101 PERÍODO ORDINARIO DE SESIONES
1 – 10 de agosto de 2022
Rio de Janeiro, Brasil

OEA/Ser. Q
CJI/doc. 671/22 rev.2 corr.1
25 octubre 2022
Original: español

INFORME DEL COMITÉ JURÍDICO INTERAMERICANO.

SEGUNDO INFORME: EL DERECHO INTERNACIONAL APLICABLE AL CIBERESPACIO

1. INTRODUCCIÓN

Este informe fue originalmente elaborado por la doctora Mariana Salazar Albornoz, en su calidad de relatora. Corresponde a su segundo informe en la materia, documento que en su última revisión ante el pleno del Comité fue aprobado por consenso por todos sus miembros. En este informe, comenzamos describiendo las nociones de ciberespacio y de ciberoperaciones, para después adentrarnos en un análisis de las implicaciones que pueden tener este tipo de operaciones para el Derecho Internacional a partir de ejemplos de ciberoperaciones estatales que han ocurrido a lo largo de las últimas dos décadas. Posteriormente, examinamos los principales procesos de negociación intergubernamental y académica que han existido y continúan existiendo para contribuir a dilucidar el alcance de la aplicabilidad del derecho internacional existente al ciberespacio, incluyendo, desde luego, la labor que ha realizado el Comité Jurídico Interamericano. Finalmente, presentamos una visión general de los principales temas específicos del derecho internacional que están siendo discutidos en torno a su aplicación al ciberespacio, aclarando en lo posible las posiciones oficiales que han adoptado los pocos Estados de la región americana que a la fecha se han pronunciado en la materia. Con ello, esperamos que el informe sirva de herramienta útil para los numerosos Estados de la región americana que se encuentran en proceso de preparar sus posiciones nacionales oficiales sobre esta relevante temática del alcance de la aplicación del Derecho Internacional al ciberespacio.

2. CIBERESPACIO Y CIBEROPERACIONES.

El término "ciberespacio" proviene del griego *kybernetes,* que significa 'el arte de manejar un navío' y que alude a la cibernética –el estudio del control remoto a través de dispositivos–. El término se utilizó por primera vez en 1960 en el título *'Atelier Cyberspace',* utilizado por la artista Susanne Ussing y el arquitecto Carten Hoff para denominar su obra de instalaciones sensoriales e imágenes. La primera asociación del término a lo digital, si bien para fines novelísticos, fue en la década de los ochentas, cuando el escritor canadiense-americano de ciencia ficción, William Gibson, lo utilizó en su cuento "Quemando Cromo" y en su novela '*Neuromante'.* En esta última, lo describió como:

> "*Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones* […]*... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información."*[1]

La palabra fue retomada con el auge del internet en la década de los noventas. El propósito de referirse al 'ciberespacio' vino inicialmente aparejado con la concepción de que el internet era un espacio

[1] GIBSON, W., *Neuromante,* Minotauro, 1996 (traducción al español del original en inglés *Neuromancer,* Ace Books, 1984), p. 35.

o dominio distinto al del 'mundo real', y por ende debía ser una jurisdicción separada, exenta de la aplicación del poderío de los Estados y de sus leyes, sino regida por la voluntad de sus usuarios[2]. La idea generó un doble debate: por un lado, si realmente el ciberespacio se trata de un dominio o espacio distinto, y, por el otro lado y en consecuencia, si debe o no regirse por normas jurídicas.

En este debate, diversas voces han dilucidado que el internet y otras partes que constituyen el ciberespacio son redes de comunicación situadas dentro del espacio real, y por tanto no se trata de un espacio distinto: el ciberespacio incluye tanto los componentes físicos (hardware) como los digitales.[3] Delerue, por ejemplo, aclara que el ciberespacio no es un quinto dominio o ámbito de aplicación del derecho, sino un medio que puede utilizarse para conducir actividades en cualquiera de los cuatro ámbitos físicos existentes: tierra, mar, espacio aéreo y espacio ultraterrestre.[4] Dias y Coco, a su vez, se refieren al ciberespacio no como un espacio virtual o separado, sino como un conjunto de tecnologías digitales multidimensionales –o tecnologías de la información y comunicación (TIC)– que están plenamente integradas con actividades humanas que tienen lugar en diferentes dominios físicos o espacios del 'mundo real'.[5] El Manual de Tallin 2.0 (al que nos referiremos con más detalle más adelante) define el ciberespacio como *el ambiente formado por componentes físicos y no-físicos, para almacenar, modificar e intercambiar datos usando redes computacionales*[6].

Una "ciberoperación" u operación cibernética es la utilización de capacidades cibernéticas con la finalidad principal de alcanzar sus objetivos en o a través del uso del ciberespacio[7]. Este término abarca sólo los actos que tienen lugar dentro de una red computacional, con lo cual la conducción de algún acto hostil físico contra una computadora o red computacional –por ejemplo la destrucción del disco duro de una computadora con un arma cinética– no calificaría como una ciberoperación. Las ciberoperaciones forman parte creciente de nuestras vidas cotidianas.

Al no tratarse de un ámbito distinto ni exento de jurisdicción, las ciberoperaciones o actividades conducidas a través del ciberespacio deben respetar las normas jurídicas aplicables. El derecho no prohíbe *per se* las ciberoperaciones: por el contrario, éstas han venido a facilitar nuestras vidas e interacciones significativamente. Sin embargo, un uso malicioso de éstas sí puede llegar a constituir una violación al derecho internacional, como se expone en la siguiente sección.

3. CIBEROPERACIONES MALICIOSAS Y SUS IMPLICACIONES PARA LOS ESTADOS

El siglo XXI ha sido el siglo de la digitalización, lo cual ha sido exacerbado aún más a raíz de las medidas de aislamiento que acompañaron la pandemia del COVID-19 que azoró al mundo en los últimos años. A su vez, el uso creciente de las TIC y su interconexión e interdependencia han venido también a exponer los inmensos riesgos que entraña el mal uso de éstas, pudiendo poner al descubierto información delicada de gobiernos, empresas o particulares o dañar sistemas o infraestructura vital.

Las ciberoperaciones maliciosas se dirigen contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo último de perjudicar a personas, instituciones o empresas. Se pueden clasificar de diversas maneras y pueden causar daños a software, a hardware, a

---

[2] Véase, por ejemplo: BARLOW, J.P., *Declaración de Independencia del Ciberespacio,* proclamada en 1996, disponible en español en: http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf. Para un excelente recuento del origen del término véase, por ejemplo: DIAS, T. & COCO, A., *Cyber due diligence in international law,* Oxford Institute for Ethics, Law and Armed Conflict, 2022, pp. 39-48.

[3] EASTERBROOK, F.H., "Cyberspace and the Law of the Horse", *University of Chicago Legal Forum* 207, 1996, p. 207.

[4] DELERUE, F., *Cyber Operations and International Law,* Cambridge University Press, 2020, pp. 11-12.

[5] DIAS, T. & COCO, A., *Cyber due diligence in international law,* Oxford Institute for Ethics, Law and Armed Conflict, 2022, pp. 47-48.

[6] SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, 2017, p. 564.

[7] *Ibidem.*

datos, así como a personas físicas (individuos) y morales (Estados, empresas y organizaciones no gubernamentales). Una sola ciberoperación puede causar daños a varias de estas categorías. Una de las clasificaciones más comunes para las ciberoperaciones maliciosas que dañan software, hardware y datos es la denominada "tríada de la CIA"[8], por sus siglas en inglés. Conforme a ésta, una ciberoperación maliciosa puede dañar:

(i) La *confidencialidad,* a través de un acceso no autorizado a computadoras, sistemas y redes informáticas para obtener cierta información;

(ii) La *integridad,* al alterar, borrar, corromper o denegar el acceso a ciertos datos o software; o

(iii) La *disponibilidad*, al disrumpir parcial o totalmente el funcionamiento de una red o sistema de computación.

Los tipos más comunes de ciberoperaciones maliciosas incluyen:

(i) El *phishing*, que consiste en "el envío de mensajes fraudulentos, usualmente a través de correo electrónico, que aparentemente proceden de fuentes fiables y seguras" con el objetivo de "robar datos personales muy sensibles, como información sobre inicios de sesión o datos de tarjetas de crédito, entre otros."[9];

(ii) El *malware,* que es el "software malicioso que incluye virus y gusanos", que "aprovecha […] las vulnerabilidades para infringir las redes y suele atacar cuando un usuario hace clic en un enlace o en un archivo adjunto a un *email*", y cuyo impacto "va desde la instalación de software dañino al bloqueo del acceso a componentes claves de la red *(ransomware)* o a la obtención furtiva de información *(spyware)"*[10]*;*

(iii) La *inyección de SQL* o lenguaje de consulta estructurado, que "se produce cuando un hacker inserta un código malicioso en un servidor que utiliza SQL, forzándolo a desvelar información protegida o que normalmente no revelaría"[11]; y

(iv) El *ataque de denegación de servicio distribuido* (o DDoS por sus siglas en inglés), que "provoca la saturación de los sistemas, los servidores e, incluso, las redes con tráfico con el objetivo de agotar los recursos y el ancho de banda", generando como consecuencia la incapacidad para completar las solicitudes legítimas[12].

Las ciberoperaciones maliciosas tienen, a su vez, efectos nocivos sobre personas físicas y morales. Como lo indican Dias y Coco, será raro encontrar instancias en las que las ciberoperaciones que causen daños a software, hardware o datos no causen efectos significantes sobre personas, sean tangibles o intangibles. Como mínimo, se generarán costos de ciberseguridad para identificar las vulnerabilidades y el alcance del daño y, de ser necesario, repararlo.[13] Los daños a personas físicas pueden incluir afectaciones al medio ambiente, a su salud, integridad, vida, privacidad, educación o acceso a la información y libertad de expresión, entre otros. En el caso de personas morales, incluyendo Estados, empresa y organizaciones no gubernamentales, una ciberoperación maliciosa puede generarle pérdidas financieras significantes, altos costos legales y daños a su reputación y confiabilidad.

Tratándose particularmente de Estados, una ciberoperación maliciosa puede dañar sistemas de gobierno, servicios financieros, y servicios estatales esenciales como la electricidad, el agua, el

---

[8] Véase, por ejemplo: WALKOWSKI, D., ¿Qué es la tríada de la CIA?", *Computer Weekly,* 2019, disponible en: https://www.computerweekly.com/es/opinion/Que-es-la-triada-de-la-CIA

[9] Iberdrola, *Ataques Cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos?,* disponible en: https://www.iberdrola.com/innovacion/ciberataques

[10] *Ibidem.*

[11] *Ibidem.*

[12] *Ibidem.*

[13] DIAS, T. & COCO, A., *op. cit. supra* nota 2, pp. 99-100.

suministro de alimentos y medicinas, servicios médicos o sistemas de transportes y de seguridad, entre otros. Tales ciberoperaciones contra Estados pueden provenir no sólo de entes privados sino también de otros Estados que las realizan directamente (a través de sus órganos u agencias) o indirectamente a través de entes o personas que contratan.

Las décadas recientes han visto numerosas ciberoperaciones maliciosas que han involucrado o afectado significativamente a Estados[14]. La atribución es una cuestión delicada, ya que a la fecha ningún Estado ha reconocido directamente su responsabilidad por la realización directa o indirecta de una cibeoperación maliciosa. Sin embargo, la información disponible de varias ciberoperaciones que han afectado a Estados en las últimas décadas ha llevado en ocasiones al país afectado a asumir que se han tratado de operaciones conducidas en su contra por otros Estados. Como lo indican Finnemore y Hollis, entre 2010 y 2020, se calcula que 28 Estados – incluyendo China, Irán, la República Popular Democrática de Corea, Rusia, Reino Unido y Estados Unidos – han sido acusados de realizar o apoyar ciberoperaciones con impactos graves sobre gobiernos, pueblos y recursos[15]. Describiremos algunos ejemplos de casos a continuación.

