 203; Scott J. Shackelford & Richard B. Andres "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem" *Georgetown Journal of International Law*, 42 (2010), 988.

como lo explicó la CIJ en el Caso de Genocidio, uno de los principios que rigen al derecho de la responsabilidad internacional establece que los Estados únicamente pueden resultar responsables por su propia conducta. En virtud de lo anterior, proponer la aplicación de un estándar—el estándar de *control general*— que no requiere acreditar que todas y cada una de las conductas de la persona o grupo de personas en cuestión fueron dirigidas y controladas por el Estado que se pretende imputar y efectuados a nombre y por cuenta del Estado, implica establecer un estándar contrario a la naturaleza y esencia del Derecho Internacional Público, cuyo sujeto son los Estados y no los particulares que habitan dentro del territorio de dichos Estados.[77]

Ahora bien, podría considerarse que un estándar tan riguroso por parte de la CIJ permite un amplio margen de actuación a los Estados para cometer actos ilícitos a través de terceros (actores no estatales). En virtud de lo anterior, en la doctrina se ha establecido que la obligación de los Estados de no permitir que su territorio se utilice para realizar actos contrarios a los derechos de otros Estados (que de ahora en adelante llamaré la obligación de debida diligencia)[78] constituye un estándar de atribución que permite establecer la responsabilidad directa de los Estados por conductas realizadas por

[77] Rosalyn Higgins, "Problems and Process: International Law and How to Use it" (Oxford, OUP, 1995), 39-55; *Genocide Convention Case,* §406.
[78] *Corfu Channel Case,* 22; *S.S Lotus Case (France v Turkey)* [1927] PCIJ Reports Series A No 10 (Dissenting opinion of Judge Moore), 88,89.

actores no estatales. Este estándar conlleva la ventaja de no ser tan riguroso como el estándar de *control efectivo* hasta ahora establecido por la CIJ.[79]

La discusión doctrinaria anteriormente planteada ha surgido a partir de los ataques terroristas de al Qaeda del 11 de septiembre de 2001 a las Torres Gemelas en Estados Unidos. Específicamente, la afirmación de que la obligación de debida diligencia constituye un estándar de atribución se basa en el lenguaje de algunas resoluciones emitidas por organismos internacionales y en el probable surgimiento de una norma de costumbre internacional. Aparentemente, esta norma encuentra sustento en el respaldo de la comunidad internacional de la decisión de Estados Unidos de atribuir responsabilidad directa al régimen Taliban por su falta de debida diligencia respecto de los ataques. Tras los sucesos del 11 de septiembre el entonces Presidente de Estados Unidos, George W. Bush, declaró que "*Estados Unidos no distinguiría entre los perpetradores de los ataques y aquellos que los albergan* [a los perpetradores]"[80]. Unos días más tarde, Bush solicitó al régimen Taliban "*la entrega al gobierno de Estados Unidos de todos los*

[79]Tal Becker, *Terrorism and The State: Rethinking the Rules of State Responsibility* (America del Norte, Hart Publishing, 2006) [en adelante "*Tal Becker, Terrorism and the State*"].

[80]A DAY OF TERROR. Bush Remarks to the Nation on the Terrorist Attacks https://www.nytimes.com/2001/09/12/us/a-day-of-terror-bush-s-remarks-to-the-nation-on-the-terrorist-attacks.html (traducción propia) (consultada el 4 de julio de 2018)

líderes de al Qaeda que se esconden en su territorio, la clausura de todos los centros de entrenamiento de terroristas y el acceso al gobierno de Estados Unidos a esos centros, con la finalidad de poder asegurarse de que realmente han dejado de operar". Asimismo, el Presidente reiteró que "*mediante la ayuda e incitación al homicidio, el régimen Taliban estaba cometiendo homicidio también, por lo que en caso de no cumplir con las demandas compartiría el mismo destino que los terroristas que cometieron los ataques*".[81] Sin embargo, el régimen no cumplió con estas demandas, por lo que en octubre de ese mismo año Estados Unidos dió inicio a ataques armados en su contra, invocando su derecho a la autodefensa, establecido en el artículo 51 de la Carta de las Naciones Unidas como una excepción al principio de no uso de la fuerza[82]. De esta manera, con base en el lenguaje utilizado en sus declaraciones oficiales y el posterior ejercicio de su derecho a la autodefensa, podría interpretarse que para Estados Unidos la falta de diligencia por parte del régimen Taliban respecto de los ataques terroristas de al Qaeda lo hizo directamente responsable por dichos ataques.

[81] Address to a Joint Session of Congress and the American People https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html (traducción propia) (consultada el 4 de julio de 2018).

[82] Carta de las Naciones Unidas (adoptada el 26 junio de 1945, entró en vigor el 24 de octubre de 1945) I UNTS XVI art. 51.

Si bien el texto de la Carta de las Naciones Unidas no establece expresamente que los Estados únicamente pueden ejercer el derecho a la autodefensa cuando han sido víctimas de un ataque armado por parte de otro Estado[83], en 2003 y 2004 la CIJ se pronunció al respecto y estableció que para que este derecho pueda ser ejercido de manera legal es necesario que el ataque armado contra un miembro de las Naciones Unidas sea atribuible a un Estado de conformidad con el derecho internacional[84]. Sin embargo, en ese momento (2001) ningún Estado se opuso al ejercicio por parte de Estados Unidos de su derecho a la autodefensa en contra del régimen Taliban, a pesar de que no le había atribuido responsabilidad por los ataques con base en los estándares establecidos en los Artículos de Responsabilidad

[83] Artículo 51 de la Carta de las Naciones Unidas: "*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.*"

[84] *Oil Platforms (Islamic Republic of Iran v. United States of America*) (Judgement) ICJ Rep 161 § 50 y 51 [en adelante "Oil Platforms Case"]; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* [2004] (Advisory Opinion) ICJ Rep 136, §139 [en adelante "The Wall Advisory Opinion"]. En ninguna de estas dos resoluciones la CIJ estableció que el ataque debe ser atribuible a un Estado "*de conformidad con el derecho internacional*". Sin embargo, considero que el lenguaje utilizado por la Comisión de Derecho Internacional en los Artículos de Responsabilidad Estatal, el *Nicaragua Case* y el *Genocide Convention Case* conducen a esta conclusión.

Estatal, sino por falta de debida diligencia. Por el contrario, gran parte de la comunidad internacional, incluyendo a algunas organizaciones internacionales, respaldaron este criterio. El 12 de septiembre de 2001 el Consejo de Seguridad adoptó en forma unánime la resolución 1368, misma que reafirma el derecho inherente de los Estados a la autodefensa y declara *inter alia* que aquellos [Estados] "*responsables de auxiliar, tolerar o albergar a los perpetradores, patrocinadores u organizadores de esos ataques serán considerados responsables*"[85]. La resolución 1373 posteriormente emitida por el Consejo de Seguridad de las Naciones Unidas también hace referencia al derecho inherente a la autodefensa[86]. La Organización de los Estados Americanos (OEA) y el Consejo de Europa también emitieron resoluciones que establecen que los Estados responsables de auxiliar, tolerar o albergar a los perpetradores, patrocinadores u organizadores serán igualmente considerados cómplices de esos actos y el derecho a la autodefensa puede ser ejercido en contra de esos Estados[87]. Asimismo, no solamente los Estados miembro de la OTAN sino muchos más

[85]UNSC Res 1368 (12 September 2001) UN Doc S/RES/1368. La traducción original de la Resolución 1368 establece que los Estados "*tendrán que rendir cuenta de sus actos*". Sin embargo, a mi parecer, el lenguaje original de la Resolución que establece que los Estados "*wil be held accountable*" más bien se refiere a que serán considerados responsables.

