97º PERÍODO ORDINARIO DE SESIONES
3 – 7 agosto de 2020
Sesión virtual

OEA/Ser. Q
CJI/doc. 615/20 rev.1
7 agosto 2020
Original: inglés

DERECHO INTERNACIONAL Y OPERACIONES CIBERNÉTICAS DEL ESTADO: MEJORA DE LA TRANSPARENCIA - QUINTO INFORME

(presentado por el profesor Duncan B. Hollis)

1. Este es mi quinto y último informe sobre el tema relativo a la mejora de la transparencia con respecto a cómo los Estados Miembros entienden la aplicación del derecho internacional a las operaciones cibernéticas estatales. Este proyecto tiene como objetivo 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. Al así hacerlo, lo que se persigue es lograr cuatro objetivos:

a. identificar áreas de convergencia en cómo los Estados entienden qué reglas legales internacionales se aplican y cómo lo hacen. Cuando se combina con declaraciones existentes de Estados situados fuera de la región, una uniformidad de puntos de vista puede proporcionar evidencia adicional para delinear las reglas de derecho internacional consuetudinario relevantes;

b. identificar puntos de vista divergentes sobre qué normas internacionales se aplican o cómo lo hacen. Esto puede ayudar a establecer una línea de base para un diálogo adicional, ya sea para conciliar posiciones en conflicto, aclarar el contenido de la ley o, tal vez, incluso buscar modificaciones a la misma;

c. limitar los riesgos de escalada o conflicto involuntario debido a que los Estados poseen interpretaciones diferentes sobre la aplicación del derecho internacional y desconocen o no entienden cómo otros ven el problema; y

d. brindar a la OEA y sus Estados Miembros una voz apropiada en las conversaciones mundiales sobre la aplicación del derecho internacional.

Al mismo tiempo, es importante reiterar lo que este proyecto no está destinado a hacer. No tiene como objetivo codificar o desarrollar progresivamente el derecho internacional (ni siquiera identificar las mejores prácticas u orientación general). Tampoco pretende ofrecer una perspectiva integral o general sobre cuestiones legales internacionales en el contexto cibernético.

2. En lugar de ello, este proyecto está destinado, y debe leerse, como un modesto primer paso. El Comité Jurídico (y la OEA en términos más generales) pueden utilizar los materiales proporcionados aquí para evaluar qué actividades adicionales, si las hubiera, podrían llevarse a cabo para agregar más transparencia a la forma en que el derecho internacional se aplica a los Estados de la región, sus operaciones cibernéticas y sus reacciones a amenazas cibernéticas por parte de otros. El Comité también podría considerar aumentar los esfuerzos existentes de creación de capacidad para mejorar el conocimiento y la experiencia de los funcionarios pertinentes sobre las cuestiones de la aplicación del derecho internacional al ciberespacio. Esto puede implicar la compilación (y publicación) de puntos de vista nacionales adicionales y/o establecer plataformas u otros procesos para compartir información y dialogar sobre la relación del derecho internacional con el ciberespacio y las tecnologías de la información y la comunicación (TIC) de las que deriva.

3. Mi primer informe destacó la limitada visibilidad del derecho internacional en la regulación de las operaciones cibernéticas estatales, a pesar del creciente número de tales operaciones y

sus implicaciones económicas, humanitarias y de seguridad nacional[1]. Es cierto que muchos Estados han confirmado la aplicabilidad del derecho internacional a su comportamiento en el ciberespacio[2]. Y, aunque la OEA no lo ha hecho, otras organizaciones internacionales (la ASEAN, la Unión Europea y las Naciones Unidas) también lo han realizado[3]. Hasta la fecha, sin embargo, los esfuerzos para delinear cómo los Estados entienden la aplicación del derecho internacional al ciberespacio han tenido un éxito limitado.

4. Parte del problema en la aplicación del derecho internacional al ciberespacio se deriva de la falta de normas o estándares a medida. Cuando se trata de la paz y la seguridad internacionales, por ejemplo, no existen tratados específicos sobre ciberseguridad. Y esas convenciones que se ocupan del delito cibernético - la Convención de Budapest y (si alguna vez entra en vigor) la Convención de la Unión Africana - solo se dirigen, por definición, al comportamiento de los actores no estatales con el apoyo de una minoría de Estados nacionales[4]. Por lo tanto, la aplicación del derecho internacional al ciberespacio depende de la analogía con tratados multilaterales más generales (por ejemplo, la Carta de las Naciones Unidas) o el derecho internacional consuetudinario.

5. Sin embargo, como destaqué en mi segundo informe, a nivel mundial no existe un consenso universal entre los Estados sobre qué normas internacionales generales vigentes se aplican a las operaciones cibernéticas, y mucho menos cómo lo hacen[5]. Para varios regímenes jurídicos internacionales (por ejemplo, defensa propia, derecho internacional humanitario, contramedidas, soberanía (como regla independiente) y debida diligencia) uno o más Estados impugnan su aplicación *in toto* al ciberespacio, mientras que otros difieren (a veces dramáticamente) en cómo interpretan la aplicación de esas reglas a las operaciones cibernéticas estatales y patrocinadas por el Estado.

---

[1] *Ver* Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia*, OEA/Ser.Q, CJI/doc 570/18 (Agosto 9, 2018) ("Hollis, Primer Informe"), en http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf.

[2] *Ver* Secretario General de la ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶19, U.N. Doc. A/68/98 (Junio 24, 2013) ("el derecho internacional, y en particular la Carta de las Naciones Unidas, se aplica" al ciberespacio); *ver también* Secretario General de la ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶24, U.N. Doc. A/70/174 (Julio 22, 2015)

[3] *Ver* UNGA Res. 266, U.N. Doc. A/RES/73/266 (Ene. 2, 2019); Declaración de los líderes de la ASEAN-Estados Unidos sobre cooperación en ciberseguridad (Nov. 18, 2018), en https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf ; Declaración de la UE: 1.er Comité de las Naciones Unidas, debate temático sobre otras medidas de desarme y seguridad internacional (Oct. 26, 2018) ("EU Statement"), en https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-%E2%80%93-united-nations-1st-committee-thematic-discussion-other-disarmament-measures-and_en. Tanto el G7 y el G20 realizaron afirmaciones similares. *Ver, por ej.,* Declaración del G7 sobre la Responsabilidad de los Estados por su Conducta en el Ciberespacio (Abril 11, 2017) en https://www.mofa.go.jp/files/000246367.pdf; G20 Comunicado de los Líderes de la Cumbre de Antalya (Nov. 15-16, 2015) ¶26, en http://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf.

[4] Consejo de Europa,Convención sobre el Ciberdelito, (Budapest, 23 Nov 2001) CETS No 185; Convención de la UA sobre seguridad cibernética y protección de datos personales, junio 27, 2014, AU Doc. EX.CL/846(XXV). La Convención de Budapest cuenta ahora con 65 partes, aunque varios otros Estados la ven con cierta hostilidad. *Ver* Convención sobre Cibercrimen, *en* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

[5] Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia*, OEA/Ser.Q, CJI/doc 578/19 (Ene. 21, 2019) ("segundo Informe, Hollis"), en http://www.oas.org/en/sla/iajc/docs/CJI_doc_578-19.pdf

6. Los Estados parecen igualmente reacios a invocar el lenguaje del derecho internacional al hacer acusaciones sobre las operaciones cibernéticas de otros Estados[6]. En una notable excepción, en 2018 cinco estados (Australia, Canadá, los Países Bajos, Nueva Zelanda y el Reino Unido) acusaron al GRU, el brazo de inteligencia militar de Rusia, de responsabilidad por una serie de operaciones cibernéticas, incluidas las dirigidas a la Organización para la Prohibición de Armas Químicas (OPAQ) y la Agencia Mundial Antidopaje (AMA). El Secretario de Relaciones Exteriores del Reino Unido sugirió que Rusia tenía un "deseo de operar sin tener en cuenta el derecho internacional o las normas establecidas", mientras que los Países Bajos sugirieron, en términos más generales, que estas actividades rusas "socavan el estado de derecho internacional".[7] Lamentablemente, estas acusaciones no delinearon si todas las supuestas operaciones de GRU violaron el derecho internacional o si solo algunas lo hicieron; ni elaboraron respecto de qué normas internacionales los acusadores creían se habían violado. Sin embargo, la mayoría de los casos son similares a las recientes acusaciones de Canadá, Estados Unidos y el Reino Unido de que el GRU se ha enfocado en la investigación de la vacuna COVID 19; no se menciona el derecho internacional en absoluto[8].

7. En los últimos años, varios Estados han comenzado a ofrecer algunas explicaciones sobre cómo entienden que el derecho internacional se aplica al ciberespacio. A partir de 2012, Estados Unidos comenzó a ofrecer sus puntos de vista en una serie de discursos y declaraciones oficiales[9]. En

---

[6] *See* Dan Efrony and Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-Operations and Subsequent State Practice,* 112 AJIL 583, 586 (2018); Duncan B. Hollis & Martha Finnemore, *Beyond Naming and Shaming: Accusations and International Law in Global Cybersecurity,* 33 EURO. J. INT'L L. (próximamente 2020).

[7] Comunicado de Prensa, Foreign Commonwealth Office, *UK exposes Russian cyber-attacks* (Oct. 4, 2018), at https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks; National Cyber Security Centre (NCSC), *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (Oct. 4, 2018), at https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; Ministerio de Defensa de los Países Bajos, *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW* (Oct. 4, 2018), en https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw. Acusación de Canadá incorporó ambas formulaciones. Comunicado de Prensa, Global Affairs Canada, *Canada identifies malicious cyber-activity by Russia* (Oct. 4, 2018) en https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html (La actividad rusa demuestra "falta de interés en el derecho internacional y mina el orden internacional basado en las reglas."). Contrastando, Australia y Nueva Zelanda acusaron a Rusia de "ciberactividad maliciosa" sin hacer referencia al derecho internacional en absoluto. *Ver, por ej.* Comunicado de Prensa. Gobierno de Nueva Zelanda, Comunicaciones del Buró de Seguridad, *Malicious cyber activity attributed to Russia* (Octubre 4, 2018), en https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/; Comunicado de Prensa, Primer Ministro de Australia, *Attribution of a Pattern of Malicious Cyber Activity to Russia* (Oct. 4, 2018), en https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia

[8] *Ver, por ej..,* NCSC (Reino Unido), *Comunicado de Prensa: UK and allies expose Russian attacks on coronavirus vaccine development* (16 July 2020), at https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development; Establicimiento de seguridad (Canadá), *Statement on Threat Activity Targeting COVID-19 Vaccine Development* (16 Julio 2020), en https://cse-cst.gc.ca/en/media/2020-07-16; Servicio de Seguridad Central de la Agencia Nacional de Seguridad de los EE. UU., *NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers* (16 Julio 2020), en https://www.nsa.gov/news-features/press-room/Article/2275378/nsa-teams-with-ncsc-cse-dhs-cisa-to-expose-russian-intelligence-services-target/

[9] *Ver, por ej.,* Brian Egan, *Remarks on International Law and Stability in Cyberspace* (Nov. 10, 2016), *en* DIGEST OF U.S. PRACTICE IN INT'L LAW 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Oct. 2016), *en* DIGEST OF U.S. PRACTICE IN INT'L LAW 823 (2016) ("2016 US GGE Submission"); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Oct. 2014), *en* DIGEST OF U.S. PRACTICE IN INT'L LAW 732 (2014) ("2014 US GGE Submission "); Harold Koh, *International Law in Cyberspace* (Sept. 18, 2012), *en* DIGEST OF U.S.

2018, el Procurador General del Reino Unido hizo una importante declaración sobre la opinión del Reino Unido[10]. En los años siguientes, otros Estados (en su mayoría europeos) han comenzado a ofrecer sus propias perspectivas detalladas, como Australia[11], Estonia[12], Francia[13], Alemania[14] y los Países Bajos[15]. Aunque es un hecho positivo, el número y la especificidad de estas declaraciones no ha sido (aun) suficiente para confiar en ellas como evidencia de la práctica general del Estado o de la *opinio juris*[16].