Uno de los primeros y más representativos casos –debido a los desarrollos que generó[16]– fue la campaña de ciberoperaciones maliciosas que sufrió Estonia en 2007, que ese país atribuyó a Rusia. Inhabilitó durante 22 días numerosos sitios web de organizaciones de Estonia, incluyendo el parlamento, bancos, ministerios, periódicos y medios de comunicación. El motivo fue el desacuerdo con Rusia en torno a la reubicación de un monumento de la era soviética en la ciudad de Tallin.

En 2010, el malware *Stuxnet*, que algunos atribuyen a Israel y a Estados Unidos, atacó los sistemas computacionales de cinco instalaciones nucleares en Natanz, en Irán: el gusano tomó el control de 1,000 máquinas que participaban en la producción de materiales nucleares y dio comandos para que las centrifugadoras se destruyeran. Se considera que fue la primera vez que un ataque cibernético logró dañar infraestructura física[17].

En 2015, la red eléctrica de Ucrania se vio interrumpida por un ataque cibernético a través del malware llamado *BlackEnergy,* que ese país atribuye a Rusia en el marco de la guerra iniciada en 2014. Se trató del primer ciberataque contra infraestructura crítica que ocasionara un apagón y el primero a una red eléctrica que se realizara de manera enteramente remota.[18] Desconectó 30 subestaciones eléctricas y ocasionó que unas 80,000 personas se quedaran sin electricidad durante seis horas. Afectó también a diversas compañías distribuidoras y a un total de 225,000 clientes.[19]

En 2015 y 2016, un ciberataque infiltró la red computacional del Comité Democrático Nacional de los Estados Unidos, espiando comunicaciones, correos electrónicos y documentos y filtrándolos, para interferir en las elecciones presidenciales estadounidenses de 2016. Este ciberataque fue seguido de una

---

[14] Para un recuento de los principales ciberataques estatales, véase por ejemplo: DELERUE, F., *op. cit. supra* nota 4, Apéndice, pp. 499-501.

[15] FINNEMORE, M. y HOLLIS, D., "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity", en The European Journal of International Law, Vol. 31 No. 3, 2020, pp. 969-1003, en p. 970.

[16] Véase, por ejemplo: CALERO, F.J., " Heli Tiirmaa-Klaar: «Los ciberataques no caen del cielo, suceden por razones políticas»", en *ABC Internacional,* 2019, disponible en: https://www.abc.es/internacional/abci-heli-tiirma-klaar-ciberataques-no-caen-cielo-suceden-razones-politicas-201911050326_noticia.html

[17] Véase, en este sentido: "El virus que tomó control de mil máquinas y les ordenó autodestruirse", en *BBC News*, 11 octubre 205, disponible en: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[18] Véase: BROEDERS, D., DE BUSSER, E., CRISTIANO, F. & TROPINA, T., "Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?", *Journal of Cyber Policy,* 7:1, 2022, pp. 97-135, en pág. 108.

[19] Véase, por ejemplo: TIDY, J., "Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente", en *BBC News,* 24 marzo 2022, disponible en: https://www.bbc.com/mundo/noticias-60850173#:~:text=En%202015%2C%20la%20red%20el%C3%A9ctrica,en%20el%20oeste%20de%20Ucrania.&text=Pie%20de%20foto%2C,visto%20afectada%20anteriormente%20por%20ciberataques

campaña de "trolls" en redes sociales para influenciar al electorado estadounidense. Estados Unidos atribuye el ataque a las agencias de inteligencia de Rusia.

En 2017, el ransomware *WannaCry,* atribuido por algunos a grupos vinculados a Corea del Norte, afectó alrededor de 230,000 computadoras con sistema operativo Microsoft Windows en más de 150 países alrededor del mundo. Se considera el ataque de ransomware más grande de la historia. Los países más afectados fueron Rusia, Ucrania, India y Taiwán, así como partes del servicio nacional de salud de Reino Unido (NHS), la compañía Telefónica de España, FedEx de Estados Unidos, Deutsche Bahn de Alemania y las aerolíneas LatAm, entre otros. Generó costos globales de alrededor de 7,000 millones de dólares. En el mismo año 2017, el ransomware *NotPetya,* atribuido por algunos a Rusia, golpeó diversas organizaciones en Ucrania, incluido su banco central, hospitales, aeropuertos y empresas estatales de energía eléctrica, así como empresas privadas, antes de extenderse a sistemas en otros 63 Estados en Europa y a Estados Unidos. Provocó en total daños por más de 10,000 millones de dólares, con lo cual se le ha considerado el ciberataque más devastador en la historia[20]. También en 2017, el ransomware *BadRabbit* afectó medios de comunicación en Rusia y organizaciones de infraestructura crítica en el sector de transportes en Ucrania.

En 2020 y 2021, el ciberataque contra la empresa estadounidense de software *SolarWinds,* que algunos atribuyen a los servicios de inteligencia de Rusia, se extendió a los clientes de la compañía afectando la base de datos de más de 18,000 empresas a nivel mundial (incluyendo Microsoft, Cisco, Intel y Deloitte) y de agencias federales clave del gobierno de los Estados Unidos (incluyendo los Ministerios de Seguridad Interior, de Estado, de Energía, de Finanzas y la Administración Nacional de Seguridad Nuclear). El ataque generó a la empresa Solarwinds costos de 40 millones de dólares en los primeros nueve meses de 2021, y un promedio de 12 millones de dólares a cada cliente afectado.

La guerra que actualmente tiene lugar entre Rusia y Ucrania no ha estado exenta del uso de ciberataques para acompañar las actividades cinéticas[21]. Desde la anexión ilegal de Crimea en 2014, Ucrania ha sido objeto de continuos ciberataques atribuidos a Rusia. Un día antes de la invasión del 24 de febrero de 2022, se lanzó el ciberataque *Foxblade,* que buscó eliminar los datos de las redes computacionales de 19 entidades gubernamentales y entidades de infraestructura crítica del gobierno ucraniano. Desde la invasión y hasta finales de junio de 2022, Microsoft calcula que han existido ciberataques dirigidos a redes computacionales de 48 agencias y empresas dentro de Ucrania, así como intentos de penetración de redes y ciberespionaje a 128 organizaciones en 42 Estados aliados a Ucrania[22]. El efecto ha sido limitado, debido a que Ucrania ha recibido gran refuerzo en sus capacidades de ciberdefensa por parte de diversos Estados, empresas y organizaciones de la sociedad civil. Por ejemplo, la información y operaciones digitales ucranianas se han protegido a través de su traslado a la nube pública, almacenada en centros de datos en otros lugares de Europa. Algunos expertos no descartan la posibilidad de que Rusia esté esperando el momento oportuno para lanzar un ciberataque masivo con efectos mucho más destructores.[23]

---

[20] Véase, por ejemplo: BROEDERS, D., DE BUSSER, E., CRISTIANO, F. & TROPINA, T., *op. cit. supra* nota 18, en pág. 117; TIDY, J., *op. cit. supra* nota 19.

[21] Véase, a este respecto: ORENSTEIN, M., "Russia's Use of Cyberattacks: Lessons from the Second Ukraine War", en *Foreign Policy Research Institute,* June 7, 2022. Disponible en: https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

[22] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War,* 22 de junio, 2022, págs. 2-3, disponible en: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK . Véase también: Microsoft, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine,* abril 2022, disponible en: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[23] Véase: European Parliament, *Russia's War on Ukraine: Timeline of cyber-attacks*, Briefing, June 2022, Unión Europea, disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

4. LA APLICABILIDAD DEL DERECHO INTERNACIONAL AL CIBERESPACIO: PROCESOS MULTILATERALES Y ACADÉMICOS

Cuando comenzaron los ciberataques inter-estatales como los antes descritos, académicos y gobiernos tornaron su atención a determinar si es que el derecho internacional resulta aplicable o no al ciberespacio y, en caso afirmativo, en qué medida o aspectos. La cuestión es de relevancia ya que, con muy contadas excepciones, el derecho internacional no tiene reglas específicamente redactadas para regular el ciberespacio, y las principales normas del derecho internacional surgieron mucho antes de que la tecnología cibernética fuera una realidad y, por tanto, no la contemplan. Los únicos dos tratados internacionales existentes relacionados con el ciberespacio son, por un lado, la Convención de Budapest sobre el Cibercrimen, del Consejo de Europa[24], y, por el otro, la Convención de la Unión Africana sobre la Seguridad Cibernética y la Protección de Datos Personales[25] que aún no está en vigor. Ninguno de estos, sin embargo, se refiere específicamente a la cuestión sobre las ciberoperaciones realizadas por, o en contra de, Estados. Los desarrollos para dilucidar esta cuestión se han dado tanto en el ámbito académico como en el intergubernamental.

4.1 Los Manuales de Tallin

En el año 2009, el Centro de Excelencia en Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (CCDCOE, por sus siglas en inglés), una organización militar internacional basada en Tallin, reunió a un grupo de expertos internacionales independientes para producir un manual, no vinculante, sobre el derecho internacional existente aplicable a la ciberguerra. Como resultado del ejercicio, en 2013 el grupo produjo el *Manual de Tallin sobre el Derecho Internacional Aplicable a la Ciberguerra*[26]*,* que, además de reafirmar que los principios generales del derecho internacional aplican al ciberespacio, identificó 95 reglas y desarrolló sus respectivos comentarios en temas de soberanía, responsabilidad de los Estados, *jus ad bellum,* derecho internacional humanitario y las leyes de neutralidad en lo concerniente a la guerra cibernética. Tras su publicación, CCDCOE convocó a un nuevo grupo de expertos independientes internacionales para realizar una investigación y ampliación de la cobertura del manual, a fin de abarcar también el derecho internacional aplicable a las actividades cibernéticas ocurridas en tiempos de paz. Como resultado, en 2017 se publicó el *Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Ciberoperaciones*[27], que identifica 154 reglas que rigen las ciberoperaciones y desarrolla sus respectivos comentarios. Dados los avances recientes en la práctica y posicionamiento de los Estados, en 2021 la CCDCOE lanzó el proyecto, que tendrá una duración de cinco años, para la realización del Manual de Tallin 3.0, para revisar capítulos existentes y explorar nuevos temas de importancia para los Estados[28].

---

[24] Council of Europe, Budapest Convention on Cybercrime, ETS No. 185, en vigor desde el 7 de enero de 2004.
[25] African Union Convention on Cyber Security and Personal Data Protection, adoptada el 27 de junio de 2014, aún no en vigor. Ha sido ratificada por 13 Estados (se requieren 15 para su entrada en vigor).
[26] SCHMITT, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.
[27] SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op. cit. supra* nota 6.
[28] Véase, en este sentido: https://ccdcoe.org/research/tallinn-manual/

4.2 Procesos intergubernamentales en las Naciones Unidas y posicionamientos de los Estados

El tema de la seguridad de la información ha formado parte del programa de las Naciones Unidas desde 1998, tras una propuesta presentada por Rusia[29]. Desde 2004, la Asamblea General de las Naciones Unidas ha creado grupos de expertos gubernamentales (GGE, por sus siglas en inglés) en seis ocasiones para examinar las amenazas reales y potenciales en esa esfera y recomendar medidas para abordarlas. Los GGE adoptaron inicialmente informes de consenso en 2010[30], 2013[31] y 2015[32]. Desde el informe de 2013 se reconoció expresamente que "*[e]l derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías."*[33] Además, el informe de 2015 incluyó 11 normas voluntarias, no vinculantes, sobre el comportamiento responsable de los Estados en el ciberespacio, con recomendaciones sobre medidas de construcción de confianza, capacidad y cooperación[34].