[86] UNSC Res 1373 (21 September 2001) UN Doc S/RES/1373.

[87] OAS Res RC23/RES1/01 (21 September de 2001); European Union Conclusions and Plan of Action of the Extraordinary European Council Meeting (21 September 2001).

miembros de la comunidad internacional como Japón, Jordania, Pakistan, Qatar, Turquía Albania y Azerbajan, entre otros, ofrecieron apoyo militar y logístico a Estados Unidos. Incluso Gran Bretaña participó junto con Estados Unidos en los ataques armados dirigidos al régimen Taliban justificando este acto en la tolerancia y apoyo brindado a los miembros de al Qaeda por parte del régimen[88].

Desde mi perspectiva esta visión es contraria a los criterios de la CIJ que he abordado a lo largo de este apartado. Por lo tanto, en aras de ser coherente con el orden argumentativo de este trabajo, en el siguiente apartado (que contiene el desarrollo de todas las normas primarias del Derecho Internacional Público que considero que fueron violadas en los casos anteriormente expuestos), abordaré cuestiones relacionadas con el contenido y naturaleza de la obligación de debida diligencia. Ahí mismo expondré también las razones por las que considero que esta obligación es una norma primaria y no un estándar de atribución como desde 2011 se ha comenzado a plantear.

[88] Tal Becker, *Terrorism and the State,* 214 - 215.

Las normas primarias del Derecho Internacional Público aplicadas a la actividad cibernética. El segundo elemento.

En el capítulo anterior se comprobó la aplicabilidad de los Artículos de Responsabilidad Estatal a los casos materia de estudio del presente trabajo. Sin embargo, de conformidad con lo establecido en el segundo elemento del artículo 2 de los Artículos de Responsabilidad Estatal, para poder determinar que un ciberataque es un hecho ilícito que genera la responsabilidad de los estados, también es necesario comprobar que constituyen una violación a las obligaciones internacionales de los Estados.

Con la finalidad de probar el segundo elemento anteriormente mencionado, en este capítulo expondré cuáles son los principios de derecho internacional que fueron violados por los Estados a los que se les atribuyó la comisión de los ciberataques. Es importante mencionar que, para dichos efectos, consideraré que la atribución de los ciberataques a los Estados mencionados en cada uno de los casos ha quedado firmemente establecida. De lo contrario, el contenido del presente capítulo carecería de sentido, ya que de nada sirve argumentar que los ciberataques son un acto violatorio de normas internacionales si dicho acto resulta ser imputable a un sujeto del sistema jurídico internacional, como lo son los Estados.

Caso Stuxnet

Principio de no uso de la fuerza

Se ha considerado que el ciberataque Stuxnet, dirigido a la planta nuclear de Natanz Irán, constituye un ataque armado y por lo tanto una violación al principio de no uso de la fuerza.[89] En los siguientes párrafos expondré cuál es el contenido de este principio y las razones por las cuales considero que, efectivamente, dicho ataque es un hecho internacionalmente ilícito por constituir una violación a dicho principio.

La prohibición de los Estados de hacer uso la fuerza establecida en el artículo 2(4) de la Carta de las Naciones Unidas es una norma de costumbre internacional de tipo *jus cogens.*[90] En virtud de lo

[89]Rusell Buchanan, *Cyber Attacks, Unlawful Uses of Force or Prohibited Interventions?* ?", *Journal of Conflict and Security Law* 17:2 (2014), 225-226 [en adelante "Rosell Buchanan, *Cyber Attacks: Unlawful Uses of Force of Prohibited Interventions?"*], 211; James P. Farwell & Rafal Rohozinski "Stuxnet and the Future of Cyber War", *Survival*, 53:1(2011); NATO research team calls Stuxnet attack on Iran an "act of force" https://www.rt.com/news/act-force-iran-cyberattack-831/ (consultada el 7 de julio de 2018).

[90] *Nicaragua Case*, §§187 -190; Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda) [2005] (Judgment) ICJ Rep 168 § 148; Guyana v Suriname (Award) PCA Case ICGJ 370 (2007) §§ 151, 202, 445; *Legality of the Threat or Use of Nuclear Weapons* [1996] (Advisory Opinion) ICJ Rep 1 § 70 – 73 § 87 [en adelante "*Nuclear Weapons Advisory Opinion"*]; Marco Roscini, *Cyber Operations and the Use of Force in International Law*, 44; F Grimal, Threats of Force: International law and strategy (Routledge, New York, 2013), 6; Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations UNGA Res 42/22 (18 November 1987) art. 2.

anterior, no resulta necesario que Estados Unidos, Israel e Irán formen parte de ningún tratado internacional que los obligue a respetar este principio. Sin embargo, lo que puede resultar problemático es la aplicabilidad de dicho principio al ámbito del ciberespacio.

De acuerdo con la doctrina, existen tres enfoques con base en los cuales se puede establecer si un ciberataque resulta ser violatorio del principio de no uso de la fuerza, el enfoque instrumental, el enfoque del objetivo, y el enfoque de los efectos.[91]

El enfoque instrumental. Este enfoque se refiere a los medios que fueron utilizados para realizar el ciberataque. Establece que, para que un determinado acto pueda considerarse violatorio del principio de no uso de la fuerza, el mismo debe haber sido realizado a través del uso de la fuerza armada. Dicho enfoque ha sido criticado por centrarse únicamente en las características físicas de los instrumentos que se utilizan en un ataque, dejando a un lado los efectos del mismo. En virtud de que es incierto si los recursos digitales pueden o no ser considerados un arma, el uso de este enfoque nos llevaría necesariamente a concluir que un ciberataque nunca podría resultar ser violatorio del principio de no uso de la fuerza, a pesar de que el mismo implicara la destrucción de objetos

[91] Marco Roscini, *Cyber Operations and the Use of Force in* International *Law*, 46-48.

físicos o daño a personas. En virtud de lo anterior, se descarta su aplicabilidad.[92]

El enfoque del objetivo. Este enfoque se refiere a la infraestructura que puede resultar afectada por el ciberataque. Establece que, siempre que un ciberataque afecte la infraestructura crítica del Estado al que fue dirigido, independientemente de los efectos que cause sobre dicha infraestructura, el ciberataque constituye una violación al principio de no uso de la fuerza. Esta postura ha sido criticada por ser demasiado incluyente, ya que implicaría calificar aquellas operaciones cibernéticas que únicamente causan pequeños inconvenientes o que simplemente se utilizan para robar información, como violatorias del principio de no uso de la fuerza.[93]

El enfoque de los efectos. Establece que cualquier ataque cibernético que resulte tener efectos destructivos sobre cierta propiedad, infraestructura crítica de un Estado o personas puede ser calificado como violatorio del principio de no uso de la fuerza. Sin embargo, el autor observa que dicho enfoque pierde de vista que existen ciberataques que, a pesar de no implicar la destrucción de objetos, propiedad o daño a personas, tienen efectos similares a los que

[92] *Ibidem*, 47.
[93] *Id.*,47.

podría tener un ataque realizado a través de cualquier otro medio que sí tuviera implicaciones físicas.[94]

Por un lado, considero que en este punto es necesario hacer énfasis en el hecho de que, tanto en la doctrina como en la jurisprudencia, se acepta que todo ataque armado constituye una violación al principio de no uso de la fuerza, pero no viceversa. Es decir, no todo uso de la fuerza constituye un ataque armado[95] En virtud de lo anterior, considero que los enfoques que se propone utilizar para analizar si un ciberataque implica o no una violación a dicho principio, son igualmente aplicables para analizar si un ciberataque constituye un ataque armado.[96]

Por otro lado, el grupo de expertos que elaboraron el Manual de Tallinn establecieron, en la regla 13, que los elementos que deben considerarse para determinar si un ciberataque constituye un ataque armado son la escala y los efectos de dicho ciberataque.[97] Lo anterior

---

[94] *Id.,* 50-52.