8. Varios actores no estatales han tratado de llenar este déficit de información ofreciendo sus propios puntos de vista sobre cómo el derecho internacional consuetudinario regula las operaciones cibernéticas estatales. Las dos voces más destacadas son, sin duda, las del Comité Internacional de la Cruz Roja (CICR) y el Grupo Independiente de Expertos que escribió los *Manuales de Tallin*.[17] Sin

---

PRACTICE IN INT'L LAW 593 (2012). En 2020, el Asesor Jurídico del Departamento de Defensa de EE. UU. Ofreció puntos de vista sobre varias cuestiones clave de la aplicación del derecho internacional al ciberespacio. Sin embargo, aún no está claro si sus puntos de vista reflejan los de los Estados Unidos en general o solo del Departamento de Defensa de los Estados Unidos. *Ver* Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (Marzo 2, 2020), at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/;

[10] Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century* (Mayo 23, 2018), at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("U.K. Views"/ Puntos de Vista del Reino Unido).

[11] Misión Australiana a las Naciones Unidas, *Australian Paper—Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (Sept. 2019), en https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf ("Australian Views"/Puntos de Vista de Autralia); Commonwealth de Australia, Departmento de Relaciones Exteriores y Comercio, *Annex A: Australia's position on how international law applies to State conduct in cyberspace*, en AUSTRALIA'S INT'L CYBER ENGAGEMENT STRATEGY (2017) *en*https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf.

[12] Kersti Kaljulaid, Presidente de Estonia, *President of the Republic at the opening of CyCon 2019* (May 29, 2019), en https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("Estonian Views"/Puntos de Vista de Estonia)

[13] Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (Sept. 9, 2019), https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("French Ministry of Defense Views"). I have not labeled these as "French views" as at least one scholar has pointed out that the document is authored by the French Ministry of Defense and its contents may not be attributable to the French State as a whole. *See* Gary Corn, *Punching on the Edges of the Gray Zone: Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (Feb. 11, 2020) ("Cabe señalar que, a pesar de numerosas afirmaciones en contrario, el documento francés no pretende ser la posición oficial del gobierno francés. Fue escrito y publicado por el Ministère des Armées (MdA) francés, en el mismo sentido que el DoD Law of War Manual, que no necesariamente refleja los puntos de vista del gobierno de los Estados Unidos en su conjunto.").

[14] Discurso del Embajador Norbert Riedel, Comisionado de Política Cibernética Internacional, Ministerio Federal de Relaciones Exteriores de Alemania (Mayo 18, 2015), *en* https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

[15] *Letter to the parliament on the international legal order in cyberspace*, July 5, 2019, Apéndice 1, en https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("The Netherlands Views"/Puntos de Vista de los Países Bajos).

[16] *Ver, por ej.,* Egan, *supra* nota **Error! Bookmark not defined.**, en 817.

[17] *Ver, por ej.,* CICR, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts* (Nov. 2019); MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); *ver también* ICRC, *Report on International*

embargo, está claro que no todos los Estados consideran que su contenido refleje el derecho internacional.[18]

9. El año pasado, la Asamblea General de la ONU encargó a un nuevo Grupo de Expertos Gubernamentales de la ONU ("GEG") que invitara a las opiniones nacionales sobre el derecho internacional.[19] Además, en el nuevo GEG, también hay un Grupo de trabajo de Composición Abierta ("OEWG"/GTCA) sobre Avances en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional patrocinado por la ONU, que ha brindado a los participantes la oportunidad de hacer declaraciones, algunas de las cuales hacen referencia al derecho internacional.[20] Sin embargo, el GEG solo cuenta con la participación de cuatro Estados Miembros de la OEA (Brasil, México, Estados Unidos y Uruguay). En contraste, el OEWG/GTCA está abierto a todos los Estados Miembros de la OEA. Pero la mayoría de las contribuciones allí relacionadas con el derecho internacional se han mantenido muy generalizadas. Y, al igual que el GEG, el OEWG/GTCA se centra exclusivamente en cuestiones de seguridad internacional y, en consecuencia, confina las opiniones del Estado sobre la aplicación del derecho internacional.

10. Por lo tanto, existe la necesidad de foros adicionales en los cuales los Estados Miembros puedan ser alentados —y oportunidades brindadas — para expresar sus propios puntos de vista sobre la aplicación del derecho internacional. Este proyecto marca un primer intento (y algo cauteloso) de satisfacer esa necesidad en la región. No está diseñado para sustituir o competir con los procesos en curso de la ONU. Más bien, tiene como objetivo complementar esos esfuerzos al permitir que todas las voces de esta región participen y exploren la panoplia completa de la aplicación del derecho internacional al comportamiento del Estado en el ciberespacio. En este sentido, el trabajo del Comité se alinea con el llamado de la Unión Europea a que los Estados Miembros de la ONU "deben presentar contribuciones nacionales sobre el tema de cómo el derecho internacional se aplica al uso [de tecnologías de la información y la comunicación] por parte de los Estados."[21]

11. El proyecto actual ha tratado de satisfacer la necesidad de una mayor transparencia regional a través de dos métodos diferentes: (i) un cuestionario preparado junto con el Departamento de Derecho Internacional de la OEA (con aportes del CICR) y distribuido por primera vez a los Estados Miembros en febrero de 2019; y (ii) una discusión informal con representantes legales de los Estados Miembros bajo las reglas de la "Chatham House" (es decir, las declaraciones hechas durante la reunión

---

Humanitarian Law and the Challenges of Contemporary Armed Conflict (Nov. 2019); CICR, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* (Oct. 2015) 39-44.

[18] Egan, *supra* note **Error! Bookmark not defined.**, at 817 ("Las interpretaciones o aplicaciones del derecho internacional propuestas por grupos no gubernamentales pueden no reflejar la práctica o los puntos de vista legales de muchos o la mayoría de los Estados. El silencio relativo de los estados podría conducir a la imprevisibilidad en el ámbito cibernético, donde los Estados pueden hacer suposiciones sobre las opiniones de los demás sobre el marco legal aplicable. En el contexto de un incidente cibernético específico, esta incertidumbre podría generar percepciones erróneas y errores de cálculo por parte de los Estados, lo que podría conducir a una escalada y, en el peor de los casos, a conflictos.").

[19] *Ver* UNGA Res. 266, *supra* nota **Error! Bookmark not defined.**, ¶3 (sobre el mandato del GEG).

[20] *Ver* U.N. Doc. A/RES/73/27, ¶5 (Dec. 5, 2018). Varios Estados (aún en su mayoría europeos) han utilizado sus comentarios sobre los proyectos de informes del OEWG/GTCA para elaborar puntos de vista sobre cómo se aplica el derecho internacional al ciberespacio. *Ver, por ej.,* Austria, *Comments on Pre-Draft Report of the OEWG - ICT* (March 31, 2020); Ministerio de Relaciones Exteriores de la República Checa, Comentarios presentados por la República Checa en respuesta al informe "preliminar" inicial del Grupo de Trabajo de Composición Abierta sobre la evolución en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional *(Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security)*. Estas y otras presentaciones al GTCA pueden verse en https://www.un.org/disarmament/open-ended-working-group/.

[21] Declaración de la UE, *supra* nota **Error! Bookmark not defined.**.

pueden repetirse, pero las identidades de los oradores y otros participantes permanecen confidenciales). Se incluye una copia del cuestionario en el Anexo A de este informe.

12. Mi tercer informe brindó una actualización sobre el contenido del cuestionario y solicitó una extensión en lo que hacía al plazo de respuesta, con lo cual el Comité estuvo de acuerdo.[22] Mi cuarto informe se refiere a la compulsa que realicé de las respuestas recibidas de nueve Estados: Bolivia, Brasil, Chile, Costa Rica, Ecuador, Estados Unidos, Guatemala, Guyana y Perú. [23] De estos, siete resultaron sustantivos, mientras que los Estados Unidos remitió al Comité sus declaraciones públicas previas.[24] Brasil resaltó su labor pendiente en el GEG (cuyo embajador ocupa la presidencia) como el foro que debería abordar cuestiones sobre la aplicación del derecho internacional.[25] La totalidad de las siete respuestas sustantivas se adjuntan al presente informe como Anexo B.

13. Además de la compulsa de las respuestas al cuestionario, mi cuarto informe catalogó conversaciones informales adicionales al respecto en concierto con consultas celebradas por la Secretaría de la OEA del Comité Interamericano contra el Terrorismo (CICTE) con la Oficina de Asuntos de Desarme de las Naciones Unidas en los días 15-16 de agosto de 2019, y la reunión informal entre sesiones del GTCA. También destaqué tres conclusiones más amplias sobre el estado de la transparencia en la región con respecto al derecho internacional en el ciberespacio:

- En primer lugar, que todos los Estados Miembros que respondieron poseen interés permanente en el estado de derecho, incluido el papel que puede desempeñar el derecho internacional en la regulación del comportamiento del Estado en el ciberespacio.
- Segundo, las respuestas revelan la desigualdad de las capacidades legales del Estado en esta área. Algunos Estados demostraron un profundo conocimiento de las operaciones cibernéticas y los nuevos problemas legales internacionales que ellas plantean, mientras que otros demostraron mucha menos familiaridad con las normas legales internacionales subyacentes y las preguntas particulares que sus aplicaciones generan en el contexto cibernético. Esto sugiere la necesidad de una mayor creación de capacidad jurídica internacional más allá del excelente trabajo realizado hasta la fecha por el CICTE y varios Estados Miembros.[26]

---

[22] Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia: Tercer Informe*, OEA/Ser.Q, CJI/doc 594/19 (Julio 24, 2019) ("Hollis, Tercer Informe"), en http://www.oas.org/en/sla/iajc/docs/CJI_doc_594-19.pdf.

[23] *Ver Nota del Estado Plurinacional de Bolivia, Ministerio de Relaciones Exteriores, Misión Permante de la OEA al Comité Jurídico Interamericano,* MPB-OEA-NV104-19 (Julio 17, 2019) (conteniendo respuestas al Cuestionario del CJI desde la oficina del Comandante en Jefe del Estado Inspector General of de las Fuerzas Armadas) ("Respuesta de Bolivia"); *Respuesta presentada por Chile al Cuestionario del Comité Jurídico Interamericano* (Enero 14, 2020) ("Respuesta de Chile"); *Comunicación de Carole Arce Echeverria, Costa Rica, Organizaciones Internacionales, Departamento de Política Externa, Ministerio de Relaciones Exteriores y Culto a la OEA (Abril3,* 2019) (incluyendo carta No. 163-OCRI2019 de Yonathan Alfaro Aguero, Oficina de Cooperación Internacional y Relaciones a Carole Arce Echeverria, que incluye una respuesta de la « autoridad relevante » - el Tribunal de Apelaciones Penales de Costa Rica ("Respuesta de Costa Rica) *Nota Verbal 4-2 186/2019 de la Misión Permanente de Ecuador a la OEA* (Junio 28, 2019) ("Respuesta de Ecuador "); Nota Of. 4VM.200-2019/GJL/lr/bm, del Sr.Gabriel Juárez Lucas, Cuarto Viceministro del Ministerio del Interior, de la República de Guatemala a Luis Toro Utillano, Secretario Técnico, Comité Jurídico Interamericano (Junio 14, 2019) ("Respuesta de Guatemala"); *Nota Nº: 105/2019 de la Misión Permanente de Guyana a la OEA(Julio 30*, 2019) ("Respuesta de Guyana"); *Respuesta presentada por Perú al Cuestionario sobre la Aplicación del Derecho Internacional en los Estados Miembros de la OEA en el Contexto Cibernético (Junio 2019)* ("Respuesta de Perú ").

[24] *Ver* nota **Error! Bookmark not defined.**.

[25] Respuesta de Brasil al CJI de la OEA Nota 2.2/14/19 (Julio 1, 2019).

[26] Para mayor información sobre las actividades del CICTE, consultar http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp. Más allá del CICTE, varios Estados Miembros apoyaron también el desarrollo de la capacidad

- En tercer lugar, el bajo porcentaje de respuestas al cuestionario del Comité sugiere que los Estados siguen siendo reacios a ser transparentes en sus puntos de vista sobre la aplicación del derecho internacional, incluso cuando se les brindan nuevas oportunidades para hacerlo. Esto sugiere la necesidad de alentar mayores respuestas estatales o buscar sus aportes de maneras menos formales.

14. Con la aprobación del Comité, el plazo para responder al Cuestionario se extendió hasta el 1 de junio de 2020. Lamentablemente, no se recibieron respuestas adicionales. Dicho esto, varios Estados Miembros hicieron declaraciones relevantes en sus comentarios escritos a los borradores de informes del OEWG/GTCA sobre seguridad internacional.[27]

15. Con la asistencia del Departamento de Derecho Internacional de la OEA, iniciamos un segundo vehículo para llevar una mayor variedad de puntos de vista del Estado sobre el derecho internacional y el ciberespacio a la esfera pública: una conversación al estilo de Chatham House sobre el tema. El 23 de junio de 2020, el Departamento de Derecho Internacional organizó, y este servidor moderó, una discusión de casi tres horas que incluyó representantes legales de 16 Estados Miembros y el CICR. La conversación en profundidad confirmó varias de las conclusiones de mi cuarto informe, especialmente la necesidad de una mayor creación de capacidad legal. También destacó varias explicaciones sobre la reticencia de los Estados Miembros a dejar constancia con respecto a la aplicación del derecho internacional al ciberespacio.