El GGE que sesionó entre 2016 y 2017 no logró producir un informe de consenso debido a desacuerdos que giraron en torno, principalmente, a la forma en que el derecho internacional aplica al ciberespacio y a cuáles elementos de derecho internacional se debían considerar primero. La prevalencia de esos desacuerdos impidió que en 2018 la Asamblea General de Naciones Unidas alcanzara un acuerdo de consenso sobre el formato que se debía seguir para reanudar las discusiones. Ante ello, se determinó la adopción, por votación dividida, de dos resoluciones distintas: por un lado, se adoptó una resolución patrocinada por Rusia que creó un Grupo de Trabajo de Composición Abierta[35] (OEWG, por sus siglas en inglés), y por el otro se adoptó una resolución patrocinada por Estados Unidos que creó un nuevo GGE[36].

Ambos procesos del OEWG y del GGE se condujeron en paralelo entre 2019 y 2021, con mandatos muy similares pero composiciones muy distintas. El OEWG, que fue presidido por el Embajador Jurg Lauber, de Suiza, estuvo abierto a la participación de todo Estado interesado e incluyó consultas con otros actores (industria, sociedad civil y academia). Adoptó su informe final por consenso

---

[29] Véase, en este sentido: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/ Asamblea General de las Naciones Unidas, Resolución A/RES/53/70, "Los avances de la informatización y las telecomunicaciones en el contexto de la seguridad internacional", 4 enero 1999.

[30] Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional,* U.N. Doc. A/65/201 (30 de julio de 2010). El Grupo sesionó entre 2009 y 2010 y estuvo compuesto por expertos de 15 Estados (dos de la región de las Américas: Brasil y Estados Unidos).

[31] Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional,* 19, U.N. Doc. A/68/98 (24 de junio de 2013) ("Informe GGE 2013"). El Grupo sesionó entre 2012 y 2013 y estuvo compuesto por expertos de 15 Estados (tres de la región de las Américas: Argentina, Canadá y Estados Unidos).

[32] Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, 10, U.N. Doc. A/70/174 (22 de julio de 2015) ("Informe GGE 2015"). El Grupo sesionó entre 2014 y 2015 y estuvo compuesto por 20 expertos gubernamentales (cuatro de la región de las Américas: Brasil (quien presidió), Colombia, Estados Unidos y México).

[33] Informe GGE 2013, *op. cit. supra* nota 31, párr. 19.

[34] Informe GGE 2015, *op. cit. supra* nota 32.

[35] Asamblea General de las Naciones Unidas, Resolución A/RES/73/27, "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", 5 de diciembre de 2018.

[36] Asamblea General de las Naciones Unidas, Resolución A/RES/73/266, "Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional", 22 de diciembre de 2018.

en marzo de 2021[37], y produjo además un Resumen del Presidente[38] que describe algunas propuestas estatales que no alcanzaron consenso, así como un compendio de los pronunciamientos oficiales de los Estados en torno a la adopción del informe final[39]. El informe final reafirmó que el derecho internacional aplica a las TIC pero que se requieren mayores intercambios de ideas entre Estados así como construcción de capacidades para desarrollar mayores entendimientos comunes sobre la forma en que resulta aplicable el derecho internacional al uso de TIC por Estados.

El GGE, por su parte, fue presidido por el Embajador Guilherme de Aguiar Patriota, de Brasil, y estuvo compuesto por expertos de 25 Estados (cuatro de la región de las Américas: Brasil México, Estados Unidos y Uruguay). El GGE adoptó su informe final también por consenso[40] en julio de 2021, en el que reafirmó nuevamente que el derecho internacional es aplicable a las TIC, y reconoció la necesidad de continuar los debates e intercambios de opiniones por parte de los Estados de forma colectiva en las Naciones Unidas sobre el modo en que las normas y principios específicos se aplican al uso de las TIC por Estados. El GGE produjo, además, un compendio oficial de contribuciones nacionales voluntarias de los expertos estatales participantes en el GGE enfocado específicamente a la cuestión de cómo aplica el derecho internacional al uso de las TIC[41].

Con el fin de "asegurar el carácter ininterrumpido y continuo del proceso" antes citado –y, de paso, subsanar la complicación de la duplicación de foros–, en 2020 la Asamblea General de las Naciones Unidas decidió[42] establecer un nuevo OEWG sobre la seguridad de y en el uso de TIC que sesiona durante el periodo 2021-2025, abierto a la participación de todos los Estados y con sesiones de consulta con otros actores relevantes, bajo la presidencia del Embajador Burhan Gafoor de Singapur[43]. Entre los temas de discusión previstos en su mandato se incluye expresamente el de "la forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones por los Estados"[44]. En su portal, el OEWG ha también publicado los pronunciamientos de los Estados

---

[37] United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security,* A/AC.290/202/CRP.2, 10 de marzo de 2021 ("Informe OEWG 2021").

[38] United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Chair's Summary*, A/AC.290/2021/CRP.3, 10 de marzo de 2021.

[39] United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Compendium of statements in explanation of position on the final report,* A/AC.290/2021/INF/2, 25 de marzo de 2021.

[40] Secretario General de las Naciones Unidas*, Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional*, U.N. Doc. A/76/135 (14 de julio de 2021) ("Informe GGE 2021").

[41] Asamblea General de las Naciones Unidas, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266,* U.N. Doc. A/76/136 (13 de julio de 2021) ("Compendio DI GGE"). De la región de las Américas, remitieron contribuciones los expertos de Brasil y de Estados Unidos.

[42] Asamblea General de las Naciones Unidas, resolución 75/240 "Avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", adoptada el 31 de diciembre de 2020.

[43] Véase: https://meetings.unoda.org/meeting/oewg-ict-2021/

[44] Asamblea General de las Naciones Unidas, resolución 75/240 "Avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", adoptada el 31 de diciembre de 2020, párrafo operativo 1.

que así lo solicitan, por sesión y por temática, incluyendo la temática específica de la forma en que el derecho internacional aplica al ciberespacio[45].

Ante la necesidad de continuar avanzando en la discusión sobre la forma en que el derecho internacional aplica al ciberespacio, poco a poco los Estados han ido adoptando y publicando posiciones nacionales oficiales sobre el tema. El CCDCOE, a través de su útil herramienta del *CyberLaw Toolkit*[46], compila, entre otros, las posiciones oficiales que han ido publicando los Estados sobre la aplicabilidad del Derecho Internacional al ciberespacio[47], tanto en su versión completa como clasificadas según la temática de derecho internacional que abordan. De las 24 posiciones nacionales[48] que han sido publicadas a julio de 2022, sólo tres provienen de países de la región de las Américas: Brasil, Canadá y Estados Unidos.

Los procesos de los GGE y OEWG descritos se refieren a la aplicabilidad del derecho internacional al ciberespacio en lo que concierne a las relaciones entre Estados, principalmente. En un tema conexo pero distinto, en diciembre de 2019 la Asamblea General de las Naciones Unidas decidió establecer un comité intergubernamental especial de expertos de composición abierta a fin de elaborar una convención integral sobre la lucha contra la utilización de las TIC con fines delictivos[49]. El comité sesionará en seis ocasiones entre 2022 y 2023 a fin de presentar a la Asamblea General un proyecto de tratado durante el 78º periodo de sesiones de la Asamblea (septiembre 2023-septiembre 2024), en el que se abordarán cuestiones como la cooperación internacional para la prevención, investigación y enjuiciamiento de ciberdelitos[50].

4.3 Otras contribuciones

El Comité Internacional de la Cruz Roja (CICR) ha producido informes y pronunciamientos valiosos sobre la cuestión específica de la aplicabilidad del derecho internacional humanitario (DIH) al ciberespacio, incluyendo, entre otros, un documento de posición general en la materia en 2019[51] y un informe de resultados de una reunión de expertos en 2020 sobre formas para evitar daños a civiles resultantes de ciberoperaciones militares durante conflictos armados[52]. En marzo de 2021 dedicó también un número completo de la Revista Internacional de la Cruz Roja a la cuestión de las tecnologías digitales y la guerra[53]. En junio de 2021 lanzó el Comité Asesor Global sobre Amenazas Digitales durante Conflictos, compuesto por 16 expertos internacionales que asesoran al CICR sobre los principales retos legales y políticos concernientes a la protección de civiles contra estas amenazas[54]. Por

---

[45] Véase: https://meetings.unoda.org/section/oewg-ict-2021_general-statements_14537_general-statements_16368/ De la región de las Américas, tras las primeras dos sesiones celebradas en diciembre de 2021 y marzo de 2022, se han publicado en el portal posicionamientos generales de Colombia, Costa Rica, Cuba y Estados Unidos.

[46] Véase: https://cyberlaw.ccdcoe.org/wiki/Main_Page

[47] https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions

[48] Siguiendo orden alfabético por sus nombres en inglés: Australia, Brasil, Canadá, China, República Checa, Estonia, Finlandia, Francia, Alemania, Irán, Israel, Italia, Japón, Kazajstán, Kenia, Países Bajos, Nueva Zelanda, Noruega, Rumania, Rusia, Singapur, Suiza, Reino Unido y Estados Unidos.

[49] Asamblea General de Naciones Unidas, resolución A/RES/74/247 "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", adoptada el 27 de diciembre de 2019.

[50] Véase: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[51] CICR, *"Derecho internacional humanitario y ciberoperaciones durante conflictos armados: Documento de posición del CICR",* 28 de noviembre de 2019, disponible en: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

[52] CICR, "Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts", ICRC Expert Meeting 21-22 January 2020, disponible en: https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations

[53] Revista Internacional de la Cruz Roja, "Las tecnologías digitales y la guerra", IRRC No. 913, marzo 2021, disponible en: https://international-review.icrc.org/es/revistas/irrc-no-913-las-tecnologias-digitales-y-la-guerra

[54] Véase: https://www.icrc.org/en/document/global-advisory-board-digital-threats

último, ha iniciado una serie de consultas regionales con Estados sobre el DIH y las ciberoperaciones durante conflictos armados: en noviembre de 2021 condujo las consultas con Estados latinoamericanos, cuyo reporte fue publicado recientemente[55], y en diciembre de 2021 realizó las consultas con Estados de Europa central y del este, cuyo reporte está próximo a publicarse.

A su vez, el CICR ha colaborado con el CCDCOE y otras universidades y organizaciones participantes para lanzar en 2019 en el portal web del CCDCOE el ya referido *Cyber Law Toolkit,* una herramienta interactiva en línea de enorme utilidad para el análisis del derecho internacional y las ciberoperaciones. Incluye escenarios hipotéticos acompañados de análisis legales, así como ejemplos de casos reales y la compilación general y temática de las posiciones oficiales que han publicado los Estados en la materia.

A estos esfuerzos globales se ha sumado también el *Proceso de Oxford sobre las Protecciones del Derecho Internacional en el Ciberespacio*, lanzado en mayo de 2020 por el Instituto de Ética, Ley y Conflicto Armado de Oxford en alianza con Microsoft. Desde su creación y hasta la fecha del presente informe, el Proceso de Oxford ha emitido cinco declaraciones públicas, consensuadas por grupos de expertos legales internacionales, sobre la protección que confiere el derecho internacional en el ciberespacio en relación con ciberoperaciones contra el sector salud, la investigación de vacunas en el contexto del COVID-19, las intervenciones electorales extranjeras por medios digitales, la regulación de operaciones y actividades de información y la regulación de operaciones de *ransomware*[56].

4.4 Avances regionales en las Américas

La Organización de los Estados Americanos (OEA) ha colaborado en los esfuerzos de capacitación y promoción del diálogo entre los Estados Miembros sobre la aplicabilidad del derecho internacional al ciberespacio. Por un lado, el Comité Interamericano contra el Terrorismo (CICTE) lleva a cabo desde hace más de 15 años el Programa de Ciberseguridad, a través del cual brinda ayuda a los Estados Miembros de la OEA en el desarrollo de capacidades de ciberseguridad a nivel técnico y de políticas públicas[57]. Entre otros, asiste en la elaboración de estrategias nacionales de ciberseguridad, elabora informes regionales y publicaciones y brinda capacitaciones a funcionarios públicos y privados, así como a estudiantes, en materia de ciberseguridad y ciberoperaciones.