[95]*Nicaragua Case*, § 191, la CIJ determinó que (i) es necesario distinguir entre las formas más graves de uso de la fuerza y las que son menores[95]; (ii) la escala y los efectos de un determinado ataque son el parámetro que se debe utilizar para determinar si un ataque alcanza el estándar de ataque armado o si simplemente implica una violación menos grave al principio de no uso de la fuerza. Asimismo, la Regla 11 del Manual de Tallinn 1.0 establece que todo ataque armado implica una violación al principio de no uso de la fuerza.

[96]En los comentarios a la Regla 11 del Manual de Tallinn 1.0 se establece que la escala y efectos de un ciberataque también son elementos que también pueden ser considerados para establecer si el mismo implica o no una violación al principio de no uso de la fuerza.

[97] Manual de Tallinn 1.0, Regla 13.

lo hicieron tomando en consideración, entre otras cosas, que la CIJ, en su Opinión Consultiva de Armas Nucleares, estableció que los medios utilizados son irrelevantes para calificar un determinado acto como un ataque armado[98].

Al parecer la regla 13 del Manual de Tallinn y el enfoque de los efectos coinciden en que el elemento relevante para efectos de analizar una posible violación a dicho principio son los efectos del ciberataque. Asimismo, el uso de este enfoque para evaluar violaciones al principio de no uso de la fuerza es el más aceptado en la doctrina en virtud de que está basado en una interpretación de la Carta de las Naciones Unidas realizada con base en la Convención de Viena Sobre el Derecho de los Tratados[99]. En virtud de lo anterior, considero pertinente utilizar dicho enfoque para analizar el Caso Stuxnet.

En los comentarios a la regla 13 del Manual de Tallinn se establece que:

a. Un ciberataque que tiene como consecuencia la destrucción o daño a propiedad o personas satisface el criterio de escala

[98] Manual de Tallinn 1.0, Regla 13, comentario 3.
[99] Ziolkowski (ed.), "Ius ad Bellum in Cyberspace –Some Thoughts on the "Schmitt Criteria" for Use of Force", *NATO CCD COE Publication* (2013), 298-299.

y efectos necesario para ser calificado como un ataque armado.

b. Un ciberataque dirigido a la infraestructura crítica de un Estado que cause un daño severo a dicho Estado puede ser calificado como un ataque armado, aunque no implique la destrucción física o daño a propiedad o personas.

En virtud de lo anteriormente expuesto, es posible deducir que el principio de no uso de la fuerza se viola cuando un Estado realiza una determinada operación cuya escala y efectos es tan grave que resulta en la destrucción de propiedad, daño físico causado a personas, o bien daño a la infraestructura crítica de un Estado. Esto último con independencia de que la operación implique destrucción o daño causado a objetos o personas.

La escala y efectos del ciberataque Stuxnet, realizado por Estados Unidos e Israel, fue tan grave que resultó en la destrucción parcial de infraestructura crítica –las centrífugas de enriquecimiento de uranio- de la planta nuclear de Natanz. En virtud de lo anterior, no solamente se acredita el elemento de destrucción física, sino también el hecho de fue dirigido a infraestructura crítica de Irán, causando un daño severo a la misma. Por lo tanto, Stuxnet resulta ser violatorio del principio de no uso de la fuerza al constituir un ataque armado dirigido a Irán.

Caso Sony Pictures

Principio de no intervención

Considero que el ciberataque realizado a Sony Pictures en 2014 constituye una violación, por parte de Corea del Norte al principio de no intervención. A continuación expondré el contenido y alcances de dicho principio y posteriormente explicaré su aplicabilidad al caso concreto con la finalidad de probar que el ciberataque fue un acto ilícito de Corea del Norte que genera su responsabilidad internacional.

El principio de no intervención deriva del derecho internacional consuetudinario.[100] Tradicionalmente, en el sistema jurídico internacional y hasta el siglo XX, este principio se entendía necesariamente ligado al uso de la fuerza. Es decir, solamente se consideraba que había sido violado cuando un Estado intervenía en los asuntos internos de otro a través del uso o amenaza de uso de la fuerza, más no cuando se utilizaban medios coercitivos de distinta naturaleza.[101] Sin embargo, la interpretación de dicho principio ha evolucionado y en la actualidad se entiende que puede ser violado independientemente de que se incumpla o no con otros principios.

[100] *Nicaragua Case*, § 202; Carta de las Naciones Unidas, art. 2(1), *Corfu Channel Case*, 35.

[101] Damrosh, Lori Fisler, "Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs", *American Journal of International Law* (1989) 83(1): 1-50, 3

Es decir, se trata de un principio autónomo cuya violación no depende de que se viole el principio de no uso de la fuerza.[102]

En cuanto al contenido del principio de no intervención, la CIJ en la sentencia del Caso Nicaragua, estableció que éste prohíbe a los Estados intervenir, directa o indirectamente, en los asuntos que, en virtud de su soberanía, competen exclusivamente a otros Estados. Una intervención es ilegal cuando un Estado interviene, a través de medios coercitivos, en los asuntos que competen exclusivamente a otro Estado. [103]Lla CIJ hizo especial énfasis en que el elemento coercitivo define y conforma la esencia del principio de no intervención.[104]

En virtud de lo anterior, es posible deducir que para acreditar una violación al principio de no intervención es necesario que (i) el acto reclamado sea susceptible de ser calificado como un acto coercitivo; (ii) la intervención verse sobre asuntos que competen exclusivamente al Estado víctima.

---

[102]Jamnejad, Maziar & Wood, Michael, "The Principle of Non-intervention", *Leiden Journal of International Law* 22:2, (2009), 345-381 [en lo sucesivo, "Jamnejad, Maziar & Wood, Michael, The Principle of Non-intervention"]; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1984] (Separate Opinion of Judge Hennins) ICJ Rep 14, 534.

[103] *Nicaragua Case*, § 202.

[104] *Nicaragua Case*, §204.

Las dudas que inmediatamente surgen respecto de dichos elementos son: ¿qué actos pueden ser calificados como actos coercitivos y qué actos no? ¿cuáles son los asuntos de competencia exclusiva de los Estados en el sistema jurídico internacional?

Respecto de la primera pregunta, en la doctrina se considera que son actos coercitivos aquellos que un Estado realiza con la intención de forzar un cambio en cierta política adoptada por otro Estado.[105] Por ejemplo, el ciberataque dirigido a Estonia en 2007 fue una intervención coercitiva en los asuntos internos de dicho país, ya que aparentemente la finalidad de dicho ciberataque era forzar al gobierno de Estonia a revertir la política que había adoptado de remover la estatua del soldado de bronce.[106]

Respecto de cuáles son los asuntos que competen exclusivamente al Estado, es pertinente mencionar la decisión de la Corte Permanente de Justicia Internacional (en lo sucesivo "CPJI") en el *Caso Lotus (Francia v. Turquía)* de 1927. En este caso la CPIJ estableció que, fuera de su territorio, los Estados únicamente pueden realizar actos que se encuentran expresamente permitidos en el sistema jurídico internacional, ya sea por un tratado o una norma de costumbre internacional. En cambio, dentro de su territorio, los Estados pueden

[105]Jamnejad, Maziar & Wood, Michael, *The Principle of Non-intervention*, 348.
[106]Rusell Buchan, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?

realizar todos aquellos actos que no se encuentren expresamente prohibidos en el sistema jurídico internacional.[107] Esta regla establecidas por la CPIJ en el Caso Lotus fue reiterada recientemente por la CIJ en la Opiniones Consultivas de Kosovo.[108] De lo anteriormente expuesto se desprende que todos aquellos aspectos que no se encuentren expresamente regulados por el derecho internacional, deben ser considerados competencia exclusiva de cada Estado, por lo que otros Estados no pueden intervenir en estas decisiones, salvo que una norma expresa de derecho internacional se los permitiera.