16. En este informe, me he detenido en tres aspectos. En primer lugar, estoy actualizando y revisando la compulsa de respuestas de los Estados al Cuestionario del Comité a la luz de la reunión del 23 de junio, así como las declaraciones relevantes de los Estados Miembros en el proceso del OEWG. Esta encuesta revisada se adjunta en el Anexo B de este Informe.

17. En segundo lugar, con base en las consultas del 23 de junio, deseo destacar tres conjuntos de retos - técnicos, políticos y legales - para lograr una mayor transparencia de los Estados Miembros sobre la aplicación del derecho internacional al ciberespacio. Técnicamente, el llamado "problema de atribución" complica la capacidad de los Estados Miembros para hablar públicamente sobre la aplicación del derecho internacional. Los Estados pueden saber que han sido víctimas de un ataque cibernético, pero no pueden discernir si su autor fue un Estado (o un representante del cual un Estado podría ser considerado legalmente responsable). Sin la capacidad técnica (o de otro tipo) de atribuir una operación cibernética a un Estado extranjero, los Estados no pueden invocar el derecho internacional, ya que esa norma solo se aplica si el perpetrador fuese un Estado o un actor del que un Estado podría ser legalmente responsable. Del mismo modo, donde los actores operan de forma anónima, es difícil identificar la práctica estatal requerida (y mucho menos la *opinio juris*) ya que el comportamiento no es atribuible a un Estado.

18. Políticamente, algunos de los problemas de transparencia son internos de los Estados Miembros: varios representantes legales informaron sobre la continua necesidad de organizar mejor la responsabilidad para abordar los problemas relacionados con la cibernética (sus marcos legales y de políticas nacionales aún no han alcanzado la realidad actual). Aunque varios Estados han estado lidiando con problemas de ciberseguridad durante algún tiempo, para otros Estados Miembros estos problemas siguen siendo relativamente nuevos y novedosos. Como tal, varios Estados Miembros

---

legal. Canadá y México, por ejemplo, fueron co-anfitriones junto con la OEA de un taller el 30 de mayo de 2019, destinado a los países de la OEA, para una discusión sobre la aplicación del derecho internacional en el espacio cibernético.

[27] (Ver, por ej., el Segundo "Anteproyecto" del informe del GTCA sobre avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional (Mayo 27, 2020) (*Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security)*, en https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf. Los textos de varias declaraciones nacionales están disponibles en https://www.un.org/disarmament/open-ended-working-group/.

informaron de la falta de experiencia gubernamental (o recursos) en cuestiones relacionadas con la cibernética.

19. En otros casos, se trata de problemas institucionales; la experiencia existe, pero se distribuye de manera que dificulta la fusión en una visión formal del Estado que pueda expresarse públicamente. Varios representantes del Ministerio de Relaciones Exteriores enfatizaron en particular la necesidad de un mayor diálogo interno para garantizar que las cancillerías asuman el papel principal en las discusiones sobre la diplomacia cibernética, incluidas las relevantes para la aplicación del derecho internacional. Al mismo tiempo, el deseo de ciertos Estados de retener la libertad de participar en operaciones cibernéticas ha llevado a una reticencia a tomar posiciones sobre qué operaciones podría prohibir o restringir el derecho internacional para no limitar su futura libertad de maniobra o reacción.

20. Otros participantes en las consultas del 23 de junio identificaron desafíos políticos externos para una mayor transparencia. Está claro que ciertos Estados (por ejemplo, Estados Unidos, Rusia, China) tienen actualmente amplias capacidades para conducir y defenderse contra las operaciones cibernéticas, capacidades que los han llevado a replantear opiniones discretas, y a menudo conflictivas, sobre el papel regulador del derecho internacional. Algunos Estados Miembros indicaron reticencias a hacer señales similares para no involucrar a ese Estado en la competencia y el conflicto entre dichos actores; se trata de problemas que los Estados pueden evitar si permanecen en silencio. Para otros participantes, la transparencia solo debería ocurrir gradualmente, con el tiempo, cuando los Estados Miembros hayan tenido más oportunidades para un diálogo y discusión diplomáticoscuidadosos.

21. Al mismo tiempo, muchos de los participantes del 23 de junio reconocieron que algunas de las razones del silencio del Estado eran tanto legales como políticas: varios Estados Miembros siguen careciendo de la experiencia suficiente sobre cómo el derecho internacional puede manifestarse en el contexto cibernético para formular una opinión sobre algunas de las preguntas más actuales y urgentes (y si un Estado no puede formular una opinión informada, no tiene nada como para ser transparente).[28] Un participante lo expresó sucintamente: "todavía no hemos llegado allí" en términos de estar listos para aplicar el derecho internacional al contexto cibernético.

22. En tercer lugar, dados los resultados del cuestionario y la discusión del 23 de junio, quien les escribe formularía tres propuestas concretas para su consideración específica por parte del Comité y de la OEA y sus Estados Miembros de manera más amplia.

Propuesta 1: El Comité debería recomendar que la Asamblea General de la OEA apoye la aplicabilidad del derecho internacional a las operaciones Estatales y a aquellas patrocinadas por el Estado

23. Como se señaló, la Asamblea General de las Naciones Unidas y varias organizaciones regionales (ASEAN, la UE) han respaldado la aplicabilidad del derecho internacional al comportamiento del Estado en el ciberespacio. Hasta la fecha, sin embargo, la OEA no lo ha hecho. Tal respaldo enviaría una señal clara del compromiso de la organización y la región con el estado de derecho en el ciberespacio. Una posible formulación para tal declaración sería:

> *La Asamblea General de la OEA afirma que el derecho internacional, incluida la Carta de las Naciones Unidas en su totalidad, la Carta de la Organización de los Estados Americanos, el derecho internacional humanitario, el derecho internacional de los derechos humanos, el deber de no intervención, la igualdad soberana de los Estados y el*

[28] Por supuesto, tales Estados podrían ser transparentes sobre su inhabilidad en formular un punto de vista, pero es comprensible que pocos Estados, si los hubiera, deseen formular tal concesión públicamente.

derecho de responsabilidad estatal, son aplicables al uso de las tecnologías de la información y de la comunicación (TIC) por parte de los Estados y de quienes son responsables internacionalmente.

La región de la OEA se beneficia de la aceptación de los Estados Miembros de la aplicación de ciertos regímenes jurídicos internacionales (por ejemplo, el derecho internacional humanitario) donde el consenso global aún no ha sido posible. También he incluido la soberanía en esta lista, aunque algunos Estados Miembros pueden plantear dudas sobre cómo se aplica. En cualquier caso, al adoptar una posición clara sobre qué normas de derecho internacional se aplican, la OEA podría contribuir a esta conversación global y, al hacerlo, promover el estado de derecho.

24. Alternativamente – o como un paso intermedio – el propio Comité podría apoyar dicha formulación en una de sus resoluciones, y enviarla a la Asamblea General para su consideración.

Propuesta 2: Retener este Tema en la Agenda del Comité y expandir su alcance más allá de los temas del derecho internacional, hacia la paz y seguridad internacionales

25. Aunque mi mandato en el Comité expira al final del año calendario, este punto del temario sin duda se beneficiaría de una mayor atención por parte del Comité. Este es el caso ya sea que el Comité (o la Asamblea General) actúe o no sobre mi primera propuesta. Los participantes en la discusión del 23 de junio estaban entusiasmados con la posibilidad de nuevos intercambios diplomáticos. Con la asistencia del Departamento de Derecho Internacional, el Comité podría continuar organizando tales intercambios diplomáticos periódicamente. Sus bajos riesgos y pocos obstáculos para el ingreso brindarían oportunidades para identificar convergencias y divergencias en los puntos de vista estatales, que pueden luego ser organizadas contra la amenaza de operaciones cibernéticas patrocinadas por el Estado carentes de regulación apropiada y libres de restricciones, como hasta la fecha.

26. Con más tiempo y esfuerzo, podría ser posible obtener más puntos de vista "oficiales" de los Estados Miembros para ayudar a cumplir el objetivo general de mejorar la transparencia sobre cómo se aplica el derecho internacional al ciberespacio. Al hacerlo, además, el Comité podría considerar expandir el alcance de la aplicación para cubrir otros temas, además de la paz y la seguridad internacionales, temas esos que dominan los procesos existentes de la ONU. Mi cuestionario no abordaba, por ejemplo, el deber de no intervención, incluso cuando varios representantes del Estado pidieron más atención sobre ese tema en mis consultas del 23 de junio. Del mismo modo, varios participantes pidieron más atención al papel del derecho internacional de los derechos humanos en el ciberespacio; un tema que el Comité podría abordar solo o en concierto con la Comisión Interamericana de Derechos Humanos.

27. Asimismo, el Comité podría tratar de mejorar la transparencia sobre cómo el derecho internacional protege al sector de la salud. La pandemia de COVID 19 ha afectado gravemente a la región tanto en términos humanitarios como económicos. Desafortunadamente, las amenazas cibernéticas corren el riesgo de hacer sufrir aún más daños, como lo demuestran los ataques cibernéticos a los hospitales y, más recientemente, los esfuerzos de investigación de vacunas. Por lo tanto, el Comité podría centralizar su atención en un tema crucial de interés actual, que sería de ayuda para los Estados Miembros y sus nacionales en toda la región.[29]

[29] Para un esfuerzo continuo para aclarar las protecciones del derecho internacional del sector de la salud contra las amenazas cibernéticas, consulte Dapo Akande, Duncan Hollis, Harold Hongju Koh, y Jim O'Brien, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector,* JUST SECURITY (mayo 21, 2020) (envío cruzado en OPINIO JURIS & EJILTALK!).

Propuesta 3: Apoyar o emprender esfuerzos adicionales de creación de capacidad legal

28. El CICTE y varios Estados Miembros han emprendido ya esfuerzos significativos e importantes para crear capacidad sobre cuestiones cibernéticas entre los Estados Miembros, tanto la capacidad de comprender la naturaleza técnica de las TIC como las amenazas que plantean, así como la capacidad de comprender y evaluar los problemas legales que plantean estas amenazas. Sin embargo, tanto las respuestas al cuestionario como las consultas del 23 de junio dejan en claro que queda mucho por hacer, especialmente en el contexto del desarrollo de la capacidad legal. Los participantes en las consultas del 23 de junio se expresaron nutridamente sobre la necesidad de desarrollar capacidades adicionales en la aplicación del derecho internacional en el contexto cibernético. Varios Estados Miembros (por ejemplo, Argentina, Canadá y Estados Unidos) expresaron opiniones similares en sus recientes comentarios al OEWG/GTCA[30]. Por lo tanto, el Comité parecería tener un sólido apoyo si escoge mostrar su disposición a prestar su experiencia o recursos a los esfuerzos existentes de creación de capacidad.

29. Alternativamente, el Comité podría considerar la posibilidad de apoyar o realizar sus propios esfuerzos adicionales (y más diversificados) de creación de capacidad. Los cursos sobre la aplicación del derecho internacional al ciberespacio podrían complementarse con cursos que ofrezcan "capacitación técnica" a expertos no técnicos para ayudar a los diplomáticos estatales y otros representantes a comprender y evaluar con precisión cómo operan las amenazas cibernéticas. Alternativamente, el Comité podría usar sus reuniones con los Asesores Legales del Ministerio de Relaciones Exteriores para "ensayar, como en un juego" ciertos escenarios que involucran amenazas cibernéticas para dar a los abogados del gobierno más oportunidades de aplicar las normas y estándares legales relevantes (y, al así hacerlo, ayudar a facilitar el desarrollo de un Estado sobre su propia visión de cómo se aplica la ley). Finalmente, el Comité podría desear llevar a cabo conversaciones regulares como las que tuvieron lugar en junio, organizando y moderando debates sobre la aplicación del derecho internacional entre los Estados Miembros (y quizás en algún momento, con otras partes interesadas relevantes de la industria y la sociedad civil).