Por su parte, el Comité Jurídico Interamericano (CJI) de la OEA comenzó a trabajar en el tema en el año 2018, a propuesta del entonces miembro y relator del tema, Duncan B. Hollis (de Estados Unidos). Bajo el título *"Mejorando la Transparencia: Derecho Internacional y Operaciones Cibernéticas del Estado"*, la iniciativa buscó "contribuir a una tendencia más amplia en las relaciones internacionales que buscan una mayor transparencia sobre cómo los Estados nacionales entienden la aplicación del derecho internacional al ciberespacio"[58], identificando áreas de convergencia y divergencia. Ello, a partir de un cuestionario circulado en 2019 a los Estados Miembros de la OEA en torno a diez preguntas[59] sobre

---

[55] CICR y Secretaría de Relaciones Exteriores de México, "Regional Consultation of Latin American States: International Humanitarian Law and Cyber Operations During Armed Conflicts", 9-10 noviembre 2021, disponible en: https://www.icrc.org/en/document/regional-state-consultations-ihl-cyber-operations

[56] Disponibles en: https://www.elac.ox.ac.uk/the-oxford-process/

[57] Véase: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

[58] Véase el quinto informe del Dr. Hollis, "Derecho Internacional y Operaciones Cibernéticas del Estado: Mejora de la Transparencia", CJI, 2020, ("Informe Hollis 2020") disponible en: https://www.oas.org/es/sla/cji/docs/Derecho_Internacional_y_Operaciones_Cibern%C3%A9ticas_del_Estado_publicacion.pdf

[59] Las preguntas realizadas a los Estados fueron: "**1.** ¿Ha hecho públicos su gobierno algún documento oficial, discurso o declaración similar que resuma cómo entiende que el derecho internacional se aplica a las operaciones cibernéticas? Se ruega proporcionar copias o enlaces a dichas declaraciones; **2**. ¿Se aplican las ramas del derecho internacional actual (incluidos la prohibición del uso de la fuerza, el derecho de legítima defensa, el derecho internacional humanitario y los derechos humanos) al ciberespa cio? ¿Existen áreas en las cuales la novedad del ciberespacio excluye la aplicación de un conjunto específico de derechos u obligaciones legales internacionales?;

cuestiones específicas del derecho internacional y su aplicabilidad al ciberespacio. Tan sólo nueve de los 35 Estados Miembros de la OEA respondieron al cuestionario: Bolivia, Brasil, Chile, Costa Rica, Ecuador, Estados Unidos, Guatemala, Guyana y Perú[60]. El relator sostuvo también una discusión informal con representantes legales de 16 Estados Miembros de la OEA bajo las reglas de "Chatham House". Los resultados de la iniciativa se publicaron en el quinto y último informe del relator Hollis en 2020, y sirven de herramienta de consulta para los Estados[61]. Entre sus conclusiones, el relator Hollis identificó que existen grandes disparidades entre los Estados de la región de las Américas en cuanto a capacidades técnicas (por ejemplo, para la atribución de una ciberoperación a un Estado extranjero), así como en cuanto a experiencia y conocimientos jurídicos sobre cómo el derecho internacional puede manifestarse en el contexto cibernético. Identificó también desafíos políticos que inhiben una mayor transparencia de los Estados americanos en la materia, así como retos institucionales internos dentro de los Estados de la región, tales como la falta de claridad en la asignación de responsabilidades en el tema cibernético entre autoridades al interior de cada Estado o bien la falta de diálogo interinstitucional entre las diferentes autoridades internas que pudieran estar involucradas directa o indirectamente en el tema cibernético.

En atención a las recomendaciones finales del relator Hollis, la Asamblea General de la OEA (AGOEA) adoptó una resolución en la cual reafirmó la aplicabilidad del derecho internacional en el ciberespacio[62]. Pese a que el relator había sugerido un lenguaje detallado que reconociera expresamente la aplicabilidad de la Carta de las Naciones Unidas, la Carta de la OEA, el DIH, el derecho internacional de los derechos humanos, la no intervención, la igualdad soberana y el derecho sobre la responsabilidad de los Estados, el lenguaje de consenso que alcanzó la AGOEA siguió la tendencia de los foros de las

---

3. ¿Puede una operación cibernética por sí misma constituir un uso de fuerza? ¿Puede constituir un ataque armado que genere un derecho de legítima defensa en virtud del artículo 51 de la Carta de las Naciones Unidas? ¿Puede una operación cibernética calificarse como uso de fuerza o ataque armado sin causar los efectos violentos que se han utilizado para marcar dichos umbrales en conflictos cinéticos pasados?; **4.** Fuera de los conflictos armados, ¿cuándo sería un Estado responsable por las operaciones cibernéticas de un actor no estatal? ¿Qué grado de control o participación debe tener un Estado en las operaciones del actor no estatal para desencadenar la responsabilidad legal internacional de ese Estado?; **5.** ¿Son las normas de responsabilidad del Estado las mismas u otras en el contexto de un conflicto armado tal como se define ese término en los artículos 2 y 3 comunes a los Convenios de Ginebra de 1949?; **6.** De acuerdo al derecho internacional humanitario, ¿puede una operación cibernética calificarse como un "ataque" de acuerdo a las normas que rigen la conducción de las hostilidades si no causa muerte, lesión ni daño físico directo al sistema informático en cuestión o a la infraestructura que apoya? ¿Podría una operación cibernética que produce solo una pérdida de funcionalidad, por ejemplo, calificarse como un ataque? Si es así, ¿en qué casos?; **7.** ¿Estaría una operación cibernética que solamente ataca datos regulada por la obligación de derecho internacional humanitario de dirigir ataques solamente contra objetivos militares y no contra objetivos civiles?; **8.** ¿Es la soberanía una norma discreta del derecho internacional que prohíbe a los Estados participar en operaciones cibernéticas específicas? Si es así, ¿esa prohibición cubre las operaciones cibernéticas que se encuentran por debajo del umbral de uso de la fuerza y que, aparte de eso, no violan el principio de no intervención?; **9.** ¿Es la diligencia debida una norma de derecho internacional que los Estados deben acatar en el ejercicio de su soberanía sobre las tecnologías de la información y la comunicación en sus territorios o bajo el control de sus nacionales?; **10.** ¿Existen otras reglas de derecho internacional que su Gobierno considere importante tener en cuenta al evaluar la regulación de las operaciones cibernéticas por parte de los Estados o actores por las que un Estado tenga responsabilidad en el ámbito internacional?"

[60] Siete de las respuestas fueron respuestas directas y sustantivas a las preguntas del cuestionario, mientras que Brasil solamente indicó que su posición se vertería en el marco del GGE que en ese entonces presidía y Estados Unidos únicamente compartió sus posicionamientos públicos previos.

[61] Informe Hollis 2020, *op. cit. supra* nota 58.

[62] *Asamblea General de la OEA*, resolución AG/RES.2959 (L-0/20) adoptada el 21 de octubre de 2020: "REAFIRMANDO la aplicabilidad del derecho internacional en el ciberespacio y la importancia de la implementación de las normas voluntarias no vinculantes para el comportamiento responsable del Estado en el ciberespacio, en los informes de consenso del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional."

Naciones Unidas al limitarse a reafirmar en términos generales la aplicabilidad del derecho internacional al ciberespacio, y remitió a las normas contenidas en los informes del GGE. Nos atrevemos a asumir que esta aproximación más precavida se debió, quizás, al hecho de que la mayoría de los Estados de la región americana aún no cuentan con posiciones oficiales públicas sobre la aplicabilidad de temas específicos del derecho internacional al ciberespacio y, por ende, no se consideraron aún listos para adoptar a través de la AGOEA un pronunciamiento conjunto detallado sobre el tema.

Otra de las recomendaciones finales del relator Hollis fue que, tras la expiración de su mandato a finales de 2020, el CJI retuviera el tema en su agenda, pudiendo expandir su alcance más allá de las diez preguntas formuladas a temas tales como la no intervención o el derecho internacional de los derechos humanos, y que el CJI apoye –en concierto con otras instituciones, Estados u organizaciones– o emprenda esfuerzos adicionales de construcción de capacidades jurídicas de los Estados Miembros de la OEA en la aplicación del derecho internacional en el contexto cibernético.

Fue en seguimiento de esta última recomendación que en 2021 el CJI decidió continuar el estudio del tema y designó a la doctora Mariana Salazar como relatora del mismo para el periodo 2021-2022. Con base en su primer informe, la relatora sostuvo una consulta informal con los representantes legales de los Estados Miembros de la OEA en 2021, en la cual planteó diversas opciones para continuar los trabajos de la relatoría, incluyendo la posibilidad de circular un nuevo cuestionario ampliado o bien de enfocarnos a la construcción de capacidades técnico-jurídicas y diálogo sobre el tema. La gran mayoría de los representantes indicaron su preferencia por continuar la construcción de capacidades y diálogo, antes de considerar cualquier posibilidad de un nuevo cuestionario, ya que la mayoría de los Estados de la región americana aún no se encuentran listos para adoptar posiciones oficiales en el tema.

A la luz de lo anterior, la relatora co-organizó, junto con CICTE y con el Departamento de Derecho Internacional de la OEA, el evento *"El Derecho Internacional Aplicable al Ciberespacio: Diálogo con Estados Miembros de la OEA"*. El foro tuvo lugar el 14 de junio de 2022 en la sede de la OEA en Washington, D.C., bajo un formato híbrido, con la participación de reconocidos expertos internacionales, para abordar los principales temas concretos de derecho internacional que están involucrados en el debate sobre su aplicabilidad al ciberespacio. El video del evento se encuentra publicado en el sitio web de la OEA, a fin de servir continuamente como herramienta de consulta y apoyo para los Estados que estén en proceso de preparar sus posiciones nacionales en la materia[63].

Adicionalmente, la relatora del CJI en la materia ha participado en concierto con otras organizaciones, en diversos foros que han continuado la reflexión sobre la aplicabilidad del derecho internacional al ciberespacio, incluyendo:

- *En el marco de la OEA:* (i) sesión especial de la Comisión de Asuntos Jurídicos y Políticos para reflexionar colectivamente sobre el fortalecimiento del régimen de responsabilidades en el uso de las TIC (2 de junio de 2022); (ii) webinar "*Derecho Internacional y Operaciones Cibernéticas del Estado*", organizado por el Departamento de Derecho Internacional (8 de marzo de 2021); y (iii) seminario de la Junta Interamericana de Defensa sobre *"Derechos Humanos y Derecho Internacional Humanitario para las Fuerzas Armadas en el Hemisferio Occidental"* para 14,000 fuerzas armadas de la región (24 de marzo de 2021).
- *Bajo la organización del CICR*: (i) consulta regional de Estados latinoamericanos sobre el DIH y las Operaciones Cibernéticas durante los Conflictos Armados, coorganizado con la Secretaría de Relaciones Exteriores de México (9 y 10 de noviembre de 2021); (ii) conversatorio global *"Tecnologías Digitales y Acción Humanitaria en Conflictos Armados"* (18 de marzo de 2021); (iii) reunión regional de Comisiones Nacionales de DIH de las Américas (4 de febrero de

[63] El video se encuentra disponible en: https://www.oas.org/es/sla/ddi/Derecho_Internacional_aplicable_al_Ciber_Espacio_2022_video.asp

2021); y (iv) reuniones del Comité Asesor Global del CICR sobre Amenazas Digitales en Conflictos Armados (9 de junio y 23 de noviembre de 2021, y 14 de junio de 2022).