La aplicabilidad del principio de no intervención en el ámbito del ciberespacio ha sido aceptada por la doctrina. En la Regla 10 del Manual de Tallinn 1.0 los expertos internacionales establecieron que la violación a dicho principio por medio de un ciberataque es factible siempre y cuando tenga fines coercitivos. En virtud de lo anterior, el ciber espionaje u otro tipo de operaciones cibernéticas carentes del elemento coercitivo no constituyen una violación a este principio.[109]

Una vez expuesto el contenido y los elementos que es necesario acreditar para establecer una violación al principio de no

[107] *SS Lotus Case*, 18;
[108] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* [2010] (Advisory Opinion) ICJ Rep 403, § 79 [en adelante "*Kosovo Advisory Opinion"*].

[109] Manual de Tallinn 1.0, Regla 10.

intervención, así como la aplicabilidad de este principio al ámbito de ciberespacio, procederé a argumentar por qué el ciberataque a Sony Pictures constituye una violación a este principio.

En la doctrina se ha establecido que el ciberataque a Sony Pictures no constituye una violación al principio de no intervención porque no fue dirigido directamente al gobierno de Estados Unidos sino a Sony Pictures, una empresa privada.[110]Al respecto, considero que es necesario enfatizar que, de conformidad con lo anteriormente expuesto, lo que resulta relevante para evaluar si existe o no una violación al principio de no intervención no es el blanco de la operación cibernética, sino su objetivo, es decir, si es un acto coercitivo realizado con la intención de forzar un cambio en las políticas internas o externas de un Estado. El ciberataque dirigido a Sony Pictures cumple con los elementos necesarios —el elemento coercitivo y la intervención en una competencia exclusiva del estado víctima— para actualizar una violación al principio de no intervención.

El elemento coercitivo

De conformidad con los hechos del caso Sony Pictures, Corea del Norte denunció la película *"The Interview"* ante Naciones Unidas y

[110]Michael N. Schmitt, International Law and Cyber Attacks: Sony v. Korea https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (consultada el 23 de diciembre de 2015).

amenazó con tomar medidas en caso de que Estados Unidos apoyara, tácita o explícitamente, el lanzamiento de la película. A pesar de lo anterior, Estados Unidos no se opuso al lanzamiento y estreno de la película.

El elemento coercitivo del ciberataque radica en el hecho de que los objetivos del ciberataque fueron ciudadanos de Estados Unidos, los empleados de Sony Pictures, y una empresa localizada dentro de su territorio y, por lo tanto, protegida por su soberanía: Sony Pictures. Además el ciberataque tuvo lugar con posterioridad a las amenazas por parte de Corea del Norte de tomar medidas si Estados Unidos apoyaba, tácita o explícitamente, el lanzamiento de la película, y con anterioridad al estreno de la misma. De lo anterior se deriva que el ciberataque fue un acto realizado con la finalidad de que Estados Unidos cambiara su decisión de no intervenir con el lanzamiento y estreno de la película.

La competencia exclusiva del Estado víctima

Existe normativa internacional que establece la prohibición de los Estados de interferir con los sistemas de comunicación o servicios radioeléctricos de otros Estados.[111] En este sentido, Cuba ha

[111]El Artículo 45 de la Constitución de la Unión Internacional de Telecomunicaciones establece que "*Todas las estaciones, cualquiera que sea su objeto, deberán ser instaladas y explotadas de tal manera que no puedan causar interferencias perjudiciales a las comunicaciones o servicios radioeléctricos de otros Estados Miembros, de las empresas de explotación reconocidas o de*

declarado que la difusión de transmisiones extranjeras dentro de su territorio constituyen una violación a su soberanía y a la normativa prevista en en algunos instrumentos internacionales.[112] Asimismo, cuando menos una resolución de la Asamblea General de las Naciones Unidas establece el derecho de los Estados y sus ciudadanos a desarrollar, sin intervención externa, sus sistemas de información y medios masivos de comunicación, y a utilizar dichos medios para promover sibility of Intervention and Interference in the Internal Affairs of States UNGA Res 36/103 (9 December 1981) , II(c).us aspiraciones e intereses políticos, sociales y culturales.[113]

De conformidad con el criterio de la CIJ, las resoluciones de la Asamblea General pueden tener cierto valor normativo a pesar de no ser vinculantes, ya que en algunos casos constituyen evidencia de la existencia de una norma de costumbre o, por lo menos, de uno de sus elementos (*opinio iuris*). Sin embargo, esto debe determinarse con base en un análisis de cada resolución con la finalidad de evaluar *inter alia* su contenido, las circunstancias y el contexto en el que

aquellas otras debidamente autorizadas para realizar un servicio de radiocomunicación y que funcionen de conformidad con las disposiciones del Reglamento de Radiocomunicaciones. […]"

[112]Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/64/129/Add.1 (9 de septiembre de 2009).

[113]Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States UNGA Res 36/103 (9 December 1981) , II(c).

fueron adoptadas. Por ejemplo, para analizar si existía suficiente *opinio iuris* respecto de la ilegalidad del uso de armas nucleares, la CIJ consideró el número de votos y abstenciones que existían en una serie de resoluciones de la Asamblea General que establecían que el uso de este tipo de armas debía prohibirse en virtud de que constituye una violación directa a la Carta de las Naciones Unidas. Una vez analizadas las resoluciones, la CIJ concluyó que en virtud de que habían sido adoptadas con una cantidad substancial de votos en contra y numerosas abstenciones no existía suficiente *opinio iuris* respecto de la ilegalidad del uso de armas nucleares.[114]

A diferencia de lo que sucede con las resoluciones de la Asamblea General en materia nuclear, la resolución en materia de telecomunicaciones anteriormente citada fue adoptada con un total de 120 votos a favor, 22 en contra y 6 abstenciones.[115] Además, no solamente reafirma la existencia y prevalencia del principio de no intervención, sino que relaciona el contenido de ese principio con el derecho de los Estados y sus ciudadanos de desarrollar, sin

[114] *Nuclear Weapons Advisory Opinion* § 70 – 73.

[115] La cantidad de votos a favor, en contra y abstenciones de esta resolución pueden ser consultados en http://unbisnet.un.org:8080/ipac20/ipac.jsp?session=15308W7912O5C.348963&menu=search&aspect=power&npp=50&ipp=20&spp=20&profile=voting&ri=&index=.VM&term=A%2FRES%2F36%2F103&matchoptbox=0%7C0&oper=AND&x=13&y=8&aspect=power&index=.VW&term=&matchoptbox=0%7C0&oper=AND&index=.AD&term=&matchoptbox=0%7C0&oper=AND&index=BIB&term=&matchoptbox=0%7C0&ultype=&uloper=%3D&ullimit=&ultype=&uloper=%3D&ullimit=&sort=

interferencia externa, sus sistemas de información y medios masivos de comunicación. De esta manera puede considerarse que, dado el contexto en el que el derecho de los Estados fue adoptado y la cantidad de votos a favor de su contenido existe, cuando menos suficiente *opinio iuris* respecto de la ilegalidad de la intervención de los Estados en los sistemas de información y medios masivos de comunicación de otros Estados. Lo anterior aunado al hecho de que las sentencias de Yahoo! Inc., Google Inc., entre otras, mencionadas en el primer apartado constituyen prueba de que existe una práctica reiterada por parte de los Estados de regular el contenido al que pueden acceder sus ciudadanos, podría afirmarse que existe una norma de costumbre internacional que establece que los Estados no pueden intervenir directa o indirectamente en los sistemas de información y comunicación masiva de otros Estados.