30. En resumen, a través de más esfuerzos de transparencia y creación de capacidad, el Comité podría hacer una contribución importante para mejorar la aplicación (y eficacia) del derecho internacional como herramienta reguladora en el ciberespacio. Además, podría hacerlo solo o en concierto con otras instituciones de la OEA, ciertos Estados Miembros u otras organizaciones. El CICR, por ejemplo, ha expresado su entusiasmo por apoyar más esfuerzos de creación de capacidad en torno al derecho internacional en la región.

31. Ha sido para mí un verdadero privilegio trabajar en este tema durante mi paso por el Comité. Creo en verdad que las amenazas cibernéticas, incluidas las operaciones de los Estados y sus representantes, crean riesgos que tienen importantes consecuencias económicas, humanitarias y de seguridad nacional. El derecho internacional proporciona un mecanismo - que el tiempo ha demostrado - para regular las nuevas amenazas. Sin embargo, los retos técnicos, políticos y legales han hecho que la ley en general (y la práctica del Estado y la *opinio juris* que comprenden la costumbre específicamente) sean menos visibles, y por lo tanto menos efectivas, hasta la fecha. Con más transparencia sobre cómo los Estados entienden la ley para operar, se debería avizorar una mayor oportunidad de desempeñar un papel regulador muy necesario para restringir el comportamiento no

---

[30] *Ver, por ej.,* Argentina, *Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security* ("Anteproyecto"del informe del GTCA sobre la evolución en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional); Michael Walma, *Canadian Comments on Draft OEWG Report* (April 6, 2020); United States, *United States Comments on the Chair's Pre-draft of the Report of the U.N. Open Ended Working Group (OEWG)* (Abril 6, 2020). Estas (y otras) declaraciones Nacionales están disponibles en el *Grupo Trabajo de Composición Abierta (GTCA)* en https://www.un.org/disarmament/open-ended-working-group/.

deseado y facilitar una mayor asistencia y cooperación. Es mi deseo que estos informes sobre los resultados del cuestionario y otras conversaciones dentro de la región pudiesen marcar un primer y modesto paso para mejorar la visibilidad de la aplicación del derecho internacional al ciberespacio. Estimularían también al Comité (y a la OEA) a continuar participando en esfuerzos similares en el futuro y estaré ansioso de ver los productos y procesos resultantes de tales esfuerzos.

ANEXO A

EQO KVû"LWT½FKEQ"KPVGTCO GTKECPQ"
"
EQO KUUœQ"LWT½FKEC"KPVGTCO GTKECPC"
Cx0'O ctgejcnHrqtkcpq."3;8"/"5q"cpfct"/"RcnÑelq"Kco ctcv{"/"Egpvtq"/"Tkq"fg"Lcpgkq."TL"/"422:2/224"/"Dtcuki'
Vgn0<"77/43+"5394/3696"/""
"

OEA/2.2/14/19

El Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la Secretaría General de la Organización de los Estados Americanos, en su calidad de Secretaría Técnica del Comité Jurídico Interamericano (en adelante CJI), saluda muy atentamente a las Misiones Permanentes en ocasión de informarles que el CJI realiza un estudio sobre la aplicación del derecho internacional en el contexto cibernético en los Estados Miembros de la OEA.

Para ello, el Comité solicita muy respetuosamente tenga a bien responder las siguientes preguntas:

1. ¿Ha hecho público 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 ciberespacio? ¿Existen áreas en las cuales la novedad del ciberespacio excluye la aplicación de un conjunto específico de derechos u obligaciones legales internacionales?

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?

Explicaciones adicionales sobre el cuestionario pueden ser consultadas en el informe del CJI titulado "El derecho internacional y las operaciones cibernéticas de los Estados: mejorar la transparencia", documento anexo CJI/doc. 578/19.

Las respuestas deben ser enviadas antes del 28 de junio de 2019 a la Secretaría Técnica del CJI, el Departamento de Derecho Internacional, a través de Luis Toro Utillano por vía electrónica a ltoro@oas.org. Adicionalmente puede contactarnos al Teléfono (202) 370-0632 y al Fax (202) 458-3293.

El Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la Secretaría General de la Organización de los Estados Americanos aprovecha la oportunidad para renovar a las Misiones Permanentes ante la OEA las seguridades de su más alta y distinguida consideración.

Washington, D. C., 20 de marzo de 2019

Anexo B

Respuestas al cuestionario del Comité Jurídico Interamericano del 14 de febrero de 2019 sobre la aplicación del derecho internacional dentro de los Estados Miembros de la OEA en el contexto cibernético[1]

Pregunta 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.

1. En esta primera pregunta se pedían las declaraciones nacionales efectuadas sobre el derecho internacional y el ciberespacio. La idea era que el Comité estuviera al corriente de las opiniones vertidas anteriormente y que los Estados Miembros no tuvieran que responder a las preguntas si ya habían adoptado una posición de fondo pertinente. Sin embargo, de las nueve respuestas, solo en la de Estados Unidos decía que se habían hecho declaraciones y discursos anteriormente sobre la aplicación del derecho internacional al ciberespacio, como los discursos de 2012 y 2016 de los entonces asesores jurídicos del Departamento de Estado y los escritos presentados por Estados Unidos en 2014 y 2016 en reuniones del Grupo de Expertos

[1] Siete Estados-Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana y Perú – respondieron formalmente al cuestionario. *Véase Nota del Estado Plurinacional de Bolivia, Ministerio de Relaciones Exteriores, Misión Permanente de la OEA ante el Comité Jurídico Interamericano*, MPB-OEA-NV104-19 (17 de julio de 2019) (que contiene respuestas de la Oficina del Comando en Jefe de las Fuerzas Armadas del Estado, Inspectoría General de las Fuerzas Armadas, al cuestionario del CIJ ("Respuesta de Bolivia"); *Respuesta presentada por Chile al cuestionario del Comité Jurídico Interamericano de la OEA* (14 de enero de 2020) ("Respuesta de Chile"); *Comunicación de Carole Arce Echeverría, Organismos Internacionales, Dirección General de Política Exterior, Ministerio de Relaciones Exteriores y Culto de Costa Rica a la OEA* (3 de abril de 2019) (a la cual se adjunta la carta 163-OCRI2019, de Yonathan Alfaro Aguero, Oficina de Cooperación y Relaciones Internacionales, dirigida a Carole Arce Echeverría, con la respuesta de la Sala de Casación Penal, (la "instancia pertinente") ("Respuesta de Costa Rica"); *Nota verbal 4-2 186/2019 de la Misión Permanente de Ecuador ante la OEA* (28 de junio de 2019) ("Respuesta de Ecuador"); Nota Of. 4VM.200-2019/GJL/lr/bm, de Gabriel Juárez Lucas, Cuarto Viceministro, Ministerio de Gobernación, a Luis Toro Utillano, Secretaría Técnica del Comité Jurídico Interamericano (14 de junio de 2019) ("Respuesta de Guatemala"); *Nota No: 105/2019 de la Misión Permanente de Guyana ante la OEA* (30 de julio de 2019) ("Respuesta de Guyana"); *Respuesta de Perú al cuestionario sobre la aplicación del derecho internacional en los Estados Miembros de la OEA en el contexto cibernético* (junio de 2019) ("Respuesta de Perú").

La respuesta de Estados Unidos dirigió al Comité a sus declaraciones públicas anteriores. *Véase*, Brian Egan, *Remarks on International Law and Stability in Cyberspace* (10 de noviembre de 2016), en *Digest of U.S. Practice in Int'l Law* 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (octubre de 2016), en *Digest of U.S. Practice in Int'l Law* 823 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (octubre de 2014), en *Digest of U.S. Practice in Int'l Law* 732 (2014); Harold Koh, *International Law in Cyberspace* (18 de septiembre de 2012), en *Digest of U.S. Practice in Int'l Law* 593 (2012). Recientemente, el Asesor Jurídico del Departamento de Defensa de los Estados Unidos pronunció un discurso que incluyó también opiniones formales sobre la aplicación del derecho internacional (aunque no está claro si estaba hablando por Estados Unidos en su conjunto o solamente por el Departamento de Defensa). *Véase, por ejemplo,* Paul C. Ney, "*DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, 2 de marzo de 2020, en: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

Brasil respondió al cuestionario del Comité con la observación de que utilizaría el Grupo de Expertos Gubernamentales de Naciones Unidas (GEG) sobre "Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional" como el foro en el cual abordar estos temas. *Véase*, Respuesta de Brasil al CJI, OEA, Nota 2.2/14/19 (1 de julio de 2019).

Gubernamentales (GEG) de las Naciones Unidas sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional.[2]

2. Otros Estados que respondieron dijeron que no estaban al tanto de posiciones anteriores sobre la aplicación del derecho internacional en el contexto cibernético[3]. Varios aprovecharon la oportunidad para poner de relieve su acción interna encaminada a establecer organizaciones pertinentes o regímenes regulatorios con el fin de abordar asuntos relacionados con las tecnologías de la información y la comunicación (TIC)[4].

3. Varios Estados Miembros han utilizado al Grupo de Trabajo de Composición Abierta sobre Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional patrocinado por Naciones Unidas para efectuar declaraciones públicas que incluyeron referencias a la aplicación del derecho internacional. Sin embargo, en su mayor parte, estas declaraciones se expresaron en términos muy generales o se adaptaron para abordar aspectos específicos del texto del informe del Grupo de Trabajo de Composición Abierta. Varias de estas declaraciones son de Estados que ya respondieron directamente al cuestionario del Comité. Sin embargo, algunos Estados, tales como Argentina, Brasil, Canadá, Colombia, México, Nicaragua y Uruguay efectuaron comentarios pertinentes al cuestionario.[5] Por lo tanto, se presentan a continuación referencias a las declaraciones nacionales.

---

[2] Con respecto a las citas, véase la nota 1 *supra*. Cabe señalar, sin embargo, que en la respuesta de Estados Unidos decía que estos eran solo "algunos" de los documentos en los que expresaba sus opiniones. Por lo tanto, es posible que haya otros que merezcan atención. En particular, podría ser útil saber en qué medida el *Laws of War Manual*, del Departamento de Defensa, refleja los puntos de vista de Estados Unidos en conjunto. Véase Office of General Counsel, U.S. Department of Defense, *Department of Defense Law of War Manual* (junio de 2015, actualizado en diciembre de 2016) ("Manual del Departamento de Defensa").

[3] Véase, por ejemplo, la respuesta de Ecuador, nota 1 *supra*, en 1 ("No se conoce sobre un documento Oficial del Gobierno del Ecuador que sea público, en cuanto a las Operaciones Cibernéticas"); véase también la respuesta de Guyana, nota 1 *supra*, en 1 (ídem).

[4] Respuesta de Bolivia, nota 1 *supra*, en 1 (donde se cita una nueva ley de 2015); respuesta de Chile, nota 1 *supra*, en 1 (donde se menciona la "Política Nacional de Ciberdefensa", del Ministerio de Defensa, publicada el 9 de marzo de 2018); respuesta de Guatemala, nota 1 *supra*, en 1 (donde se señalan la "Estrategia Nacional de Seguridad Cibernética" y la nueva Ley contra la Ciberdelincuencia); véase también la respuesta de Costa Rica, nota 1 *supra*, en 1.

[5] Todas las declaraciones nacionales pueden encontrarse en Naciones Unidas, *Grupo de Trabajo de Composición Abierta*, en el sitio: https://www.un.org/disarmament/open-ended-working-group/. *Véanse, por ejemplo*, Argentina, *Proyecto preliminar del Informe del Grupo de Trabajo de Composición Abierta sobre Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (Comentarios de Argentina"); Brasil, *Comentarios presentados por Brasil al Proyecto preliminar del Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (8 de abril de 2020) ("comentarios de Brasil"); Michael Walma, *Comentarios de Canadá sobre el Proyecto Preliminar de Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (6 de abril de 2020)* ("Comentarios de Canadá"); Colombia, *Comentarios de Colombia sobre el Proyecto Preliminar de Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (16 de abril de 2020) ("comentarios de Colombia"); México, *Comentarios preliminares de México al Proyecto Preliminar de Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (2020) ("comentarios de México"); Nicaragua, *MINIC-MIS-143-04-2020* (abril de 2020) ("comentarios de Nicaragua"); Uruguay, *Comentarios sobre el Proyecto Preliminar de Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (2020) ("comentarios de Uruguay").