- *En la academia:* Seminario sobre la evolución del conflicto cibernético y el derecho internacional (*The evolving face of cyber conflict and International Law: A futurespective)* organizado por el Programa de Tecnología, Derecho y Seguridad de la American University, Washington College of Law (15 al 17 de junio de 2022).

5. TEMAS ESPECÍFICOS DEL DERECHO INTERNACIONAL APLICABLE AL CIBERESPACIO Y LAS NACIENTES POSICIONES DE LOS ESTADOS DE LA REGIÓN AMERICANA

Son muy vastas y variadas las aristas de cada uno de los temas de derecho internacional que pueden estar implicados en relación con una ciberoperación estatal, y esta sección no pretende ser un análisis exhaustivo de las mismas. Nos limitaremos a hacer un mapeo de las principales cuestiones en debate y de las posiciones que han comenzado a adoptar los Estados de la región de las Américas al respecto, con base en las posiciones que los propios Estados han hecho públicas, a través de (i) las compiladas en el portal del CCDCOE (retomadas, a su vez, de las páginas web de los gobiernos o de las Naciones Unidas)[64], (ii) las publicadas en el compendio de posiciones nacionales del GGE de 2021[65], (iii) las que los Estados han solicitado sean publicadas en el portal del nuevo OEWG 2021-2025[66], y (iv) las respuestas brindadas al cuestionario circulado en 2019 por este Comité Jurídico Interamericano y compiladas en el informe de 2020 del relator Hollis[67].

De tales fuentes, se desprende que los Estados de la región americana que han adoptado posiciones oficiales más completas sobre la mayoría de los temas jurídicos implicados en el debate sobre el ciberespacio son Brasil, Canadá y Estados Unidos. A su vez, Bolivia, Chile, Cuba, Ecuador, Guatemala, Guyana, y Perú han hecho algunos posicionamientos claros sobre algunos temas específicos. Esta sección retoma las posiciones de esos diez países[68]. Los pronunciamientos que algunos otros Estados han formulado en términos generales sin posicionarse específicamente sobre un tema no han sido incluidos en esta sección. Debe subrayarse, asimismo, que estas fuentes no contienen la totalidad de las intervenciones que han hecho verbalmente los Estados durante las negociaciones intergubernamentales en el seno del GGE y el OEWG, sino únicamente las que los propios Estados han decidido sean publicadas.

Seguiremos la estructura general prevista en los *Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos*[69] (que en gran medida reflejan el derecho internacional consuetudinario en la materia), los cuales indican que se da un hecho internacionalmente ilícito (HII) del Estado cuando un comportamiento consistente en una acción u omisión (a) es atribuible al Estado

---

[64] https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions

[65] Compendio DI GGE, *op. cit. supra* nota 41.

[66] https://meetings.unoda.org/section/oewg-ict-2021_general-statements_14537/

[67] Informe Hollis 2020, *op. cit. supra nota* 58.

[68] Las posiciones previstas en esta sección son: las posiciones de Brasil (2021) y de Estados Unidos (2021) contenidas en el Compendio DI GGE, *op. cit. supra* nota 41; la posición de Canadá (2022) publicada en el portal de su gobierno y compilada en el portal del CCDCOE; algunas posiciones de Bolivia, Chile, Ecuador, Guatemala, Guyana y Perú del Informe Hollis 2020, *op. cit. supra* nota 58; y la posición de Cuba pronunciada ante el nuevo OEWG en diciembre de 2021, disponible en: primera sesión del OEWG de diciembre de 2021, disponible en: https://documents.unoda.org/wp-content/uploads/2021/12/GTCA-Ciberseguridad-2021-2025.-Intervencion-Cuba-sobre-aplicacion-del-Derecho-Internacional.pdf

[69] *Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos,* adoptados por la Comisión de Derecho Internacional de las Naciones Unidas en su 53º periodo de sesiones en 2001 y anexado por la Asamblea General en su resolución 56/83 del 12 de diciembre de 2001, corregido por documento A/56/49(Vol I)/Corr4.

según el derecho internacional; y (b) constituye una violación de una obligación internacional del Estado[70].

5.1 La cuestión de la atribución

Una conducta es atribuible a un Estado cuando es realizada por los órganos del Estado, por personas o entidades que ejerzan atribuciones del poder público o por órganos puestos a disposición de un Estado por otro Estado[71]. También es atribuible al Estado una conducta realizada por actores no estatales cuando esas personas actúan de hecho por instrucciones o bajo la dirección o el control de ese Estado, o cuando ejercen de hecho atribuciones del poder público en ausencia o en defecto de autoridades oficiales, o cuando es realizada por un movimiento insurreccional o de otra índole que se convierta en el nuevo gobierno del Estado o establezca un nuevo Estado, o cuando el Estado reconoce y adopta como propia la conducta[72]. En estos últimos casos relativos a actores no estatales, la atribución al Estado se hará tras una evaluación separada caso por caso.

En el ámbito cibernético, lo anterior significa que, por ejemplo, una ciberoperación conducida por las fuerzas armadas o por los servicios de inteligencia de un Estado, o por una empresa privada de ciberseguridad que ha sido contratada por el Estado para realizar ciberdefensa en su nombre, o bien por un grupo de hackers instruido por el Estado, serán conductas atribuidas al Estado en cuestión. Sin embargo, en el ámbito del ciberespacio, la cuestión de la atribución es técnica, jurídica y políticamente difícil[73].

Técnicamente, con el fin de buscar identificar a la persona o grupo responsable de la ciberoperación maliciosa, se evalúan, por ejemplo, los métodos o técnicas utilizados (el denominado "tradecraft"), la infraestructura física y virtual que se utilizó (los equipos desde los que se preparó, lanzó o transitó la ciberoperación, los nombres de dominio, direcciones IP, etc.) y el malware utilizado, entre otros. Se trata de un proceso complejo, debido a la anonimidad, la interconexión, el carácter transfronterizo, y a que en muchas ocasiones los autores del ciberataque falsifican identidades o "disfrazan" sus métodos copiando los de otros grupos para evadir ser encontrados.

Jurídicamente, debe determinarse si existe un vínculo entre la persona o grupo de personas que perpetró el ciberataque y el Estado, según los criterios de atribución descritos al inicio de esta sección. Probar este vínculo ha sido sumamente difícil en la práctica. A la fecha ningún Estado se ha "auto-atribuido" la autoría de un ciberataque contra otro Estado. Tampoco ha existido hasta ahora un proceso judicial ante la Corte Internacional de Justicia u otro tribunal internacional en el que un Estado demande a otro por su presunta responsabilidad en una ciberoperación maliciosa, por lo que no ha existido propiamente un proceso legal de atribución al respecto.

Los señalamientos a posibles perpetradores estatales de ciberataques se han mantenido, hasta ahora, en la esfera política.[74] En algunas ocasiones, han sido empresas privadas las que dan el paso de atreverse a atribuir autoría de un ciberataque a un Estado. En otros casos, el propio Estado víctima del ciberataque realiza pronunciamientos políticos acusando a otros Estados del mismo. A veces incluso se trata de pronunciamientos estatales conjuntos. Lo cierto es que la práctica es aún poco uniforme, y estos pronunciamientos varían mucho en la cantidad de información y de evidencia, tanto la que presentan públicamente como la que sustenta sus aseveraciones. La atribución es una cuestión delicada y en muchas ocasiones requiere el trabajo colaborativo tanto de gobiernos como entidades privadas y

---

[70] *Ídem*, artículo 2.
[71] *Ídem*, artículos 4, 5, y 6.
[72] *Ídem,* artículos 8, 9, 10 y 11.
[73] Véase, en este sentido: DELERUE, F., *op. cit. supra* nota 4, pp. 55-85.
[74] Para un análisis detallado de los mismos, véase: TSAGOURIAS, N. y FARRELL, M., "Cyber Attribution: Technical and Legal Approaches and Challenges", *European Journal of International Law* vo. 31 no. 3, 2020, pp. 941-966.

sociedad civil. Un señalamiento de este tipo tiene consecuencias políticas, como la realización de gestiones diplomáticas o la adopción de medidas de retorsión[75].

No existe una norma de derecho internacional que regule el estándar de prueba específico para atribuir ciberoperaciones a Estados. En un proceso judicial, dependerá del foro respectivo, mientras que, para los pronunciamientos políticos, el Manual de Tallin 2.0 indica que los Estados deben actuar "razonablemente" al hacer atribución de una ciberoperación, considerando la información relevante disponible y las circunstancias[76]. Estados Unidos se adhiere a este criterio de razonablilidad previsto en el Manual de Tallin, y reitera que no es un asunto previsto en el derecho internacional ni requerido para las atribuciones políticas. Agrega que tampoco es un requisito para que un Estado pueda responder a una ciberoperación maliciosa en su contra con medidas de "autoayuda" como son contramedidas, reafirmando que recurrir a éstas es un derecho del Estado víctima en caso de contar con información sobre la atribución de una ciberoperación a otro Estado.

Por lo que respecta a los criterios de atribución aplicables, Brasil, Canadá y Estados Unidos reconocen en términos generales que los criterios de atribución contenidos en los Artículos sobre Responsabilidad de los Estados son derecho internacional consuetudinario. Brasil y Chile consideran que, tratándose de conductas de personas o entes privados, debe comprobarse que el Estado tenía "control efectivo" sobre la ciberoperación para que sea atribuible a éste.

Finalmente, en lo que respecta a la necesidad de presentar o no evidencia al hacer atribuciones públicas de ciberoperaciones, Canadá y Estados Unidos han reafirmado que los Estados no tienen la obligación de revelar públicamente la evidencia en la que se basa la atribución. Estados Unidos agrega que, sin embargo, para facilitar la comprensión global de la práctica emergente, tales atribuciones públicas deberían, en lo posible, incluir evidencia suficiente que permita corroborar lo alegado. Brasil, a su vez, reitera la importancia de que las determinaciones de atribución estén debidamente fundamentadas y justificadas, y que las dificultades técnicas no deben ser justificación para reducir el umbral.

5.2 La violación de una obligación internacional

Como se ha mencionado, la existencia de un HII requiere, además de la atribución, que la conducta sea la violación de una obligación internacional que sea vinculante para el Estado al momento de producirse el hecho[77]. Pese a que las ciberoperaciones entre Estados no están prohibidas *per se* por el derecho internacional, no cabe duda de que pueden llegar a constituir una violación a obligaciones internacionales. Las obligaciones internacionales derivan de las fuentes primarias del derecho internacional, a saber: tratados internacionales, derecho internacional consuetudinario y principios generales del derecho. Se analizan a continuación algunas de las principales obligaciones internacionales que pueden ser violadas a través de una ciberoperación.

5.2.1 Soberanía

Como dicta la conocida sentencia arbitral en el asunto de la *Isla de Palmas* en 1928, *"[l]a soberanía en las relaciones interestatales equivale a independencia. La independencia respecto a una parte del globo (terrestre) es el derecho a ejercer en dicho lugar las funciones estatales, con exclusión de cualquier otro Estado."*[78] La soberanía es un principio fundamental del derecho internacional. En el ámbito cibernético, el Manual de Tallin 2.0 aclara que, en su componente interno, los Estados tienen

---

[75] Para un análisis ampliado, véase: ROGUSKI, P., "Application of International Law to Cyber Operations: A Comparative Analysis of States' views", *Policy Brief, The Hague Program for Cyber Norms, Universiteit Leiden,* 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views

[76] Manual de Tallin 2.0, *op. cit. supra* nota 6, Capítulo 4, Sección 1, párr. 10.

[77] Artículos sobre Responsabilidad de los Estados, *op. cit. supra* nota 69, artículo 13.