En virtud de lo anterior, es factible considerar que el ciberataque dirigido a Sony Pictures, implica una intervención indirecta por parte de Corea del Norte en un asunto que compete exclusivamente a Estados Unidos [el desarrollo de su sistema de información y medios masivos de comunicación] y, por lo tanto, una violación al principio de no intervención.

Obligación de debida diligencia

La obligación de debida diligencia fue establecida en el derecho internacional por primera vez en 1928 por la Corte Permanente de

Trail Smelter Case (US v Canada) (1941) UNRIAA Vol III at 1965; Eritrea Ethiopia Claims Commission, Civilians Claims, Ethiopia's Claim No 5, 17 December 2004, at 11Arbitraje (en lo sucesivo la "CPA") en el caso de la Isla de Palmas. En dicha resolución la CPA estableció lo siguiente: "[…]*una de las principales consecuencias que se derivan del principio de soberanía es que los estados tienen la obligación de proteger, dentro de sus propios territorios, los derechos de los demás Estados…[…]*".[116] Esta obligación ha sido reafirmada en múltiples ocasiones en materia ambiental[117], en el ámbito de los derechos humanos[118] y por la CIJ, la cual resolvió por primera vez en este sentido en 1948 en el caso del Canal de Corfu y ha repetido la existencia de esta obligación en sentencias y opiniones consultivas posteriores[119].

Un ejemplo de cómo aplica la debida diligencia que deben tener los Estados respecto de su obligación de no permitir que su territorio sea utilizado para realizar actos que afecten los derechos de otros estados

[116] *Island of Palmas Arbitration*, 829 y 839.

[117] *Trail Smelter Case* (*US v Canada*) (1941) UNRIAA Vol III at 1965; Eritrea Ethiopia Claims Commission, Civilians Claims, Ethiopia's Claim No 5, 17 December 2004, at 11; *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] (Judgment) ICJ Rep 14 § 101

[118] *Velazquez-Rodriguez Case (Velazquez-Rodríguez vs. Honduras)* [1988] (Judgement) ICHR *§172*

[119] *Case concerning United States Diplomatic and Consular staff in Tehran* (*United States of America v* Iran) [1980] (Judgment) ICJ Rep 3 §§ 69-75 [en adelante "*Tehran Hostages Case*"]; *Nuclear Weapons Advisory Opinion* § 29; *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* [2007] (Judgment) ICJ Rep 43 *§429,430*

es el caso del Canal de Corfu. En este caso una explosión de minas suscitada en las aguas territoriales de Albania resultó en la pérdida de vidas humanas y el daño irreparable de varios buques británicos.[120] Gran Bretaña demandó a Albania frente a la CIJ argumentando que Albania era directamente responsable por la explosión de las minas en virtud de que las había colocado en ese lugar, a sabiendas de que tarde o temprano los buques ingleses pasarían por ahí. Sin embargo, Gran Bretaña no presentó evidencia que probara, más allá de toda duda razonable, que había sido Albania quien había colocado las minas en sus aguas territoriales[121]. La CIJ estableció firmemente que el hecho de que un suceso de esta magnitud hubiese tenido lugar dentro del territorio de Albania no era suficiente para atribuirle responsabilidad por el mismo. Sin embargo, en virtud de la estricta vigilancia que Albania había mantenido sobre sus aguas territoriales durante los días previos a la explosión y de la posibilidad de observar la puesta de las minas desde los lugares en los que los oficiales albanenses vigilaban sus aguas, seguramente se había, cuando menos, percatado de que las minas habían sido colocadas en sus aguas territoriales. A pesar de contar con el tiempo suficiente para advertir a los buques británicos de la presencia de las minas, no hizo nada por prevenir la explosión. En virtud de lo

[120] *Corfu Channel Case, 13.*
[121] *Corfu Channel Case,* 20.

anterior, la falta de acción por parte de Albania implicaba una violación a su obligación de debida diligencia.[122]

Como podemos observar en la sentencia de la CIJ, la responsabilidad que se le atribuyó a Albania no fue directa por la explosión de las minas ni porque las explosiones sucedieron dentro de su territorio, sino porque la CIJ determinó que había pruebas suficientes para determinar que Albania sabía de la existencia de las minas y omitió tomar medidas para prevenir la explosión de los buques ingleses, a pesar de que pudo haberlo hecho. Es decir, el acto atribuible a Albania fue la omisión de tomar medidas para prevenir que las minas causaran daño a los buques ingleses, lo cual derivó en un incumplimiento de su obligación de debida diligencia.

La sentencia de la CIJ en el caso del Canal de Corfu es acorde al derecho de la responsabilidad internacional. El artículo 2 de los Artículos de Responsabilidad Estatal establece claramente que la responsabilidad internacional de un Estado se suscita cuando un acto u omisión atribuible a dicho estado resulte en la violación de sus obligaciones internacionales[123], por lo que si pudiera establecerse que existe una Obligación de Debida Diligencia en el ámbito del ciberespacio, esta obligación resultaría aplicable en este caso y podría, eventualmente, argumentarse que fue violada por Corea del

[122] *Corfu Channel Case*, 22.
[123] DARSIWA, art. 2.

Norte. Sin embargo, antes de abordar la discusión respecto de la existencia de esta norma en el ámbito del ciberespacio, considero necesario establecer con claridad (i) cuáles son los elementos que deben cumplirse para acreditar que un Estado incumplió con su Obligación de Debida Diligencia; (ii) cuál es el estándar de prueba que debe acreditarse para establecer que incumplió con dicha obligación y, por último; (iii) si la Obligación de Debida Diligencia es aplicable en el ciberespacio.

Elementos que deben acreditarse

Tal como se deriva de la sentencia del caso de Canal de Corfu, para poder establecer que un Estado incumplió con su Obligación de Debida Diligencia es necesario acreditar que el Estado: (i) sabía que era probable que el hecho sucedería; y (ii) que existían medidas que podría haber tomado para prevenir la realización de dicho acto; (iii) el Estado no tomó dichas medidas.

Lo anterior encuentra sustento en el caso *Personal Diplomático y Consular de los Estados Unidos en Teherán (Estados Unidos v. Irán)* (en lo sucesivo "Caso Teherán"). En este caso, un grupo de estudiantes iraníes invadieron la embajada de Estados Unidos en Teherán y mantuvieron al personal de dicha embajada como sus rehenes. Al momento de las invasiones, Estados Unidos e Irán eran parte de una serie de tratados internacionales que los obligan a proteger las premisas diplomáticas del otro Estado y a su personal

diplomático y consular.[124] La CIJ concluyó que el gobierno de Irán (i) sabía que era probable que la invasión a la embajada de Estados Unidos sucediera en virtud de que sucedió en un contexto de tensión diplomática entre Estados Unidos e Irán y se habían llevado a cabo varias manifestaciones afuera de algunas embajadas[125]; (ii) existían medidas que Irán podía haber tomado para prevenir la invasión de la embajada, ya que con anterioridad había prevenido ataques a otras embajadas[126]; (iii) las autoridades de Irán no tomaron dichas medidas[127]; (iv) Irán tampoco detuvo el ataque a la embajada a pesar de las llamadas de auxilio del personal de la misma[128]. En virtud de lo anterior, Irán era responsable por no haber tomado medidas para prevenir que los estudiantes atacaran la embajada de Estados Unidos.[129]

Como podemos observar de los casos anteriormente expuestos, por un lado existe la Obligación de Debida Diligencia y por otro lado existen las condiciones con base en las cuales se juzga si un Estado cumplió o no con dicha obligación. La debida diligencia que deben tener los Estados respecto de la obligación previamente mencionada, se refiere a las acciones u omisiones del Estado en relación con los

[124] *Tehran Hostages Case*, §68.
[125] *Tehran Hostages Case*, §§14, 15, 16 y 17.
[126] *Tehran Hostages Case*, §68.
[127] *Tehran Hostages Case*, §68.
[128] Tehran Hostages Case, §18.
[129] *Tehran Hostages Case*, §§61-68.

actos realizados, dentro de su territorio o jurisdicción, que pudieran resultar en una violación a los derechos de otros Estados.