Para información sobre los comentarios de otros Estados Miembros, véanse Chile, *Comentarios de Chile al pre-informe del Chair* (2020) ("comentarios de Chile"); Ecuador, *Comentarios Preliminares de*

4. La escasez de declaraciones oficiales anteriores en combinación con el carácter general de las declaraciones realizadas más recientemente confirma la hipótesis en que se basa este proyecto: que los Estados han dicho relativamente poco hasta ahora sobre la forma en que el derecho internacional se aplica al comportamiento de los Estados en el ciberespacio. También confirma que la mayoría de las actividades internas relacionadas con la ciberseguridad se han centrado hasta ahora en estrategias o políticas nacionales en materia de ciberseguridad y de ciberdelincuencia interna, así como en otros aspectos de la reglamentación de las TIC.

Pregunta 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 ciberespacio? ¿Existen áreas en las cuales la novedad del ciberespacio excluye la aplicación de un conjunto específico de derechos u obligaciones legales internacionales?

5. Aunque una resolución reciente de la Asamblea General de las Naciones Unidas[6] parece indicar que ahora hay apoyo generalizado a la aplicación del derecho internacional al ciberespacio, los primeros intentos realizados en las Naciones Unidas revelaron que algunos Estados tenían profundas reservas acerca de la aplicabilidad de ciertos regímenes jurídicos internacionales. De hecho, supuestamente debido a estas reservas, el GEG de las Naciones Unidas que se reunió en 2016 y 2017 no elaboró un informe final[7]. Por lo tanto, subsiste la necesidad de determinar si la existencia de ciertas áreas del derecho internacional en relación con el ciberespacio es un tema controvertido y, si lo es, cuáles son esas áreas. La finalidad de la segunda pregunta era recabar las opiniones de los Estados sobre aspectos del derecho internacional que consideraran inaplicables (o cuya aplicación pudiera ser al menos problemática) en el contexto cibernético.

6. En general, las respuestas al cuestionario reflejan un amplio apoyo a la aplicación de los campos existentes del derecho internacional al ciberespacio. Como se resume en la respuesta de Chile, "el derecho internacional vigente proporciona el marco normativo aplicable [...], incluyendo las normas relativas al *jus ad bellum*, derecho internacional humanitario, derechos humanos y aquellas que regulan la responsabilidad internacional de los Estados"[8]. Otros Estados que confirmaron la aplicación del derecho internacional fueron Ecuador, Perú y Estados Unidos[9]. Junto

---

Ecuador al Proyecto de Informe del Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (abril de 2020) ("comentarios de Ecuador"); Venezuela (Régimen de Maduro) *Consideraciones preliminares de Venezuela al Proyecto de Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (2020) ("comentarios de Venezuela"); Estados Unidos, *Comentarios de Estados Unidos sobre el Proyecto de Informe del Chair del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* (6 de abril de 2020) ("comentarios de Estados Unidos").

[6] Véase, AGNU resolución 266, UN doc. A/RES/73/266 (2 de enero de 2019).

[7] Véase, por ejemplo, Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, en *Lawfare* (4 de julio de 2017), en: https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[8] Respuesta de Chile, nota 1 *supra*, en 1 (en consecuencia, Chile observa que "la planificación, conducción y ejecución de las operaciones en el ciberespacio debe ceñirse estrictamente al respeto del Derecho Internacional Público, con especial consideración al Derecho Internacional de los Derechos Humanos y al Derecho Internacional Humanitario").

[9] Respuesta de Ecuador, nota 1 *supra*, en 1 ("se aplica[n] las ramas del derecho internacional al ciberespacio"); respuesta de Perú, nota 1 en 1 ("considerando el rol esencial que posee la Carta en su vinculación con otros instrumentos internacionales [...], podría considerarse que no existirían áreas de las relaciones internaciones que se encuentren al margen de los principios señalados. Habida cuenta [de] que el ciberespacio se convierte en escenario cotidiano de interacción internacional, los actores de tales relaciones están obligados a respetar las obligaciones mayores del Derecho internacional, entre las que se encuentran la

con el *jus ad bellum* y el *jus in bello,* en la respuesta de Perú se recalca 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 la información, derecho al secreto de las comunicaciones, etc."[10]. Estados Unidos se hace eco de la aplicación del derecho internacional de los derechos humanos, al mismo tiempo que plantea la aplicación del derecho internacional como "piedra angular" de su política para el ciberespacio[11].

7. Bolivia también da una respuesta positiva, pero centrada en el derecho internacional "destinado a ser aplicado en los conflictos armados", con opiniones sobre la forma de distinguir los casos en que el derecho internacional humanitario se aplicaría y aquellos en los que no se aplicaría[12]. Por consiguiente, no resulta claro si la respuesta positiva de Bolivia se extiende a la aplicación de otros subcampos del derecho internacional además del *jus ad bellum* y el *jus in bello*.

8. Guatemala y Guyana apoyan la aplicación del derecho internacional. No obstante, ambos formulan salvedades con respecto al alcance universal de la aplicación del derecho existente. Sin dar ningún ejemplo, Guatemala observa que podría haber áreas en las cuales "la novedad del ciberespacio sí excluya la aplicación de determinados derechos u obligaciones de carácter internacional"[13]. Guyana, entretanto, señala que las operaciones cibernéticas no se encuadran en conceptos tradicionales y que hay un enconado debate con respecto a si los campos existentes del derecho internacional se aplican al ciberespacio[14]. Teniendo en cuenta el trabajo anterior del GEG, Guyana afirma que, aunque se reconoce que el derecho internacional debería aplicarse al ciberespacio, es difícil aplicar principios existentes tales como el uso de la fuerza, que tradicionalmente implica un elemento físico y ataques con algún tipo de arma[15].

9. Por consiguiente, aunque la aplicación general del derecho internacional a las operaciones cibernéticas parece estar firmemente arraigada, las dos últimas respuestas parecen indicar la necesidad de continuar el diálogo. Sería útil indicar *qué áreas* particulares de aplicación del derecho internacional dan que pensar a algunos Estados y por qué. Eso ayudaría a comprender el grado de convergencia (o divergencia) de opiniones sobre la forma en que los regímenes jurídicos internacionales rigen las operaciones cibernéticas de los Estados o patrocinadas por los Estados.

10. Los comentarios de los Estados Miembros al Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional refuerzan estos aspectos. Los mismos reflejan el amplio consenso de que el derecho internacional, incluida la Carta de las Naciones Unidas, se aplica al espacio cibernético. Canadá, Chile, Colombia, México, Uruguay y Estados Unidos expresaron todos esta

---

prohibición del uso de la fuerza, el derecho a la legítima defensa y el respeto por los derechos humanos y el derecho internacional humanitario"); Koh, nota 1 en 594 (donde se señala que los principios del derecho internacional se aplican al ciberespacio, el cual no es una zona "desprovista de leyes" donde cualquiera pueda realizar actividades hostiles sin restricciones y sin atenerse a regla alguna).

[10] Respuesta de Perú, nota 1 supra, en 1.

[11] Escrito presentado por Estados Unidos al GGE en 2014, nota 1 *supra*, en 733 (la aplicación del derecho internacional es la "piedra angular" de las opiniones de Estados Unidos, habida cuenta de sus características distintivas); Egan, nota 1 *supra*, en 815. Sobre la aplicación de los derechos humanos, véanse Koh, nota 1 *supra*, en 598; Egan, nota 1 *supra*, en 820; escrito presentado por Estados Unidos al GGE en 2016, nota 1 *supra*, en 824.

[12] Respuesta de Bolivia, nota 1 *supra*, en 2 a 7. Bolivia indica que el derecho internacional humanitario no regiría las operaciones cibernéticas relacionadas con la seguridad nacional, la propaganda, el espionaje, la manipulación de la estructura estratégica crítica, las operaciones cibernéticas con fines políticos o la piratería de sistemas privados que ponga en peligro las operaciones económicas y sociales del Estado. Íd. en 3 a 7.

[13] Respuesta de Guatemala, nota 1 *supra*, en 1 y 2.

[14] Respuesta de Guyana, nota 1 *supra*, en 1 y 2.

[15] Íd.

idea de forma explícita.[16] Algunos Estados (por ejemplo, Nicaragua y Venezuela (representado por el régimen de Maduro) cuestionaron la conveniencia del derecho internacional vigente en el espacio cibernético aún si los mismos aceptaron su aplicación en dicho contexto. [17] Otros comentarios agregaron un nuevo grado de preocupación que no se planteó en las respuestas al cuestionario del Comité; por ejemplo, si las diferencias en la capacidad jurídica podrían afectar la verdadera aplicación o evolución de la ley (dado que los Estados que poseen una infraestructura avanzada en ciberseguridad podrían contar con la correspondiente capacidad para influir de manera desproporcionada en el contenido y los límites de las normas en materia de espacio cibernético sobre los Estados que carecen de dicha capacidad).[18]

Pregunta 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?

11. La mayoría de los Estados, pero no todos, parecen aceptar la aplicación del derecho internacional sobre el uso de la fuerza (por ejemplo, el *jus ad bellum*) a sus operaciones cibernéticas. La finalidad de esta pregunta era determinar qué Estados de la región se adhieren a esta posición predominante y cuáles a otras posiciones. Al mismo tiempo, han surgido otras cuestiones con respecto a la aplicación entre los Estados que aceptan el *jus ad bellum* en el ciberespacio, en particular la medida en que los umbrales para el "uso de la fuerza" o los "ataques armados" requieren que haya efectos "violentos" análogos a los que antes se consideraba que superaban esos umbrales. La cuestión ahora es cómo manejar las novedades en la escala o los efectos de las operaciones cibernéticas (es decir, las operaciones que no son similares a operaciones cinéticas pasadas que superaron el umbral del uso de la fuerza ni a sanciones económicas o políticas que no superaron el umbral). ¿Cómo debe el derecho internacional considerar esas operaciones cibernéticas? ¿Deben colocarse automáticamente por debajo o por encima del umbral del uso de la fuerza o se necesitan más investigaciones y análisis para dividir las operaciones cibernéticas de esta nueva "zona gris" según estén por encima o por debajo de los umbrales correspondientes?[19] En consecuencia, con esta pregunta se procuraba saber si los Estados consideran las operaciones cibernéticas como casos de uso de la fuerza (o ataques armados) enteramente por analogía con casos anteriores o si creen que es necesario establecer una norma nueva con ese fin.

---

[16] *Véase,* Comentarios de Canadá, nota **Error! Bookmark not defined.** *supra*; Comentarios de Colombia, nota **Error! Bookmark not defined.** *supra*; Comentarios de Chile, nota **Error! Bookmark not defined.** *supra*; Comentarios de México, nota **Error! Bookmark not defined.** *supra*; Comentarios de Estados Unidos, nota 5 *supra*; Comentarios de Uruguay, nota **Error! Bookmark not defined.** *supra*.

[17] Comentarios de Nicaragua, nota **Error! Bookmark not defined.** *supra* (sugieren que nos enfrentamos con una "aplicabilidad deficiente" del derecho internacional en esta esfera pero no niega en principio que el derecho internacional se aplica a la esfera de las tecnologías de la información y la comunicación); Comentarios de Venezuela, nota 5 *supra* (reafirma la necesidad de "adaptar el derecho internacional al contexto de las TIC, teniendo en cuenta los vacíos jurídicos existentes"). En sus comentarios al Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, Argentina solicitó que se bifurcaran las sugerencias del Grupo de Trabajo de Composición Abierta para clarificar la aplicación de la prohibición sobre el uso de fuerza y el derecho internacional humanitario. *Véase,* Comentarios de Argentina, *supra*, nota 5.

[18] *Véase, por ejemplo,* Comentarios de México, *supra*, nota 5; Comentarios de Bolivia *supra*, nota 5; Comentarios de Ecuador, *supra*, nota 5.

[19] Véase Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace,* 42 *Yale J. Int' L.* 1 (2017).

12. Bolivia, Chile, Guatemala, Perú y Estados Unidos entienden claramente que las operaciones cibernéticas por sí solas podrían generar la prohibición del uso de la fuerza y el derecho inherente de autodefensa para responder a un "ataque armado"[20]. Como explicó Guatemala:

> una operación cibernética por sí misma puede constituir un uso de fuerza, ya que el uso de la fuerza no se refiere exclusivamente a la fuerza física, sino además a los riesgos o vulneraciones que se hagan a la seguridad y la protección de los terceros. [...] existe el derecho de legítima defensa ante un ataque u operación cibernética que atente contra la soberanía de un país[21].