[78] Asunto de la Isla de Palmas, Estados Unidos v. Países Bajos, sentencia arbitral, 1928.

autoridad soberana con respecto a la infraestructura cibernética, personas y actividades cibernéticas localizadas dentro de su territorio.[79]

En el debate sobre el ciberespacio, el debate gira en torno a las siguientes cuestiones principales:

a) Regla o principio:

La mayoría de los Estados que se han pronunciado consideran que la soberanía es una regla independiente del derecho internacional cuya violación genera responsabilidad del Estado[80], incluyendo, de la región americana, Brasil, Canadá, Bolivia, Guatemala y Guyana. Por otro lado, una minoría, particularmente Reino Unido apoyado por Estados Unidos[81], consideran que no es una regla independiente, sino que es un principio que guía las relaciones internacionales.

b) 'De minimis' o cualquier operación:

Bajo el enfoque de que la soberanía es una regla independiente, debe entonces determinarse en qué casos una ciberoperación resulta violatoria de la soberanía de otro Estado. Algunos consideran que cualquier penetración de una red computacional ubicada en el territorio de otro Estado viola su soberanía. Otros, por el contrario, indican que no todas serían violatorias, sino únicamente aquéllas que producen más que efectos mínimos (este último es el denominado enfoque *de minimis*)[82].

De la región americana, Canadá sigue el enfoque del Manual de Tallin 2.0[83] al considerar que son violatorias de la soberanía las ciberoperaciones que infringen en un grado suficiente la integridad territorial del Estado atacado, o que interfieren con, o usurpan, funciones inherentemente gubernamentales del Estado atacado. Canadá enfatiza que sólo las ciberoperaciones que sobrepasan un umbral de efectos *de minimis* o negligentes, que causen efectos significantes dañinos en el territorio de otro Estado sin el consentimiento del otro Estado, podrían llegar a ser violatorias de la soberanía. Aclara que las que únicamente causan efectos mínimos o negligentes no serían violatorias, y enfatiza que los Estados pueden adoptar estas ciberoperaciones para defenderse de ciberactores maliciosos o defender su seguridad nacional. Indica que la ciberactividad que requiere reiniciar o reinstalar un sistema operativo no es probablemente violatoria de la soberanía.

En el mismo sentido, tanto Canadá como Estados Unidos aclaran que las ciberoperaciones remotas de un Estado que involucran computadoras u otros aparatos en red ubicados en el territorio de otro Estado no son *per se* violatorias de la soberanía, particularmente cuando no tienen efectos o tienen efectos mínimos. Aclaran en este sentido que el ciberespionaje no está prohibido por el derecho internacional, si bien puede estar prohibido en leyes nacionales.

Brasil parecería tender más hacia el enfoque de la mera penetración si bien no es del todo claro. Menciona que las intercepciones de las telecomunicaciones se considerarían violatorias de la soberanía, y que las ciberoperaciones contra sistemas informáticos ubicados en el territorio de otro Estado o que causen efectos extraterritoriales también podrían ser violatorias de la soberanía.

c) El grado de infracción necesario

Para determinar qué es "un grado suficiente" de infracción a la integridad del Estado atacado, Canadá sigue el enfoque de considerar el alcance, escala, impacto o severidad de la disrupción, incluyendo la disrupción de actividades económicas y sociales, servicios esenciales, funciones inherentemente gubernamentales, orden público o seguridad pública. Considera que el impacto o severidad debe evaluarse de la misma manera y bajo los mismos criterios que para actividades físicas.

---

[79] Manual de Tallin 2.0, *op. cit. supra* nota 6, regla 2.
[80] Esta visión también se apoya por el Manual de Tallin 2.0.
[81] Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,* 2 March 2020.
[82] ROGUSKI, P., *op. cit. supra* nota 76, p. 4.
[83] Manual de Tallin 2.0, *op. cit. supra* nota 6, regla 4.

Si la ciberoperación causa una pérdida de funcionalidad de infraestructura cibernética ubicada en el territorio de otro Estado, Canadá considera que violaría la soberanía si la pérdida de funcionalidad causa efectos dañinos significantes similares a los ocasionados por el daño físico a personas o propiedades. Cita como ejemplo que el daño requiera reparación o reemplazo de componentes físicos de infraestructura cibernética, o la pérdida de funcionalidad de equipo físico que depende de la infraestructura afectada para operar.

d) Usurpar funciones inherentemente gubernamentales

Canadá aclara que las ciberoperaciones pueden violar la soberanía si usurpan tales funciones, independientemente si hubo daño físico, lesión o pérdida de funcionalidad. Para Canadá, las funciones inherentemente gubernamentales incluyen actividades gubernamentales en las áreas de servicios de cuidado de la salud, procuración de justicia, administración de elecciones, recolección de impuestos, defensa nacional y la conducción de las relaciones internacionales, así como los servicios en los cuales depende.

5.2.2 No Intervención

La no intervención es un principio fundamental del derecho internacional y una norma de derecho internacional consuetudinario. Siguiendo la definición brindada por la Corte Internacional de Justicia en el caso *Nicaragua v. Estados Unidos,* la no intervención implica: (a) no interferir en los asuntos que cada Estado puede, por el principio de soberanía de los Estados, decidir libremente, incluyendo la elección del sistema político, económico, social y cultural y la formulación de política exterior; y (b) el uso de métodos de coerción respecto de tales asuntos, que deben mantenerse libres.[84]

En el ámbito cibernético, existen diferentes posiciones sobre lo que constituye una coerción. Por un lado, para algunos, el acto es coercitivo si está diseñado específicamente para obligar al Estado víctima a modificar su comportamiento sobre un asunto que está dentro de su *domaine reservé.* Para otros, basta con que el acto prive efectivamente al Estado atacado de su habilidad de controlar o gobernar asuntos que están dentro de su *domaine reservé* (sin que de hecho busque obligar al Estado a cambiar su comportamiento). De la región americana, Brasil suscribe esta última postura. Canadá abarca ambas posturas, al mencionar el requisito de imponer un resultado en el Estado afectado y, a su vez, mencionar que también puede haber coerción cuando se prive al Estado afectado de la posibilidad de elegir.

Entre los ejemplos que brindan, tanto Brasil como Canadá y Estados Unidos mencionan que la interferencia electoral, de contar con coerción, sería violatoria del principio de no intervención. Canadá agrega el ejemplo de la ciberoperación que disrumpe el funcionamiento de una tubería de gas significante, ocasionando que el Estado afectado cambie su posición en negociaciones bilaterales en torno de un acuerdo internacional de energía. Estados Unidos también agregó el ejemplo de una ciberoperación que interfiera coercitivamente con la habilidad del Estado de proteger la salud de su población por ejemplo a través de realizar investigación sobre vacunas o establecer ventiladores cibercontrolados en sus territorios durante una pandemia, lo cual, indicó, podría ser violatorio de la regla de la no intervención.

5.2.3 Prohibición del uso de la fuerza

La mayoría de los Estados que se han pronunciado coinciden en que una ciberoperación puede violar la prohibición del uso de la fuerza prevista en el artículo 2(4) de la Carta de las Naciones Unidas, conforme a la cual los Estados miembros de las Naciones Unidas *"en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas."* Dado que la noción de "fuerza" en esa prohibición se refiere a fuerza

[84] *Actividades Militares y Paramilitares en y contra Nicaragu*a (Nicaragua v Estados Unidos) (Méritos) 1986 ICJ Rep 14, para 205.

'armada'[85], el debate gira principalmente en torno a determinar cuándo se considera que una ciberoperación constituye un uso de la fuerza armada prohibido bajo ese artículo.

De la región americana, Brasil, Bolivia y Canadá consideran que una ciberoperación violaría la prohibición del uso de la fuerza si su escala y efectos son comparables a los de ataques cinéticos que constituyen uso de la fuerza bajo el derecho internacional, bajo una evaluación caso por caso. Estados Unidos también reconoce que una ciberoperación que resulte en daño similar al de lanzar una bomba o disparar un misil sería considerada un uso de la fuerza.

Para efectos de la evaluación caso por caso, Estados Unidos considera que deben tenerse en cuenta factores como la naturaleza y alcance del daño o de la muerte a personas y la destrucción de, o daños a, propiedad, así como el contexto del evento, el actor que perpetra la acción, el objetivo y su ubicación, los efectos, y la intención del actor. Indica que las ciberoperaciones que causen muerte, lesiones o destrucción significante, o representan una amenaza inminente de ello, probablemente sean vistas como un uso de la fuerza.

A su vez, Brasil llama a tener cautela al realizar analogías entre acciones cibernéticas y cinéticas, particularmente considerando que a la fecha ningún Estado ha alegado que se violó esta prohibición en su contra a raíz de un ciberataque. Considera que en muchos casos podría resultar difícil establecer una analogía directa entre los actos de agresión previstos en la resolución 3314 de la Asamblea General de las Naciones Unidas (que data de 1974)[86] y las ciberoperaciones, por lo que considera aconsejable que se actualice el entendimiento multilateral sobre cuáles actos constituyen uso de la fuerza y agresión a fin de incluir supuestos de ciberataques.

Guyana[87] ha expresado dudas respecto a que operaciones únicamente cibernéticas puedan constituir un uso de la fuerza prohibido bajo el artículo 2.4 de la Carta.

5.2.4 Deber de debida diligencia

La mayoría de los Estados que se han pronunciado consideran que la jurisdicción exclusiva que tienen los Estados sobre la infraestructura cibernética localizada en sus territorios crea derechos, pero también obligaciones[88]. Según lo ha indicado la Corte Internacional de Justicia en el caso *Canal de Corfú,* todo Estado tiene la obligación de no permitir, a sabiendas, que su territorio se utilice para actos contrarios a los derechos de otros Estados[89]. Siguiendo este criterio, una de las normas voluntarias contenidas en el informe del GGE de 2015 fue que los Estados no permitan, a sabiendas, que su territorio se utilice para hechos internacionalmente ilícitos usando TICs.

En el ámbito del ciberespacio, existe cierto debate sobre:

a) Obligación independiente o criterio de atribución

De la región americana, Chile, Ecuador, Guatemala, Guyana y Perú parecen seguir la posición de que la debida diligencia se trata de una obligación que aplica para el ciberespacio. Canadá se refiere a una expectativa o conducta esperada de los Estados. Por su parte, Estados Unidos, considera que no existe suficiente práctica estatal y *opinio juris* para considerar que la debida diligencia es una obligación general bajo el derecho internacional.

b) *Alcance de las obligaciones que tiene el Estado bajo la regla de la debida diligencia*

De la región americana, tanto Canadá como Estados Unidos han indicado que la obligación aplica cuando un Estado *tiene conocimiento* de una actividad cibernética maliciosa que emana desde su

---

[85] Dörr, Oliver y Randelzhofer, Albrecht, 'Article 2(4)', en Simma, Bruno et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2012) 208 párr. 16.

[86] Asamblea General de las Naciones Unidas, resolución 3314(XXIX), "Definición de la agresión", adoptada el 14 de diciembre de 1974.

[87] Informe Hollis 2020, *op. cit. supra* nota 58, p. 37.

[88] ROGUSKI, P., *op. cit. supra* nota 76, p. 11.

[89] Corte Internacional de Justicia, Caso Canal de Corfú (Reino Unido v. Albania), Fondo, 1949, ICJ Rep 4, 22.

territorio, en cuyo caso debe adoptar medidas razonables para atenderlo. Estados Unidos restringe esta obligación a los casos en que el Estado "es notificado" de la ciberoperación. Por su parte, Canadá la amplía también a supuestos de ciberoperaciones inminentes que *resultarían* en daños significantes para otro Estado.

Como lo indica el informe del GGE de 2021, *"no se espera que los Estados puedan o deban controlar todas las actividades relacionadas con las TIC que se realizan en su territorio"*[90]. Ello no sólo sería imposible sino que además podría constituir una justificación peligrosa de sistemas de vigilancia masiva[91]. En este sentido, Estados Unidos aclara que la soberanía sobre TICs en el territorio de un Estado no debe servir de excusa para violar derechos humanos y otras obligaciones bajo derecho internacional.