Por ejemplo, si un Estado A resulta afectado por las acciones de una persona o grupo de personas que se encontraban dentro del territorio de un Estado B, o que utilizaron el territorio de dicho estado B para violar los derechos del Estado A, entonces el Estado A tendrá que acreditar que el Estado B (i) sabía que era probable que dichos actos se llevaran a cabo; y (ii) existían medidas razonables que dicho Estado podría haber adoptado o implementado para prevenir que estos actos sucedieran. Si estos dos elementos se prueban, entonces el Estado B resultará responsable por haber violado su Obligación de Debida Diligencia. Por el contrario, si el Estado B logra acreditar que a pesar de que tomó medidas preventivas al respecto, los actos fueron realizados, el Estado B no resultaría ser responsable por haber violado dicha obligación.

La necesidad de acreditar dicho elemento se desprende de que el sistema jurídico internacional no impone a los Estados la obligación de asegurar que su territorio no será utilizado para realizar conductas contrarias a los derechos de los Estados, es decir, una obligación de resultado. Más bien esta obligación consiste únicamente en adoptar e implementar medidas razonables que contribuyan a la disuación, terminación o persecución de dichas conductas, es decir, es una

obligación de medios.[130] De lo anterior se desprende que no existen medidas pre establecidas que un Estado debe o no debe adoptar con la finalidad de cumplir con esta obligación, ya que no todos los Estados tienen la misma capacidad económica y estructural para cumplir con esta obligación. Sin embargo, sí se ha considerado que, el hecho de que un Estado adopte políticas o medidas que de una manera u otra faciliten la comisión de actos que resulten violatorios de los derechos de otros Estados, implica que dicho Estado no es diligente respecto de la prevención de dichos actos.[131] Por lo tanto, al momento de determinar si un Estado cumplió o no con su Obligación de Debida Diligencia, es necesario considerar las capacidades de dicho Estado en relación con la magnitud y características del acto que resultó ser violatorio de los derechos de otro Estado.[132]

Aplicabilidad de la obligación de debida diligencia al ámbito digital

De conformidad con lo mencionado anteriormente, la existencia y aplicabilidad de la obligación de debida diligencia se reconoce, desde hace muchos años, en la jurisprudencia y la doctrina internacionales. Sin embargo, la aplicación de esta obligación respecto de operaciones cibernéticas realizadas por actores no

[130] Tal Becker, *Terrorism and the State*: *Rethinking the Rules of State Responsibility*, 141.
[131] *Ibidem*, 133.
[132] *Ibidem*, 132.

estatales es un punto controversial. Hay autores que afirman que esta obligación se extiende a las operaciones cibernéticas realizadas por actores no estatales dentro del territorio de un Estado que tenga efectos extraterritoriales adversos.[133] Asimismo, en la versión 2.0 del Manual de Tallinn, los expertos internacionales coincidieron en que la obligación de debida diligencia es aplicable respecto de operaciones cibernéticas realizadas por actores no estatales. Lo anterior bajo el argumento de que "*en varios regímenes especiales del derecho internacional, esta obligación claramente se ha cristalizado en virtud del grave peligro que los actores no estatales implican para los Estados*."[134] Por lo tanto, para dichos expertos esta obligación cubre todas aquellas "[…]*operaciones cibernéticas que, aunque no violen, per se, una norma de derecho internacional, tengan consecuencias extraterritoriales adversas […]*, los expertos internacionales pusieron especial atención en el hecho de que *"las operaciones cibernéticas son un medio ideal para causar daño en otros Estados*". Sin embargo, finalmente advirtieron que no todas las operaciones cibernéticas que tienen efectos extraterritoriales adversos están cubiertas por la obligación de debida diligencia, sino solamente aquellas en las que "[…]*actores no estatales realicen una*

[133] Michael N. Scmitt, "In Defence of Due Diligence in Cyber Space", *The Yale Law Journal Forum,* 125 (2015) [en adelante "Michael N. Schmitt, Due Diligence in Cyberspace"]; Beatrice A. Walton, "Duties Owed: Low Intensity Cyber Attacks and Liability for Transboundary Torts in International Law", *The Yale Law Journal* 126:1460 (2017).
[134] Manual de Tallinn 2.0, Regla 6, § 21.

conducta que afecte el derecho de otro Estado, esto es, si la conducta hubiese sido realizada por el Estado desde cuyo territorio los actores no estatales están actuando, hubiese implicado la violación de una obligación internacional de dicho Estado".[135]

De lo anteriormente citado se desprende que, de conformidad con el criterio de los expertos internacionales en el Manual de Tallinn 2.0, a) en virtud de que la obligación de debida diligencia existe en varios regímenes especiales, ésta se ha cristalizado al ámbito del derecho internacional general; b) los Estados podrían incurrir en una violación de su obligación de debida diligencia en caso de no ejercerla respecto de aquellas operaciones ciberneticas realizadas por actores no estatales que causen daño en el territorio de otro Estado; y sean contrarios a las obligaciones del Estado desde cuyo territorio se están realizando.

Las afirmaciones mencionadas en el párrafo anterior contienen cuestiones con las que no coincido, por lo que considero que valdría la pena analizarlas a la luz de los principios del Derecho Internacional Público. Por un lado, considero que es técnicamente incorrecto proponer la aplicación de la obligación de debida diligencia respecto de aquellas operaciones cibernéticas que, "además de causar daño en el territorio de otro Estado, sean contrarias a las obligaciones del Estado desde cuyo territorio se

[135] Manual de Tallinn 2.0, Regla 6, § 21-22.

cometen". De conformidad con lo establecido en los Artículos de Responsabilidad Estatal y en los comentarios hechos por la Comisión de Derecho Internacional a dicho artículo, el daño no es un elemento que, de manera general, debe acreditarse para establecer la responsabilidad de un Estado. La necesidad de acreditar la existencia de un daño es más bien un requisito que, en su caso, será determinado por el contenido de la norma primaria relevante en el caso concreto.[136] Dicha norma primaria sería la obligación del Estado desde cuyo territorio se comete la operación[137], misma que se traduce en el derecho del Estado víctima. Por ejemplo, imaginemos que existe una norma de derecho internacional que establece que el Estado A tiene la obligación de prevenir que se cause un daño. En caso de que el Estado A omita tomar las medidas necesarias para prevenir que se cause ese daño, ha incumplido con su obligación internacional. Independientemente de que se acredite o no que la omisión del Estado A efectivamente ha causado un detrimento. En otras ocasiones, puede suceder que, al formar parte de un tratado internacional, los Estados Parte adquieran la obligación de incorporar ciertas normas a su marco jurídico nacional. Por ejemplo, el artículo 4 de la "Convención para la Represión de los Ataques Terroristas Cometidos con Bombas" se establece la obligación de los Estados Parte de tipificar como delito, en su

[136] DARSIWA, art. 2(9), art. 31(6)
[137] DARSIWA, comentario general.

régimen jurídico interno, las ofensas establecidas en el artículo 2 de dicha convención. En caso de que cualquiera de los Estados Parte no tipificase como delito dichas ofensas estaría incumpliendo con su obligación internacional de tipificar, independientemente de que esa omisión cause o no inconveniente a otros Estados. De esta manera, puede entenderse que los Estados incumplen con sus obligaciones internacionales en el momento en el que omiten realizar el mandato que contiene la norma, independientemente de que se cause un daño por esa omisión o no. En virtud de lo anterior, a diferencia de lo que proponen los expertos internacionales en el Manual de Tallin 2.0, el daño no debería ser considerado un elemento que, de manera general, debe ser tomado en cuenta para evaluar el incumplimiento de un Estado con sus obligaciones internacionales. Dicho análisis dependerá, más bien, del caso concreto y en particular de los elementos que contenga la norma primaria que se considere violada.