En el escrito presentado al GEG en 2014, Estados Unidos puso de relieve su idea de que el derecho inherente a la legítima defensa podría aplicarse al uso ilegal de la fuerza, lo cual parece indicar un solo umbral para ambas normas[22]. Eso difiere de la postura de los Estados que consideran que todos los ataques armados constituyen uso de la fuerza, pero no todos los casos de uso de la fuerza constituyen ataques armados (los cuales implicarían solo las formas "más graves" de uso de la fuerza)[23]. Estados Unidos afirmó también que puede ejercer su derecho inherente de legítima defensa a raíz de actividades cibernéticas que representen un ataque armado real o inminente, independientemente de que el atacante sea un Estado o un agente no estatal[24].

13. En cambio, Guyana expresa dudas en su respuesta con respecto a la aplicabilidad del *jus ad bellum* a las operaciones únicamente cibernéticas. Basándose en la definición de fuerza que aparece en *Black's Law Dictionary* ("poder considerado de manera dinámica"), Guyana señala que es posible que una operación cibernética de por sí no constituya uso de la fuerza[25]. Asimismo, afirma que un ataque armado implica el uso de armamento y que una operación cibernética, que no

---

[20] Respuesta de Bolivia, nota 1 en 2 a 7; respuesta de Chile, nota 23 en 1 (Chile se abstendrá del uso de la fuerza "a través del ciberespacio" de una manera que contravenga el derecho internacional y podrá ejercer "su derecho a la legítima defensa frente a un ataque armado perpetrado a través del ciberespacio"); Respuesta de Guatemala, nota 23 *supra*, en 2; respuesta de Perú, nota 1 *supra*, en 1 a 3; Koh, nota 1 *supra*, en 595 (donde se presenta la opinión de Estados Unidos de que *a*) las actividades cibernéticas podrían constituir uso de la fuerza en ciertas circunstancias de acuerdo con el significado establecido en el artículo 2.4 de la Carta de las Naciones Unidas y el derecho internacional consuetudinario, y *b*) las actividades de redes informáticas que representen un ataque armado o una amenaza inminente de ataque armado podrían llevar al ejercicio del derecho nacional de legítima defensa de un Estado, reconocido en el artículo 51 de la Carta de las Naciones Unidas); escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 734; Egan, nota 1 *supra*, en 816 (donde se indica que el GEG de las Naciones Unidas que se reunió en 2015 refrendó el derecho a la legítima defensa). Ecuador también respondió a la pregunta de manera afirmativa, pero citó la definición de "ataque armado" que se usa en el artículo 92 del manual *Tallinn 2.0*, donde se define esta expresión en el contexto de un conflicto armado (es decir, el *jus in bello*), a diferencia de la forma en se usa en el artículo 51 de la Carta de las Naciones Unidas y en el *jus ad bellum*. Véase la respuesta de Ecuador, nota 1 *supra*, en 1.; MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); *Véase,* también *CICR*, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict*. En sus comentarios al Grupo de Trabajo de Composición Abierta, Colombia expresó la idea de que la autodefensa es "esencial para mantener la paz y la estabilidad en el entorno de las TIC". Comentarios de Colombia, *supra*, nota 5.

[21] Respuesta de Guatemala, nota 1 *supra*, en 2; respuesta de Perú, nota 1 *supra*, en 3 (donde se cita al CICR y a Michael Schmitt, según los cuales los usos de la fuerza no se limitan a la fuerza cinética).

[22] Koh, nota 1 *supra*, en 597.

[23] Véase *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)* [1986] ICJ Rep. 14, párrafos 176 y 191 (27 de junio) (donde se describen los ataques armados como las formas más graves de uso de la fuerza).

[24] Escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 734 y 735. En el escrito se reitera también la prueba de la falta de voluntad o de capacidad para defenderse de un Estado sin su consentimiento en los casos en que un Estado territorial no esté dispuesto a parar o prevenir un ataque real o inminente lanzado en el ciberespacio o por medio del mismo o no pueda hacerlo. Íd. en 735.

[25] Respuesta de Guyana, nota 1 *supra*, en 2.

implica el uso de armamento físico, no puede considerarse como un ataque armado que genere el ejercicio de la legítima defensa[26]. Al mismo tiempo, Guyana recalca que es posible que se usen operaciones cibernéticas en conflictos armados, que estarían regidas por el derecho internacional humanitario[27].

14. Con respecto a si una operación cibernética puede cruzar el umbral del uso de la fuerza (o de un ataque armado[28]) sin tener efectos violentos, las opiniones de los Estados son variadas. La mayoría de los Estados que respondieron prefieren trazar los umbrales pertinentes por medio de analogías entre las operaciones cibernéticas y operaciones pasadas, cinéticas o de otro tipo, que reunían o no los requisitos para ser consideradas como uso de la fuerza o ataque armado. Sin embargo, algunos Estados mencionan la posibilidad de no limitarse a analogías de ese tipo. Chile, por ejemplo, señala que las operaciones cibernéticas análogas al umbral de gravedad necesario para cumplir los requisitos establecidos en el derecho internacional para ser consideradas como un ataque armado pueden generar el derecho de legítima defensa[29]. Al mismo tiempo, la respuesta de Chile posiblemente deje margen para definir los ataques armados en términos más generales al indicar 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[30].

15. Perú admite más abiertamente "la posibilidad de que pueda ser calificada como uso de la fuerza o ataque armado una operación cibernética que no tenga efectos violentos"[31]. Sin embargo, se basa en la idea de que, en el pasado, posiblemente también se haya usado armamento cinético sin causar efectos violentos y, aun así, haya constituido uso de la fuerza (por ejemplo, el lanzamiento de un misil que cruce el territorio de otro Estado aunque no caiga en dicho Estado)[32]. En general, Perú recalca la necesidad de hacer una distinción entre los "ciberataques" (que implican que "se cause daño a un objetivo militarmente relevante, el mismo que puede ser destruido total o parcialmente, incluso capturado o neutralizado") y una "interrupción abrupta de las comunicaciones en el espacio cibernético", es decir, "las operaciones cibernéticas que causan inconvenientes, incluso inconvenientes extremos, pero no lesiones directas ni muertes, ni destrucción de la propiedad"[33]. En consecuencia, en su respuesta específica, Perú recalca la determinación de la legalidad de las operaciones cibernéticas en el contexto del uso de la fuerza teniendo en cuenta si pueden "generar la muerte o lesión de personas o bienes"[34].

16. Guatemala adopta un enfoque diferente en su respuesta y expresa la voluntad de repensar lo que constituye "efectos violentos" porque las consecuencias de una operación cibernética pueden ser "superiores y ulteriores, amenazando sectores como salud, seguridad entre otros"[35]. Indica que, en el contexto cibernético, las consecuencias que producen "muerte, zozobra, pobreza" deberían considerarse violentas[36].

17. Bolivia señala en su respuesta que podría ser difícil aplicar el umbral en la práctica porque "los efectos de los ciberataques no siempre serán conocidos de inmediato", debido a lo cual es difícil verificar si ha habido uso de la fuerza. Al mismo tiempo, Bolivia indica que evaluará el

---

[26] Íd.
[27] Véase íd. en 3 y 5.
[28] Esto parte del supuesto de que podría haber dos umbrales diferentes, contrariamente a la opinión de Estados Unidos. Véanse las notas 23-25 *supra* y el texto acompañante.
[29] Respuesta de Chile, nota 1 *supra*, en 2.
[30] Íd. en 2.
[31] Respuesta de Perú, nota 1 *supra*, en 3.
[32] Íd.
[33] Íd. en 2.
[34] Íd. en 3.
[35] Respuesta de Guatemala, nota 1 *supra*, en 2.
[36] Íd.

umbral sobre la base de analogías con el contexto cinético, es decir que se trataría de un "ataque armado" si "el ataque virtual cibernético utiliza medios no convencionales pero que tienen el mismo impacto de un ataque armado"[37].

18. Por último, Estados Unidos no respondió al cuestionario en sí, pero sus declaraciones anteriores arrojan luz sobre sus opiniones. En su discurso seminal de 2012, Harold Koh indicó la preferencia de Estados Unidos por un enfoque contextual para identificar casos de uso de la fuerza (aunque con la salvedad antedicha de que la definición utilizada por Estados Unidos abarca también los ataques armados):

> Al determinar si un evento constituyó uso de la fuerza en el ciberespacio o por medio del mismo, debemos evaluar factores tales como el contexto del evento, el perpetrador del acto (habida cuenta de las dificultades para la atribución en el ciberespacio), el objetivo y la ubicación, los efectos y la intención, entre otros posibles aspectos[38].

Al mismo tiempo, Koh considera claramente que la prueba requiere una analogía y pregunta si la lesión física directa y el daño patrimonial resultantes del evento cibernético parecen lo que se consideraría como un caso de uso de la fuerza si los hubieran producido armas cinéticas[39]. Menciona también ejemplos concretos de operaciones cibernéticas que constituirían uso de la fuerza: i) fusión del núcleo del reactor de una planta nuclear causada por un acto cibernético; ii) operaciones cibernéticas que abren una presa río arriba de una zona poblada y causa destrucción, y iii) una operación cibernética que inutiliza el control del tráfico aéreo y ocasiona accidentes de aviación[40]. En la medida en que todos estos ejemplos implican alguna forma de "violencia", parecería que Estados Unidos favorece un umbral para el uso de la fuerza análogo al utilizado en el contexto cinético.

Pregunta 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?

Pregunta 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?

19. Los Estados son responsables del comportamiento no solo de sus propios órganos y dependencias en el ciberespacio, sino también de todo agente no estatal que apoye o controle[41]. En la cuarta y quinta preguntas se inquiere qué entienden los Estados acerca de la asignación de responsabilidad jurídica internacional por actos de agentes no estatales, en particular el grado de "control" requerido por el Estado. Como es bien sabido, las amenazas cibernéticas pueden ser perpetradas no solo por Estados directamente, sino también por diversos agentes no estatales, entre ellos grupos hacktivistas y organizaciones ciberdelictivas. En algunos casos, los Estados tratan de

---

[37] Respuesta de Bolivia, nota 1 *supra*, en 2 a 7 (Bolivia recalca que el derecho de legítima defensa abarca también la "legítima defensa anticipada", a la que se puede recurrir solo cuando la amenaza es inminente y la necesidad de defenderse es inmediata (en vez de ser una represalia).

[38] Koh, nota 1 *supra*, en 595 ("las actividades cibernéticas que, en forma directa o inmediata, ocasionan muertes, lesiones o gran destrucción probablemente se consideren como uso de la fuerza". Estados Unidos ha mantenido este punto de vista desde entonces. Véase el escrito presentado al GEG en 2014, nota 1, en 734. Este escrito se anexó al de 2016, lo cual indica que su contenido seguía siendo válido.

[39] Koh, nota 1 *supra*, en 595.

[40] Íd.

[41] Véase Comisión de Derecho Internacional, *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*, en *Informe sobre la labor realizada en su quincuagésimo primer período de sesiones* (3 de mayo a 23 de julio de 1999), UN doc. A/56/10 55 [3]; *Tallinn 2.0,* nota 20 *supra*, regla 15.

utilizar estos agentes no estatales como sustitutos para llevar a cabo diversas operaciones cibernéticas.

20. Rastrear los actos de un sustituto y vincularlos a un autor principal en el ciberespacio puede ser bastante difícil desde el punto de vista técnico (aunque quizá no tan difícil como algunos suponían antes). Al mismo tiempo, un nexo fáctico no es suficiente, sino que debe haber también una atribución jurídica, es decir, una conexión suficiente entre un Estado y un agente no estatal para que el primero asuma la responsabilidad jurídica por los actos del segundo. Por ejemplo, un Estado podría refrendar los actos de un agente no estatal a posteriori y, de esta forma, asumir la responsabilidad jurídica por ellos[42]. Otra posibilidad es que los Estados sean jurídicamente responsables por los actos de los agentes estatales que operan bajo su control, aunque el grado de control no suele ser claro. En el caso de Nicaragua, la Corte Internacional de Justicia (CIJ) indicó que el derecho internacional contiene una regla que impone responsabilidad al Estado por actos de agentes no estatales sobre los cuales tenga un "control efectivo" (es decir, si ordena el acto o dirige una operación)[43]. Sin embargo, pocos años después, el Tribunal Penal Internacional para la Antigua Yugoslavia adoptó una norma menos estricta de "control general" a efectos del derecho internacional humanitario. Según el Tribunal, esta prueba requiere algo más que el mero suministro de equipo, adiestramiento militar o asistencia financiera, pero no insiste en la emisión de órdenes específicas por el Estado ni en su conducción de las operaciones[44]. Posteriormente, la Corte Penal Internacional refrendó la norma del "control general"[45].