En cuanto al alcance de las actividades que debe realizar el Estado, Canadá detalla que depende de las circunstancias, incluyendo si el Estado tienen conocimiento del acto, sus capacidades técnicas y otras para detectarlo y frenarlo, así como de las medidas que serían razonables en cada caso. Por ejemplo, un Estado con capacidades técnicas limitadas probablemente no se esperaría que responda si no detectó una ciberactividad maliciosa que emanaba desde o a través de la infraestructura cibernética en su territorio, pero una vez enterado, ese Estado tendría que responder.

El informe de consenso del GGE de 2021, al describir la norma voluntaria de la debida diligencia, agrega que el Estado afectado debe notificar al Estado en que se originó el ciberataque, para facilitar la cooperación y la clarificación de los hechos, y que el Estado notificado debe hacer todos los esfuerzos razonables para contribuir a determinar si se ha cometido un HII.

5.2.5 Derecho internacional humanitario (DIH)

En el ámbito del ciberespacio, el informe del GGE de 2015 reconoció la aplicabilidad de los principios humanitarios de humanidad, necesidad, proporcionalidad y distinción en el ciberespacio. A su vez, el informe de 2021 del GGE observó:

> *"que el derecho internacional humanitario sólo se aplica en situaciones de conflicto armado. En este sentido, recuerda los principios jurídicos internacionales establecidos, incluidos, en su caso, los principios de humanidad, necesidad, proporcionalidad y distinción que se señalaron en el informe de 2015… reconoce la necesidad de seguir estudiando cómo y cuándo se aplican estos principios al uso de las TIC por parte de Estados y subraya que recordar estos principios no legitima ni fomenta en absoluto los conflictos."*

a) Aplicabilidad del DIH

De la región americana, Canadá, Brasil y Estados Unidos reafirman que el DIH aplica a las ciberoperaciones en tiempos de conflicto armado. Brasil recuerda la opinión consultiva de la Corte Internacional de Justicia sobre la Legalidad de la Amenaza o Uso de Armas Nucleares para indicar que excluir a las ciberoperaciones del DIH sería incompatible con el carácter intrínsecamente humanitario de los principios legales en cuestión, que permean todo el derecho de los conflictos armados y aplican a todas las formas de combate y a todas las armas, las del pasado, las del presente y las del futuro. Brasil aclara que el DIH es aplicable a las ciberoperaciones (i) cuando éstas son usadas como parte de un conflicto armado en curso, para contribuir a operaciones convencionales, y (ii) cuando la ciberoperación misma cruza el umbral de violencia para ser clasificada como un conflicto armado.

Cuba adopta la posición contraria, al establecer que no considera pertinente la aplicabilidad del DIH a las TIC en el contexto de la seguridad internacional, "*en tanto ello implicaría aceptar tácitamente la posibilidad de un escenario de conflicto armado en ese ámbito; contribuiría a la militarización del ciberespacio y sería un primer paso para equiparar un ciberataque a un ataque armado tradicional*."[92]

---

[90] Informe GGE 2021, op. cit. supra nota 40, párr. 30(a).
[91] Delerue, F., op. cit. supra nota 4, p. 359.
[92] Posición de Cuba, primera sesión del OEWG de diciembre de 2021, *op. cit. supra* nota 68.

En respuesta a este argumento, tanto Brasil como Canadá aclaran que reconocer la aplicabilidad del DIH al ciberespacio no es un endoso a militarizarlo ni legitima ciberoperaciones ilegales, sino que únicamente asegura un nivel mínimo de protección en caso de conflicto armado.

b) La noción de "ataque" bajo el DIH

Si bien algunas de las normas del DIH son aplicables a cualquier operación militar, varias de ellas son aplicables específicamente en caso de 'ataque', particularmente las que prohíben ataques contra personas y bienes civiles, las que prohíben ataques indiscriminados y desproporcionados, y la obligación de tomar todas las precauciones para evitar o reducir daños a personas y bienes civiles incidentales cuando se realiza un ataque. Por ello, en el ámbito del ciberespacio, resulta crucial determinar si una ciberoperación puede constituir un 'ataque' para efectos del DIH, y bajo qué supuestos.

El artículo 49 del Protocolo Adicional I define como 'ataques' "los actos de violencia contra el adversario, sean ofensivos o defensivos". La noción de violencia puede referirse ya sea a los medios de combate o a sus efectos, lo cual significa que una operación que cause efectos violentos puede calificar como ataque aun cuando los medios utilizados no sean violentos. De ahí que se considera que las ciberoperaciones que se espere razonablemente causen lesiones o muerte a personas o daños o destrucción a objetos equivalen a 'ataques' bajo el DIH.[93] Esta posición la ha adoptado, entre otros, Canadá.

Estados Unidos ha dicho que no todas las ciberoperaciones alcanzarán el nivel de 'ataque' bajo el DIH y que los Estados deben considerar, entre otros, si resulta en efectos cinéticos o no cinéticos, así como la naturaleza y alcance de esos efectos y la naturaleza de la conexión, si existe, entre la actividad cibernética y el conflicto armado en cuestión. Aun cuando no alcance el nivel de 'ataque', Estados Unidos indica que la ciberoperación debe cumplir el principio de necesidad militar.

Sin embargo, existen posiciones divergentes sobre el concepto de "daño" para evaluar si una ciberoperación constituye un ataque. De la región americana, Chile, Perú y Estados Unidos consideran que sólo debe ser considerado un ataque si ocasiona muertes, lesiones o daños físicos directos; Chile agrega que se requiera realizar acciones para reparar o recuperar la infraestructura o sistema informático afectado. En este sentido, para tales Estados la mera pérdida de funcionalidad de la infraestructura sería insuficiente para clasificarlo como ataque. Por otro lado, Ecuador y Guatemala consideran que una ciberoperación sí podría constituir un ataque sin causar daños físicos si causan la pérdida de funcionalidad del objetivo (posición que comparte el CICR). Como umbral, Ecuador estima que debe dejarlo inoperable, mientras que Bolivia se refiere a inhabilitar los servicios esenciales de un Estado como el agua, la electricidad, telecomunicaciones o el sistema financiero. Brasil se limita a indicar que requiere mayor reflexión la cuestión de la definición del ciberataque, considerar datos civiles como bienes de carácter civil, y en qué casos un civil actuando en el ciberespacio puede ser considerado como tomando parte directa en las hostilidades.

c) *Desarrollo de armas cibernéticas*

Según el artículo 36 del Protocolo Adicional I a los Convenios de Ginebra, el desarrollo de nuevas armas debe atravesar una revisión legal para verificar que pueda cumplir con los principios humanitarios. Esta obligación aplica para cualquier arma, incluyendo las armas cibernéticas. Por ejemplo, el desarrollo de herramientas cibernéticas que se propaguen por sí solas y que causen daños indiscriminados a objetivos civiles y militares está prohibido.

Brasil, Canadá y Estados Unidos han reconocido la aplicabilidad de esta obligación de revisión legal de nuevas armas a las armas que usan capacidades cibernéticas. Al respecto, Canadá recuerda que la elección de métodos y medios de combate no es ilimitada, y aclara también que no todas las capacidades y actividades cibernéticas constituirán un arma, medio o método de combate. Brasil aclara que la revisión legal aplica para el desarrollo, adquisición y adopción de tales capacidades cibernéticas.

[93] Siguiendo el análisis del *Cyber Law Toolkit*, op. cit. supra nota 46.

d) Objetivos militares y datos electrónicos

Bajo el principio de distinción, las partes en un conflicto armado deben distinguir en todo momento entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigir sus operaciones únicamente contra objetivos militares[94]. Son objetivos militares los que, por su naturaleza, ubicación, propósito o uso contribuyen efectivamente a la acción militar y cuya destrucción total o parcial, captura o neutralización, en las circunstancias del momento, ofrece una ventaja militar definitiva[95].

En el ámbito del ciberespacio, el debate gira en torno a si los datos pueden calificar como un "bien", y por ende ser un objetivo militar sujeto a ataque o un bien civil protegido de los ataques bajo el DIH, particularmente cuando la ciberoperación no resulta en efectos físicos[96]. Para algunos Estados, como Chile, la noción de 'bienes' se limita a aquéllos con propiedades físicas, que son visibles y tangibles en el mundo real, y por tanto los datos no son bienes (esta es la posición del Manual de Tallin 2.0)[97]; sin embargo, Chile reconoce que un ataque dirigido exclusivamente contra datos informáticos podría generar consecuencias adversas que afecten a la población civil, por lo cual, por sus efectos, el principio de distinción debe ser tenido en cuenta y debe un Estado abstenerse de atacar datos en caso de que eso pudiese afectar a la población civil, a menos que dichos datos estuvieran siendo utilizados para objetivos militares. Para otros, los datos sí están comprendidos en la noción de bienes bajo el DIH y, por tanto, cuando son datos civiles, están protegidos bajo el DIH y su principio de distinción (no deben ser atacados y se debe cuidar no causar daños incidentales excesivos en su contra). Ha emergido también una posición intermedia, que considera que los datos de contenido (distintos a los datos operacionales) de carácter civil son los únicos que están protegidos bajo el DIH.

e) Alcance de los principios de distinción, proporcionalidad y precaución

Canadá reconoce expresamente que las ciberoperaciones deben cumplir con los principios de distinción, proporcionalidad y precaución. En cumplimiento al principio de *distinción*, Estados Unidos indica que las ciberoperaciones durante un conflicto armado deben dirigirse solamente hacia objetivos militares, tales como computadoras, otros aparatos en red computacional, o posiblemente datos específicos que, por su naturaleza, ubicación, propósito o uso, hagan una contribución efectiva a la acción militar y cuya destrucción total o parcial, captura o neutralización, en las circunstancias del momento, ofrezca una ventaja militar definitiva.

Sobre el principio de *proporcionalidad*, Estados Unidos indica que las partes en conflicto deben evaluar los posibles efectos de una ciberoperación sobre infraestructura y usuarios tanto militares como civiles, incluyendo infraestructura física compartida (como una presa o una red eléctrica) que pudiera afectar a civiles, a fin de evaluar si se esperaría que la ciberoperación cause pérdidas incidentales a vidas civiles, lesiones a civiles, o daño a objetos civiles que sean excesivos en relación con la ventaja militar directa y concreta anticipada. Además del potencial daño físico de una ciberactividad, como muerte o lesiones derivados de efectos sobre infraestructura crítica, las partes deben evaluar los potenciales efectos de un ciberataque sobre objetos civiles que no son objetivos militares, como computadoras privadas, civiles que no tienen significado militar pero que pueden estar conectadas a objetivos militares.

En cuanto al principio de *precaución* en la elección de medos y métodos de combate para evitar o minimizar lesiones o pérdida de vidas civiles, lesiones a civiles y daños a objetos civiles, Brasil reconoce su aplicabilidad al ciberespacio, teniendo en cuenta las particularidades del mismo, como la interconexión entre redes militares y civiles.

f) Respeto y protección a unidades y personal médico

---

[94] Protocolo Adicional I, artículo 48.
[95] Protocolo Adicional I, artículo 52(2).
[96] Para un análisis detallado, véase: Mačák, K. "Unblurring the lines: military cyber operations and international law", *Journal of Cyber Policy*, Vol. 6, 2021, disponible en: https://doi.org/10.1080/23738871.2021.2014919
[97] Manual de Tallin 2.0, *op. cit. supra* nota 6, p. 437.