Por otro lado, considero que es jurídicamente incorrecto afirmar que la Obligación de Debida Diligencia debería aplicar respecto de aquellas operaciones que, en caso de haber sido cometidas por el Estado desde cuyo territorio se realizaron, implicarían la violación de las obligaciones internacionales de dicho Estado. Es un principio fundamental de Derecho Internacional Público que los Estados tienen libertad de actuación respecto de todo aquello que no está expresamente regulado por una norma de Derecho Internacional

Público[138]. Por lo tanto, el ámbito de aplicación de la obligación de debida diligencia está expresamente delimitado por las normas que conforman el sistema de Derecho Internacional Público. Es decir, los únicos actos respecto de los cuales el Estado tiene la obligación de tomar medidas son aquellos que se encuentran expresamente prohibidos por una norma Derecho Internacional Público, ya que su realización viola los derechos de otros Estados. Los actores no estatales no son sujetos de los derechos y obligaciones contenidas en el sistema de Derecho Internacional Público general, resulta jurídicamente imposible que sus actos constituyan una violación a los derechos de los Estados[139]. En virtud de lo anterior, los Estados tienen, *prima facie,* libertad de actuación respecto de los actos realizados por actores no estatales dentro de su territorio, a pesar de que dichos actos tengan efectos o consecuencias extraterritoriales.

Para que un Estado incurra en responsabilidad internacional es necesario que exista nexo entre el evento que se reclama y el Estado[140], esta es precisamente la lógica sobre la que se fundamenta y debe operar el derecho de la responsabilidad estatal. Por esta razón,

[138]*SS Lotus Case, 19; Kosovo Advisory Opinion,* §79.

[139]Oliver De Frouville, "Attribution of conduct to the State: Private Individuals" en "*Oxford Commentaries on International Law, The law of International Responsibility*", James Crawford, Allan Pellet y Simon Olleson (Oxford, OUP, 2010), 276-277 [en adelante "Oliver de Frouville, *Attribution of Conduct to the State: Private Individuals*"].

[140]Oliver de Frouville, *Attribution of Conduct to the State: Private Individuals,* 259- 261.

tal como se expuso anteriormente, los Artículos de Responsabilidad Estatal únicamente contemplan situaciones en las que el acto fue realizado por órganos *de jure* del Estado, personas o entidades que, aunque no sean órganos *de jure,* están facultados por el ordenamiento jurídico interno de los Estados para ejercer actos de autoridad o personas o grupos de personas que, bajo las condiciones que se plantearon, pueden ser consideradas un órgano *de facto* del Estado.[141]

Por lo tanto, una norma cuyo parámetro de aplicación es "en caso de que ese acto hubiese sido realizado por un Estado, implicaría la violación de sus obligaciones internacionales" resta seguridad jurídica a los Estados y de ninguna manera favorece la legitimidad y estabilidad que se buscan en cualquier sistema jurídico. Las operaciones cibernéticas realizadas por actores no estatales no pueden ser atribuidas a los Estados por el simple hecho de haber sido cometidas desde su territorio[142], ya que no existe un nexo entre la conducta realizada por el actor no estatal y el Estado. Por otro lado, al día de hoy no existe ninguna norma primaria del Derecho Internacional Público que regule las operaciones cibernéticas realizadas por actores no estatales, por lo que el parámetro de

[141]DARSIWA, arts. 4-10; Luigi Condorelli and Klauss Kress, "The Rules of Attribution: General Considerations" en "*Oxford Commentaries on International Law, The law of International Responsibility*", James Crawford, Allan Pellet y Simon Olleson (Oxford, OUP, 2010), 228-229.
[142]*Corfu Channel Case,* 18.

aplicación de la obligación de debida diligencia respecto de este tipo de conductas no se encuentra, aún, expresamente delimitado.

Lo anterior no quiere decir que, actualmente, no existan normas de carácter primario en el sistema jurídico internacional que regulen la conducta de los Estados respecto de actos realizados por actores no estatales dentro de su territorio. Como se expuso anteriormente, este tipo de normas existen en el derecho ambiental, en el derecho internacional de los derechos humanos y en regímenes de obligaciones estatales para prevenir y suprimir el terrorismo, entre otros. Sin embargo, a diferencia de lo que los expertos internacionales sostienen en el Manual de Tallinn 2.0., en mi opinión no es tan claro que estas normas se han cristalizado al ámbito del Derecho Internacional Público general. Particularmente, no es claro si una norma o principio que surge como *lex specialis* o pertenece a un régimen auto-contenido del Derecho Internacional Público de conformidad con el artículo 55 de los Artículos de Responsabilidad Estatal puede, eventualmente, cristalizarse en el Derecho Internacional Público general. Tampoco es claro si los sujetos de algunas de las normas que han surgido en regímenes autocontenidos continúan siendo los Estados y la conducta de actores no estatales tipificada en dichas normas es únicamente un elemento catalítico de

la responsabilidad del Estado[143] o si, bajo un criterio de *lex specialis* es posible atribuir responsabilidad directa a los Estados por actos realizados por actores no estatales.

[143] Oliver de Frouville, *Attribution of Conduct to the State: Private Individuals*, 276; R. Ago, Fourth Report on State Responsibility, ILC Yearbook 1972, Vol. II, 71, 97, §65-120.

CONCLUSIÓN

Si bien en un primer momento el debate sobre remoción de contenido pone en tela de juicio la eficacia de los principios del sistema jurídico internacional, también es cierto que la flexibilidad que lo caracteriza funge un papel importante con respecto a la misma. Actualmente, existe la posibilidad de que se formule costumbre internacional que contribuya a homogenizar el alcance de la jurisdicción de los Estados respecto del contenido y los datos almacenados en servidores que se encuentran localizados dentro del territorio de otros Estados. Si bien hasta esta fecha podría considerarse que la infraestructura cibernética se encuentra protegida por la soberanía del Estado en cuyo territorio se encuentra, el 23 de marzo de 2018 Estados Unidos emitió una nueva legislación en materia digital llamada "Clarifying Lawful Overseas Use of Data", popularmente conocida como CLOUD Act. Entre otras cosas, esta legislación establece la facultad de las autoridades administrativas de Estados Unidos de solicitar a las empresas que se encuentran localizadas en dicho territorio cualquier información que se encuentre bajo su poder o resguardo, independientemente de que ésta se encuentre almacenada en servidores establecidos fuera del territorio estadounidense.

En virtud de que esta nueva legislación implica que la autoridad ejerza jurisdicción sobre un servidor que se encuentra fuera de su territorio, en principio podría considerarse que la sola emisión y

puesta en práctica de esta legislación implica una violación a la soberanía del Estado en cuyo territorio se encuentre el servidor que contiene la información solicitada por las autoridades estadounidenses. Sin embargo, en caso de que la comunidad internacional no se oponga al ejercicio e implementación por parte de Estados Unidos de esta nueva legislación, podría eventualmente argumentarse la conformación de una nueva norma de costumbre internacional que permite a los Estados ejercer su jurisdicción dentro del territorio de otros Estados para efectos de obtener información que se encuentre ahí localizada. Es altamente probable que esta nueva regulación junto con la regulación recientemente emitida por la Unión Europea en materia de protección de datos personales (GDPR) constituyan un cambio importante respecto de cómo se aplica el Derecho Internacional Público, cuando menos en materia de ciberseguridad[144].