21. Sin embargo, la CIJ ha seguido insistiendo en su fórmula del "control efectivo" en el contexto del uso de la fuerza. Al mismo tiempo, afirma que la prueba del "control general" podría ser apropiada en el contexto del derecho internacional humanitario, lo cual plantea la posibilidad de un consenso sobre el "control general" en el contexto del derecho internacional humanitario y el "control efectivo" en otros contextos[46]. En vista de ello, en el cuestionario se preguntó acerca de la responsabilidad del Estado tanto en general como en el contexto del derecho internacional humanitario sobre la base de la existencia de un conflicto armado tal como se usa esta expresión en los Convenios de Ginebra.

22. En su respuesta, varios Estados Miembros ponen de relieve la dificultad de la atribución en el ciberespacio[47]. Otros se centran menos en la cuestión de la responsabilidad por actos de sustitutos y más en el deber del Estado de cerciorarse de que su territorio no sea utilizado por agentes no estatales para lanzar ataques[48]. En ese sentido, Perú comenta que "la inercia de un

---

[42] Artículos sobre la responsabilidad del Estado, nota 41 *supra*, art. 11; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* 52 (2012).

[43] *Nicaragua Case*, nota 23 *supra*, párr. 115.

[44] *Prosecutor v. Dusko Tadić aka 'Dule'* (Sentencia) ICTY-94-1-A (15 de julio de 1999), párrs. 131 a 145 y 162.

[45] *Prosecutor v. Lubanga*, Caso No. ICC-01/04-01/06, Sala de Primera Instancia, Sentencia (Corte Penal Internacional, 14 de marzo de 2012).

[46] *Case concerning application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Sentencia) [1997] ICJ Rep. 43, 208–09, párrs. 402 a 407 (donde se indica que la prueba del control general bien podría aplicarse a los tipos de clasificaciones que se usan en el derecho internacional humanitario y ser apropiada para ellos).

[47] Respuesta de Guatemala, nota 1 *supra*, en 3 (donde se indica que "es sumamente complicado" determinar una clara responsabilidad por un ataque cibernético); Respuesta de Perú, nota 1 *supra*, en 4 (donde se señala que existe gran "incertidumbre en la atribución, y los niveles de atribución, de la autoría de los ciberataques", lo cual dificulta la posibilidad de "control de aquellos que utilizan el ciberespacio para desencadenar ataques vía Internet").

[48] Respuesta de Ecuador, nota 1 *supra*, en 1 ("Los Estados no tienen responsabilidad de un ataque de un actor no estatal, sin embargo, debería existir la forma de colaborar para encontrar a los responsables de los mismos. Así también es responsabilidad del Estado regular/normar los servicios a fin de evitar que se pueda producir un ataque desde el territorio perteneciente a un Estado"); Respuesta de Guatemala, nota 1 *supra*, en 3 (donde

Estado respecto de un actor no estatal que pudiera desencadenar un ciberataque hacia otro Estado y que estuviera en capacidad de controlar podría generar que su comportamiento sea atribuible al Estado"[49]. Bolivia, por su parte, afirma que los Estados no tienen responsabilidad si carecen de la infraestructura tecnológica necesaria para controlar a los agentes no estatales[50]. Estados Unidos señala que "el mero hecho de que una actividad cibernética haya sido lanzada desde el territorio de otro Estado, se origine de otra forma en dicho territorio o haya sido lanzada desde la infraestructura cibernética de otro Estado es insuficiente, ante la falta de más elementos, para atribuir esa actividad al Estado"[51].

23. Los Estados que se concentran en la cuestión de los agentes sustitutos atribuyen gran importancia a los artículos sobre la responsabilidad del Estado. Chile, Guyana y Perú basan su respuesta en el artículo 8:

> Un Estado será responsable por una operación cibernética internacionalmente ilícita cuando esta haya sido perpetrada a través de alguno de sus órganos, por alguna persona o entidad ejerciendo autoridad gubernamental, o bien por una persona o grupo de personas actuando conforme a las instrucciones o bajo la dirección o control de dicho Estado[52].

Sin embargo, en los artículos sobre la responsabilidad del Estado no se formula una opinión sobre el grado de "control" que el Estado debe ejercer, sino que es un asunto que debe valorarse en cada caso[53]. Esto concuerda con la opinión de Estados Unidos, que refrenda la responsabilidad del Estado por las actividades realizadas por medio de "agentes sustitutos" que actúan siguiendo instrucciones del Estado o bajo su dirección o control, aunque dice solamente que el grado de control ejercido debe ser "suficiente"[54]. Estados Unidos también ha reconocido que un Estado puede reconocer o adoptar a posteriori una operación cibernética de un agente no estatal como si fuera propia[55].

24. Chile, en cambio, al exponer su punto de vista sobre el grado de control necesario para que haya responsabilidad jurídica, menciona las causas de *Nicaragua* y del *Genocidio* y opina que "el grado o estándar de control o participación que debe tener un Estado en las operaciones de un actor no estatal para desencadenar su responsabilidad internacional es el de control efectivo"[56].

---

responde desde la óptica de la debida diligencia del Estado anfitrión en vez del grado de control ejercido sobre agentes sustitutos).

[49] Respuesta de Perú, nota1 *supra*, en 4 (donde se cita el artículo 11 de los artículos sobre la responsabilidad del Estado).

[50] Respuesta de Bolivia, nota 1 *supra*, en 3 a 7. La respuesta de Bolivia a la pregunta sobre los sustitutos es indirecta, aunque indica la existencia de un nexo entre un Estado y los agentes no estatales vinculados a los objetivos o las estrategias de la política de defensa del Estado en una situación de conflicto armado. Íd.

[51] Escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 738.

[52] Artículos sobre la responsabilidad del Estado, nota 41 *supra*, art. 8; respuesta de Chile, nota 1 *supra*, en 2; respuesta de Guyana, nota 1 *supra*, en 3; respuesta de Perú, nota 1 *supra*, en 4. Las respuestas de Chile y Perú también parecen basarse en el artículo 5 de los artículos sobe la responsabilidad del Estado, en el cual se asigna responsabilidad al Estado por "el comportamiento de una persona o entidad que [...] esté facultada por el derecho de ese Estado para ejercer atribuciones del poder público, siempre que, en el caso de que se trate, la persona o entidad actúe en esa capacidad". Véanse la respuesta de Chile, nota 1 *supra*, en 2, y la respuesta de Perú, nota 1 *supra*, en 4.

[53] Artículos sobre la responsabilidad del Estado, nota 41 *supra*, en 48 (comentario sobre el artículo 8).

[54] Koh, nota 1 *supra*, en 595; escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 738 (ídem); Egan, nota 1 *supra*, en 821; escrito presentado por Estados Unidos al GEG en 2016, nota 1 *supra*, en 826.

[55] Egan, nota 1 *supra*, en 821; escrito presentado por Estados Unidos al GEG en 2016, nota 1 *supra*, en 826.

[56] Respuesta de Chile, nota 1 *supra*, en 2.

Asimismo, opina que las normas relativas a la responsabilidad del Estado son las mismas en el contexto de los conflictos armados[57].

25. En lo que concierne al derecho internacional humanitario, Perú adopta una posición similar, que favorece una regla uniforme con respecto a la responsabilidad del Estado tanto en conflictos armados como en otros contextos. Aunque reconoce la posibilidad de que los artículos sobre la responsabilidad del Estado se reemplacen con una *lex specialis,* indica que para eso se necesita un análisis exhaustivo. En este caso, "[d]e la revisión de los Convenios de Ginebra no se identifica una alteración respecto de las normas relativas a la responsabilidad internacional plasmadas en el Proyecto de Artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos, por lo tanto, no se puede sostener un cambio respecto al ámbito de aplicación de este proyecto"[58] Sin embargo, en la norma sobre responsabilidad enunciada en los artículos sobre la responsabilidad del Estado se hace referencia al "control" solo en forma general, sin distinguir si debe ser "efectivo" o "general".

26. Otros Estados tuvieron más dificultades para responder a la pregunta 5. Guatemala indica que "es necesario continuar las discusiones en foros internacionales sobre los aspectos únicos y diferentes que presentaría un conflicto en el ciberespacio, especialmente aspectos como la atribución y la territorialidad de los ataques"[59]. Otros Estados entendieron que la pregunta se refería a las diferencias en las normas en materia de responsabilidad en los casos de conflictos armados internacionales y sin carácter internacional[60].

Pregunta 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?

27. La sexta pregunta es la primera de dos que abordan la forma en que el derecho internacional humanitario (o *jus in bello*) se aplica a las operaciones cibernéticas. Se centra en un asunto que ha dividido a los Estados y a los expertos hasta la fecha: cómo definir un "ataque" a efectos del derecho internacional humanitario. Gran parte de esta rama del derecho, incluidos sus principios fundamentales de distinción, proporcionalidad y precauciones, está formulada mayormente desde el punto de vista de la prohibición de ciertos tipos de "ataques" (por ejemplo, los dirigidos contra civiles u objetivos civiles) y la autorización de otros (por ejemplo, los dirigidos contra objetivos militares)[61]. Como señaló recientemente el CICR, el tema de la interpretación amplia o estricta del concepto de "ataque" en relación con las operaciones cibernéticas es esencial

---

[57] Íd. en 3.

[58] Respuesta de Perú, nota 1 *supra*, en 4 y 5.

[59] Respuesta de Guatemala, nota 1 *supra*, en 3.

[60] Véanse, por ejemplo, la respuesta de Bolivia, nota 1 *supra*, en 4 a 7, y la respuesta de Guyana, nota 1 *supra*, en 3. En la respuesta de Ecuador simplemente se recalca que "los Estados son los responsables por cumplir las normas en los conflictos armados, aun cuando existan partes que no formen parte del convenio" correspondiente. Respuesta de Ecuador, nota 1 *supra*, en 2.

[61] Por ejemplo, el principio de distinción se plantea regularmente como la prohibición de que la población civil sea el objeto de un ataque. Véanse, por ejemplo, Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I) (8 de junio de 1977), 1125 UNTS 3, art. 5.2 ("Protocolo adicional I"); Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional (12 de diciembre de 1977), 1125 UNTS 609, art. 13.2; Estatuto de Roma de la Corte Penal Internacional (17 de julio de 1998), art. 8.2.b.f; Convención relativa a las leyes y costumbres de la guerra terrestre (H.IV) y su anexo: Reglamento relativo a las leyes y costumbres de la guerra terrestre (18 de octubre de 1907), 36 Stat. 2277, art. 8.2.b.i-ii; Jean Marie Henckaerts y Louise Doswald-Beck, *Customary International Humanitarian Law* (ICRC, 2005), reglas 1, 7, 9 y 10.

para la aplicabilidad de estas normas y la protección que confieren a los civiles y a la infraestructura civil[62]. En efecto, en la medida en que una operación *no* constituya un "ataque", podría realizarse en el marco de un conflicto armado sin tener en cuenta la mayoría de las normas del derecho internacional humanitario[63].

28. De conformidad con el derecho internacional humanitario, se entienden por "ataques" en el derecho internacional consuetudinario (codificado en el artículo 49 del Protocolo adicional I a los Convenios de Ginebra) "los actos de violencia contra el adversario, sean ofensivos o defensivos"[64]. Asimismo, tal como se explica en el *Tallinn Manual 2.0*, "las consecuencias, no su índole, por lo general determinan el alcance del término 'ataque'; la 'violencia' debe considerarse en el sentido de las consecuencias violentas y no se limita a los actos violentos"[65]. El CICR ha señalado que "tiene amplia aceptación la idea de que las operaciones cibernéticas que se prevé que causen muertes, lesiones o daños físicos constituyen ataques de conformidad con el derecho internacional humanitario"[66]. Sin embargo, es bien sabido que algunas operaciones cibernéticas (por ejemplo, el *ransomware* o programa de secuestro de archivos a cambio de un rescate) son novedosas porque pueden perturbar el funcionamiento de objetos sin dañarlos físicamente[67]. Eso lleva a la pregunta de si las operaciones cibernéticas que no producen efectos de ese tipo (por ejemplo, la interrupción del funcionamiento de una planta potabilizadora sin causar necesariamente un daño físico) pueden constituir un ataque. Han surgido opiniones divergentes hasta la fecha, incluso entre los integrantes del grupo independiente de expertos que elaboró el *Tallinn Manual 2.0*[68].