El DIH obliga a las partes en conflictos a respetar y proteger las unidades sanitarias, las cuales no deben ser objeto de ataque [98] Esta obligación incluye no interferir con el funcionamiento de servicios médicos. El CICR y el Manual de Tallin 2.0[99] han aclarado que esta obligación abarca la prohibición de borrar, alterar o afectar de cualquier manera los datos médicos, incluyendo los necesarios para el uso apropiado de equipo médico, para el rastreo del inventario de suministros médicos, y los datos médicos personales requeridos para el tratamiento de pacientes. Por tanto, las ciberoperaciones durante conflictos armados deben cumplir también con esta obligación.

5.2.6 Derecho Internacional de los Derechos Humanos (DIDH)

Las ciberopreaciones, por sus efectos y consecuencias, pueden también afectar derechos humanos. Perú reconoce expresamente la validez de diversos derechos humanos en el ciberespacio, entre ellos "el derecho a la privacidad e intimidad, libertad de información, libertad de expresión, libre e igual acceso a la información, eliminación de la brecha digital, derechos de propiedad intelectual, libre flujo de información, derecho al secreto de las comunicaciones, etc."[100] Canadá también considera que el DIDH es aplicable a las ciberoperaciones, y estima que los derechos humanos particularmente implicados incluyen la libertad de expresión y opinión, la libertad de asociación pacifica, la no discriminación, y el derecho a la privacidad.

Estados Unidos aclara que, si bien la infraestructura física que apoya el internet y las actividades cibernéticas está ubicada generalmente en territorio soberano y está sujeto a la jurisdicción del Estado territorial, el ejercicio de jurisdicción por este Estado territorial no es ilimitado sino que debe respetar el DIDH. Se refiere en particular a la libertad de opinión y expresión, que puede ser ejercida por cualquier medio e independientemente de las fronteras.

El DIDH contiene obligaciones para el Estado respecto de los individuos *bajo su jurisdicción*: esto se refiere a su territorio o bien a situaciones en las que el Estado ejerce poder o control efectivo, sea sobre el territorio en el que está localizada una persona, sea sobre el individuo. Un Estado puede ser responsable por violaciones a derechos humanos atribuidos a éste, o bien por la ausencia de adopción de medidas razonables para proteger los derechos humanos de individuos en su territorio o bajo su jurisdicción (por ejemplo, si permite que actores no estatales violen derechos humanos[101]). En el caso de las ciberoperaciones conducidas por un Estado que afectan derechos de personas fuera de su jurisdicción, si bien la interpretación actual del DIDH no permitiría invocar la responsabilidad internacional del Estado atacante ante un tribunal internacional, existen algunas propuestas en el ámbito académico que buscan encontrar la forma de que ello sea posible: Milanovic, por ejemplo, propone un modelo bajo el cual los Estados tienen una obligación positiva de proteger y garantizar los derechos humanos dentro de su jurisdicción, sumada a una obligación negativa de respetar los derechos humanos en todo lugar independientemente de su jurisdicción. Sin embargo, de momento se trata de una propuesta académica que aún no ha sido aceptada por tribunales o Estados[102].

5.3 Respuestas disponibles para el Estado víctima de una ciberoperación maliciosa

El Derecho Internacional prevé medidas de respuesta (también llamadas de autoayuda o autotutela - *self-help*, en inglés-) que puede adoptar un Estado afectado por la conducta de otro Estado, a saber: retorsión, contramedidas o legítima defensa.

5.3.1 Retorsión

La *retorsión* constituye una medida legal pero poco amistosa adoptada por el Estado víctima en contra del Estado responsable. No interfiere con los derechos del Estado responsable bajo el Derecho

[98] I Convenio de Ginebra, art. 19; IV Convenio de Ginebra, art. 18; Protocolo Adicional I, arts. 11(1) y 12.
[99] Manual de Tallin 2.0*, op. cit. supra* nota 6, comentario a la regla 132.
[100] Informe Hollis 2020, op. cit. supra nota 58, p. 32.
[101] Siguiendo el criterio del *Cyber Law Toolkit, op. cit. supra* nota 46.
[102] Véase, en este sentido, Milanovic, M., "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015), 56 *Harvard International Law Journal* 81, 113-118; y Delerue, op. cit. supra nota 4, pp. 263-264.

Internacional. El Derecho Internacional permite estas medidas, incluso cuando las actividades que lo provocaron no alcancen el umbral de ser un HII. Así pues, ante la dificultad que representa la atribución en el caso de las ciberoperaciones, ha sido usual que los Estados afectados por ciberoperaciones recurran a la retorsión que, a diferencia de las contramedidas o de la legítima defensa, no tienen como prerrequisito la determinación de la existencia de un HII por el Estado atacante.

De la región americana, Estados Unidos reitera la posibilidad de que los Estados adopten medidas de retorsión en respuesta a una ciberoperación, y entre los ejemplos cita la imposición de sanciones o la declaración de un agente diplomático como *persona non grata*.

5.3.2 Contramedidas

Las *contramedidas* consisten en el incumplimiento temporal de obligaciones internacionales que tiene el Estado que las adopta con respecto al Estado responsable. Están previstas y permitidas en el Derecho Internacional como respuesta al HII del Estado responsable, con el único objeto "de inducirlo a cumplir las obligaciones que le incumban"[103]. La ilegalidad del incumplimiento en estos casos se exime por ser respuesta a un HII. Las contramedidas no son ilimitadas, sino que en ningún caso pueden afectar la prohibición del uso de la fuerza, las obligaciones de derechos humanos, las obligaciones humanitarias que prohíben las represalias, y otras obligaciones que emanan de normas imperativas del derecho internacional general[104]. Deben ser proporcionales al perjuicio sufrido, y su adopción requiere previa notificación al Estado responsable, salvo por casos de urgencia en los que las contramedidas son necesarias para preservar los derechos del Estado[105].

Ante las dificultades en materia de atribución y a que las contramedidas presuponen la existencia de un HII, a la fecha, ningún Estado ha enmarcado su respuesta a una ciberoperación maliciosa como una contramedida. De la región americana, Estados Unidos ha aclarado que las contramedidas en respuesta a ciberoperaciones no se limitan a medidas cibernéticas, sino que un Estado puede también recurrir a contramedidas que no sean cibernéticas.

La mayoría de los Estados de otras regiones que se han pronunciado indican que en el ámbito del ciberespacio, en ciertas circunstancias pueden estar exentos de la obligación de dar notificación previa de contramedidas al Estado responsable, debido a la naturaleza encubierta de las intrusiones cibernéticas y a la necesidad de secrecía y cobertura de las contramedidas o la urgencia de la acción. Países como Estonia van más allá, indicando que incluso Estados que no han sido afectados directamente podrán aplicar contramedidas para apoyar al Estado directamente afectado, posición que ha sido contradicha por otros Estados que indican que sólo el Estado afectado las puede adoptar.

5.3.3 Legítima defensa

Bajo el artículo 51 de la Carta de las Naciones Unidas, los Estados tienen "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".

En el ámbito del ciberespacio, es necesario determinar si una ciberoperación puede constituir un "ataque armado" para efectos de detonar este derecho. Al respecto, la mayoría de los Estados de otras regiones que se han pronunciado siguen el criterio de la Corte Internacional de Justicia en el caso *Nicaragua v. Estados Unidos,* conforme al cual debe evaluarse la "escala y efectos" para determinar si un uso de la fuerza constituye un 'ataque armado': conforme a éste, sólo los usos de la fuerza más graves[106] que causan muerte o lesión a personas o daños o destrucción de propiedades serán un ataque armado y por tanto detonarán el derecho a la legítima defensa previsto en el artículo 51. Estados Unidos,

---

[103] Artículos sobre responsabilidad de los Estados, *op. cit. supra* nota 69, artículo 49.
[104] *Ídem,* artículo 50.
[105] *Ídem,* artículos 51 y 52.
[106] *Actividades… op. cit. supra* nota 84, para. 191.

sin embargo, adopta una posición distinta, al considerar que cualquier uso de la fuerza ilegal bajo el artículo 2(4) de la Carta constituye un 'ataque armado' que detona el derecho de legítima defensa bajo el artículo 51 de la misma. Chile, por su parte, adopta un enfoque de criterios, al considerar que "los ciberataques dirigidos en contra de su soberanía, sus habitantes, su infraestructura física o de la información" podrían cumplir los requisitos para ser considerados como ataques armados.[107] Brasil recuerda que el derecho a la legítima defensa se detona ante la existencia de un ataque armado actual o inminente, por lo que no existe el derecho a la legítima defensa preventiva.

Cuba, por su parte, rechaza la aplicación automática del artículo 51 a ciberoperaciones, aclarando que "*considera que resulta inaceptable la noción que busca equiparar un ataque cibernético con un ataque armado para intentar justificar la supuesta aplicabilidad […] de la legítima defensa*".[108] Guyana considera que operaciones únicamente cibernéticas, que no impliquen el uso de armamento físico, no pueden considerarse como un ataque armado que detone el derecho a la legítima defensa.

Tanto Brasil como Estados Unidos reconocen que el derecho a la legítima defensa debe ser necesario y proporcional. En este sentido, Canadá recuerda que la respuesta a un ataque armado cibernético puede ser realizada a través de ciberoperaciones, mientras que Estados Unidos afirma que no hay requisito para que el Estado se defienda por los mismos medios con los que fue atacado, por lo que puede responder con ciberoperaciones u otras operaciones cinéticas. Estados Unidos llama a que, antes de recurrir a medidas que involucren la fuerza, los Estados consideren la ciberdefensa pasiva o defensa activa que no llegue al umbral del uso de la fuerza para neutralizar el ataque o su riesgo inminente.

Por último, Brasil considera que sólo puede ejercerse legítima defensa contra ciberoperaciones cometidas por actores estatales, y que no puede ser en respuesta a actores no estatales salvo que estén actuando en representación de o bajo el control de un Estado. Estados Unidos, por el contrario, indica que el derecho de legítima defensa aplica cuando el atacante es actor estatal o bien actor no estatal.

6. CONCLUSIÓN

Las ciberoperaciones maliciosas entre Estados son, crecientemente, parte de nuestra realidad cotidiana, y el derecho internacional debe hacer frente a este reto global. Ante la ausencia de normas de derecho internacional que regulen específicamente las ciberoperaciones estatales, es esencial que los Estados continúen avanzando en el diálogo y examen de este tema con el fin de alcanzar, eventualmente, acuerdos en torno a la manera en que las normas existentes del derecho internacional aplican en el ciberespacio. El ritmo de avance de los procesos intergubernamentales en el marco de las Naciones Unidas a lo largo de las dos últimas décadas ha puesto de manifiesto que alcanzar consensos sobre este tema enfrenta enormes dificultades, no sólo en cuanto a divergencia de interpretaciones jurídicas, sino también a implicaciones políticas y disparidades de capacidades técnicas de los Estados.

Los ejercicios académicos, como los Manuales de Tallin, los esfuerzos del CICR y el proceso de Oxford, han sido de enorme utilidad para contribuir a guiar el entendimiento y las posiciones de los pocos Estados que ya se han pronunciado oficialmente en la materia en el marco de las negociaciones de las Naciones Unidas.

Desde la región de las Américas, continúan siendo muy pocos los Estados que se han posicionado claramente sobre los principales temas de derecho internacional cuyo alcance se debate. Los esfuerzos que realiza la OEA, a través de CICTE y de este Comité Jurídico Interamericano, han sido una contribución positiva para profundizar el diálogo y transparentar posiciones en la materia. Es la intención de esta relatoría que el presente informe, junto con las actividades de diálogo y capacitación que se han realizado a lo largo de estos últimos dos años, contribuya como una herramienta de análisis útil para

[107] Informe Hollis 2020, *op. cit. supra* nota 58, p. 38.
[108] Posición de Cuba, primera sesión del OEWG de diciembre de 2021, *op. cit. supra* nota 68.

todos los Estados de nuestra región que se encuentran en proceso de preparar sus posiciones nacionales sobre el alcance de la aplicabilidad del derecho internacional al ciberespacio.

25/8/22
24/10/22 rev.2 Corr.1