Lo anterior podría suceder con respecto al debate de remoción de contenido. En caso de que los Estados no acuerden expresamente sobre el alcance del ejercicio de su jurisdicción en este sentido, es altamente probable que una aceptación tácita por parte de los mismos en caso de que el TJUE confirme la resolución del CNIL podría dar pie a la formulación de una nueva norma de costumbre internacional

[144] Este tema se aborda con mayor profundidad en: Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking" *Stanford Law Review Online* 71 (2018).

respecto de la facultad de los Estados de ejercer su jurisdicción sobre servidores localizados dentro del territorio de otros Estados para efectos de implementar obligaciones en materia de protección de datos personales. Sin embargo, este análisis requiere tiempo de implementación y funcionamiento de la nueva legislación que permita evaluar el comportamiento de los Estados y las interpretaciones judiciales al respecto.

Ahora bien, a pesar de que el estándar de *control efectivo* reiterado por la CIJ sea acorde a los principios de Derecho Internacional Público, su aplicabilidad y funcionalidad práctica podría llegar a ser cuestionada. Lo anterior se debe a que, en ciertas circunstancias, resulta difícil obtener los medios de prueba necesarios para satisfacer un estándar tan alto. La obtención de evidencia directa en el ámbito digital resulta ser altamente compleja. El "spoofing" es fácil y los códigos maliciosos se encuentran siempre encriptados y configurados de tal forma que el rastreo de su verdadero origen es, sino imposible, muy difícil y costoso de descifrar. Por otro lado, los Estados casi siempre se encuentran con una terrible barrera para obtener evidencia directa (testigos, poder detener e interrogar a quienes probablemente participaron directamente en el ciberataque, periciales del servidor del que pudo haber emanado el ataque) se encuentran en el territorio del otro Estado.

En virtud de lo anterior, algunos autores han propuesto como solución la atribución de responsabilidad indirecta a los Estados. Es decir, atribuirles responsabilidad por incumplir con su obligación de debida diligencia y no por la comisión del ciberataque en sí misma. Lo anterior, de conformidad con la jurisprudencia de la CIJ, permitiría reducir el estándar de prueba y utilizar evidencia indirecta para establecer la responsabilidad del Estado.[145]

Otros autores han establecido que la CIJ debería de permitir una reversión de la carga de la prueba.[146] Sin embargo, el Caso de Canal de Corfu se estableció claramente que una reducción en el estándar probatorio no implica una reversión de la carga de la prueba.[147] Por lo tanto, sería poco probable que en el contexto de un litigio la CIJ admita dicha reversión.

Otros autores han propuesto que el estándar de prueba se reduzca aún más de lo que se reduce cuando es necesario probar que los Estados incumplieron con su obligación de debida diligencia.[148] Sin embargo, "*El estándar de prueba no fue creado para poner a la víctima en una situación de desventaja, sino para proteger al*

[145] Michael N. Schmitt, Due Diligence in Cyberspace.
[146] Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations" *Texas International Law Journal*, 50 (2014), 245 [en lo sucesivo, "Marco Roscini, *Evidentiari Issues in International Disputes"*]
[147] *Corfu Channel Case,* 18.
[148]David E. Graham, Cyber Threats and the Law of War, 4 J. NAT'L SECURITY L. & POL'Y 87, 93 (2010)

acusado de acusaciones falsas, las cuales, gracias a herramientas como spoofing, enrutamiento de cebola, y el uso de botnets son de particular riesgo en e ámbito del ciberespacio"[149]. En virtud de lo anterior, considero que dicha propuesta resulta ser poco factible e inapropiada. Provocaría una pérdida de legitimidad del sistema jurídico internacional en virtud de que muy probablemente en la mayoría de los casos se atribuiría responsabilidad a Estados inocentes.

Hasta esta fecha la CIJ no ha establecido reglas claras respecto del estándar probatorio, los medios de prueba o el tipo de evidencia —directa o indirecta— que deben presentarse y acreditarse dependiendo del cargo que se le atribuye al Estado demandado. Si bien existen sentencias donde dicho tribunal se ha pronunciado respecto de ciertas reglas que podrían resultar aplicables en caso de buscar atribuir responsabilidad a un Estado[150], no se han establecido reglas o lineamientos claros respecto de cuál es el estándar de prueba que debe satisfacerse en relación con la acusación en el caso concreto. En este sentido, sería recomendable que tribunales como la CIJ establezcan criterios claros respecto de los estándares que es necesario satisfacer para efectos de probar el incumplimiento con un

[149] Marco Roscini, *Evidentiary Issues in International Disputes,* 251.
[150] *Corfu Channel Case*; *Genocide Convention Case*; *Oil Platforms Case.*

determinado principio o norma perteneciente al sistema jurídico internacional.

BIBLIOGRAFÍA

Jurisprudencia

Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo [2010] (Advisory Opinion) ICJ Rep 403, § 79 [en adelante "*Kosovo Advisory Opinion"*].....55, 70

Asunto C-131/12, Sentencia del Tribunal de Justicia Europeo (Gran Sala), *Google Spain, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, 13 de mayo de 2014. [en adelante "*Caso Costeja*"]. 20

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) [2007] (Judgment), ICJ Rep 43 § 210 [en lo sucesivo "*Genocide Convention Case*"]. .....

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda) [2005] (Judgment) ICJ Rep 168 § 148 48

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)

Otras autoridades

Tratados Internacionales

Regulaciones domésticas

Articulos de Revista

Michael N. Scmitt, “In Defence of Due Diligence in Cyber Space”, *The Yale Law Journal Forum,* 125 (2015) 66

Roland R. Foulke, “Definition and Nature of International Law*”,* *Columbia Law Review,* 19:6 (1919): 429-466.....7

Rusell Buchanan, *Cyber Attacks, Unlawful Uses of Force or Prohibited Interventions? ?*”, *Journal of Conflict and Security Law* 17:2 (2014), 225-226 .....48, 55

Scott J. Shackelford & Richard B. Andres “State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem” *Georgetown Journal of International Law,* 42 (2010), 988. 41

Scott J. Shackelford, “State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem”, *Georgetown Journal of International Law,* 42 (2010).....41

Sean Kanuck, “Sovereign Discourse on Cyber Conflict Under International Law” *Texas Law Review* 88:7 (2010),

Thomas Schultz, “Carving up the Internet: “Jurisdiction, Legal Orders, and the Private/Public International Law Interferface” *European Journal of International Law,* 19:4 (2008), 812. 18

Libros

Noticias

Obama ordered wave of cyber attacks against Iran http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (consultada el 8 de noviembre de 2017). 31

Obama ordered wave of cyber attacks against Iran http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (consultada el 9 de noviembre de 2017) 30

Revela *Times* que Obama incrementó los ciberataques contra el programa nuclear iraní http://www.jornada.unam.mx/2012/06/02/mundo/023n2mun (consultada el 16 de diciembre de 2015) 29

Sony Report Employee http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf (consultado el 12 de diciembre de 2015). 32

Stuxnet Worm Attack on Iranian Nuclear Facilities, Michael Holloway http://large.stanford.edu/courses/2015/ph241/holloway1/ (consultada el 2 de noviembre de 2017). 28

Stuxnet: la filtración de un ciberataque
http://www.proceso.com.mx/346707/stuxnet-la-filtracion-de-un-ciberataque (consultada el 5 de noviembre de 2017) 29

The Guardian, Sony Cyber Attack linked to North Korean Government, FBI says http://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official (consultada el 10 de diciembre de 2015).....34

Update on Sony Investigation
https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (consultada el 15 de diciembre de 2015) 33

Documentales

Documental “Zero Days”; Virus infecta planta nuclear iraní
http://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw.shtml (visto el 15 de mayo de 2016).....29