29. La mayoría de los autores del *Tallinn Manual 2.0* opinan que, para que haya violencia, debe haber algún daño físico que requiera, por ejemplo, el "reemplazo de componentes físicos" tales como un sistema de control[69]. Otros entienden que el daño incluye los casos en que no sea necesario reemplazar componentes físicos y se pueda restablecer el funcionamiento reinstalando el sistema operativo, mientras que unos pocos expertos consideran que un ataque podría consistir en la "pérdida de aptitud para el uso de la infraestructura cibernética" en sí[70]. El CICR, por su parte, ha argumentado que, en un conflicto armado, una operación con la finalidad de poner fuera de servicio una computadora o una red informática constituye un ataque de acuerdo con el derecho internacional humanitario, independientemente de que el objeto sea inhabilitado por medios cinéticos o cibernéticos[71].

---

[62] CICR, *Documento de posición sobre Derecho internacional humanitario y ciberoperaciones durante conflictos armados* (noviembre de 2019) en 7 ("Documento de posición del CICR").

[63] Incluso en ausencia de ataques, los Estados deben actuar con un "cuidado constante" en un conflicto armado internacional para "preservar a la población civil [...] y a los bienes de carácter civil". Protocolo adicional I, nota 61 *supra*, art. 57.1; *Tallinn 2.0,* nota 20 *supra*, en 476.

[64] Protocolo adicional I, nota 61 *supra*, art. 49.

[65] *Tallinn 2.0*, nota 20 supra en 415.

[66] Véase el Documento de posición del CICR, nota 62.

[67] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* (octubre de 2015) 41 ("Informe del CICR de 2015").

[68] *Tallinn 2.0*, nota 20 supra en 417.

[69] *Id.*

[70] Informe del CICR de 2015, nota 67 *supra*, en 41. Véase también ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (noviembre de 2019), en 28 ("Informe del CICR de 2019") ("Las normas del DIH que protegen los objetos civiles pueden, sin embargo, proporcionar un alcance completo de la protección legal solo si los Estados reconocen que las operaciones cibernéticas que afectan la funcionalidad de la infraestructura civil están sujetas a las normas que rigen los ataques en virtud del DIH ".)

[71] Véanse el Documento de posición del CICR, nota 62 *supra*, en 7-8, y el Informe del CICR en 2015, nota 67 *supra*, en 43 (donde se afirma que el derecho internacional debe tratar como ataques las operaciones cibernéticas que desactiven objetos, ya que la definición de objetivo militar abarca la neutralización, de lo

30. Por consiguiente, la finalidad de la sexta pregunta era determinar si los Estados Miembros también consideran el umbral para un ataque en el contexto del derecho internacional humanitario en términos de violencia (o efectos violentos) o si consideran que la rúbrica de "ataque" podría aplicarse a las operaciones cibernéticas sobre la base de la pérdida de funcionalidad, en vez de los conceptos más tradicionales de daño físico o destrucción.

31. Las respuestas al cuestionario reflejan apoyo a la aplicabilidad del derecho internacional humanitario en general y a la idea de que las operaciones cibernéticas pueden constituir un ataque en ese contexto[72]. Sin embargo, hay más variedad en las respuestas a la pregunta de si una operación cibernética puede calificarse como un "ataque" de conformidad con el derecho internacional humanitario si no causa muertes, lesiones o daños físicos directos. Chile, Perú y Estados Unidos respondieron que no[73]. Chile cita el artículo 49 del Protocolo adicional I a los Convenios de Ginebra al insistir en que los ataques en el contexto del derecho internacional humanitario deben implicar "efectos o consecuencias originados por el acto en sí, los cuales deben ser violentos"[74]. En particular, indica que, para que el acto pueda considerarse como un ataque, su resultado debe requerir que "el Estado afectado debe realizar acciones para reparar o recuperar la infraestructura o sistema informático afectado, debido a que en aquellos casos las consecuencias del ataque son similares a las descritas anteriormente, en particular daños físicos a la propiedad"[75]. Perú responde que, para que haya un "ataque", se deben causar "daños físicos" a "personas" o "bienes públicos o privados"[76]. Estados Unidos, entretanto, ha recalcado que el umbral para un "ataque" en el contexto del derecho internacional humanitario requiere la determinación, entre otras cosas, de si una actividad cibernética produce efectos cinéticos irreversibles o efectos no cinéticos reversibles en la población civil, en objetivos de carácter civil o en la infraestructura civil[77]. Eso implica que, si una operación cibernética produce efectos no cinéticos o reversibles, no constituye un ataque armado[78], lo cual parecería excluir, por ejemplo, los programas intrusos de *ransomware* que no sean cinéticos de por sí o los casos en que los datos que se interrumpan puedan restablecerse.

32. En cambio, Guatemala y Ecuador apoyan la idea de delimitar los ataques sobre la base de las pérdidas de funcionalidad, en vez de las muertes, las lesiones o la destrucción de bienes que puedan causar. Guatemala señala que, entre las operaciones cibernéticas que pueden considerarse como un ataque, se encuentran las "que solo producen una pérdida de funcionalidad"[79]. Ecuador opina que "[u]na operación cibernética puede considerarse un ataque en caso de dejar sin funcionalidad la infraestructura crítica del Estado u otros que pongan en peligro la seguridad del Estado"[80].

---

cual se infiere que la neutralización de objetos está comprendida en el ámbito del derecho internacional humanitario).

[72] Véanse, por ejemplo, respuesta de Bolivia, nota 1 *supra*, en 3 a 7; íd. en 4 a 7 (donde se señalan dos puntos de vista con respecto a si una operación cibernética por sí sola puede dar lugar a un conflicto armado sujeto al derecho internacional humanitario); respuesta de Chile, nota 1 *supra*, en 3; respuesta de Guyana, nota 1 *supra*, en 3; respuesta de Perú, nota 1 *supra*, en 1; Koh, nota 1 *supra*, en 595 (opinión de Estados Unidos).

[73] Respuesta de Guyana, nota 1 *supra*, en 4.

[74] Respuesta de Chile, nota 1 *supra*, en 3.

[75] Íd.

[76] Sin embargo, la respuesta de Perú es un poco ambigua, ya que parece basarse en elementos del *jus ad bellum* para indicar las normas aplicables a un ataque en el contexto del derecho internacional humanitario y menciona el enfoque contextual de Estados Unidos por el cual expresa preferencia Harold Koh. Respuesta de Perú, nota 1 *supra*, en 6.

[77] Escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 736.

[78] Egan, nota 1 *supra*, en 818. Egan no mencionó en su discurso el criterio de daños reversibles o irreversibles, pero recalcó en cambio "la naturaleza y el alcance de esos efectos, así como la índole de la relación, si la hubiere, entre la actividad cibernética y el conflicto armado particular en cuestión". Íd.

[79] Respuesta de Guatemala, nota 1 *supra*, en 3.

[80] Respuesta de Ecuador, nota 1 *supra*, en 3.

33. Las respuestas de Bolivia y Guyana son más ambiguas. Por una parte, Bolivia afirma que la definición de ataques según el derecho internacional humanitario incluiría una operación cibernética "de la cual se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes"[81]. Por otra parte, dice que una operación cibernética "podría ser considerada como un ataque cuando tiene el objetivo de inhabilitar los servicios básicos (agua, luz, telecomunicaciones o el sistema financiero, etc.) de un Estado"[82]. Guyana observa que, cuando una operación cibernética produce una pérdida de funcionalidad, puede o no constituir un ataque[83]. Igual que Chile, hace referencia al artículo 49 del Protocolo adicional I y vincula el concepto de ataque a la necesidad de que haya violencia (en lo que se refiere a los medios o a las consecuencias): "una operación cibernética que no ocasione muertes, lesiones o daños físicos no puede constituir un ataque" de acuerdo con el derecho internacional humanitario[84]. Por otro lado, señala que "las operaciones cibernéticas que socavan el funcionamiento de los sistemas y la infraestructura informáticos necesarios para el suministro de servicios y recursos a la población civil constituyen un ataque". Entre ellos incluye "plantas nucleares, hospitales, bancos y sistemas de control del tráfico aéreo"[85]. Estas respuestas parecen indicar la necesidad de profundizar el diálogo sobre cuán inmediata deber ser la muerte o la destrucción tras la pérdida de funcionalidad. En otras palabras, ¿la pérdida de funcionalidad de un servicio esencial constituye por sí sola un ataque o debe haber muertes, lesiones o daños materiales concomitantes (o razonablemente previsibles)?

Pregunta 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?

34. El derecho internacional humanitario requiere claramente que los Estados "atacantes" hagan una distinción entre objetivos civiles y militares y permite los ataques a objetivos militares, pero prohíbe los ataques contra la población civil y objetivos de carácter civil[86]. Sin embargo, cuando se trata del ciberespacio, no siempre resulta claro qué constituye un "objetivo" al cual se aplica este principio. El debate fundamental se ha centrado en los "datos." ¿Quiere decir que los "datos", por su índole no física, no constituyen un objetivo y que, en consecuencia, los militares no necesitan hacer una distinción y excluirlos de sus operaciones cibernéticas? ¿O por lo menos algunos "datos" deberían considerarse como un "objetivo" al cual se aplica el principio de la distinción y las normas pertinentes del derecho internacional humanitario?

35. La mayoría de los expertos del grupo independiente que redactó el *Tallinn Manual 2.0* adoptaron la primera posición: "no debe entenderse que el concepto de 'objetivo' en el conflicto armado incluye los datos, por lo menos en el derecho actual"[87]. No obstante, los expertos están de acuerdo en que una operación cibernética dirigida contra datos podría desencadenar la aplicación de las normas del derecho internacional humanitario en los casos en que "pueda preverse que ocasione lesiones, muertes, daños materiales o destrucción de objetos físicos", ya que las personas y los objetos afectados estarían protegidos por las reglas pertinentes del derecho internacional humanitario, como las relativas a la distinción[88]. En cambio, el CICR ha propuesto una definición más amplia de datos con la expresión "datos civiles esenciales" (por ejemplo, datos médicos, biométricos y de seguridad social, expedientes tributarios, cuentas bancarias, expedientes de

[81] Respuesta de Bolivia, nota 1 *supra*, en 4 a 7.
[82] Íd.
[83] Respuesta de Guyana, nota 1*supra*, en 3.
[84] Íd.
[85] Íd. (donde se cita el artículo 54.2 del Protocolo adicional I
[86] Cuando un objeto particular se usa para fines civiles y militares (los llamados "objetos de doble uso"), se convierte en un objetivo militar (excepto por las partes que puedan separarse). Véanse fuentes en las cuales se codifica este principio de "distinción" en la nota 61 *supra*.
[87] *Tallinn 2.0*, nota 20 *supra*, en 437.
[88] Íd. en 416.

clientes de empresas, padrones y registros electorales). Ha señalado que "borrar o alterar de manera fraudulenta datos civiles esenciales puede ocasionar más daños a la población civil que la destrucción de objetos físicos"[89]. Aunque el CICR reconoce que la cuestión de si los datos pueden constituir un objetivo civil sigue pendiente, ha indicado que debería resolverse en el ámbito del derecho internacional humanitario. De lo contrario, habrá una gran "brecha en la protección" que es incompatible con el objeto y el propósito del derecho internacional humanitario. Con la séptima pregunta se trató de recabar la opinión de los Estados Miembros sobre este importante asunto.

36. Ninguno de los Estados que respondieron a esta pregunta adoptó la posición de que los datos civiles estén sujetos directamente al principio de distinción en el conflicto armado. De hecho, varios Estados mencionan el principio de distinción sin formular una opinión sobre la condición de los datos como objeto[90]. Sin embargo, la respuesta de Chile parece indicar que el principio de distinción podría aplicarse a las operaciones cibernéticas dirigidas contra datos indirectamente sobre la base de sus repercusiones. Cita el comentario del Protocolo adicional I de que un objeto debe ser "visible y tangible", lo cual significa que, "bajo el derecho internacional humanitario vigente, los mencionados datos no calificarían como objetos, en principio, por ser esencialmente intangibles, sin perjuicio de los elementos físicos en los cuáles se encuentran contenidos los datos, por ejemplo hardware"[91]. Al mismo tiempo, Chile señala que "un ataque dirigido exclusivamente en contra de datos informáticos podría perfectamente generar consecuencias adversas que afecten a la población civil". Da como ejemplo la posibilidad de una operación cibernética que elimine la base de datos de seguridad social de un Estado[92] y concluye que "el principio de distinción debe ser tenido en consideración en el contexto de las operaciones cibernéticas, por lo cual un Estado debiera abstenerse de atacar datos en caso de que esto pudiese afectar a la población civil, a menos que dichos datos estuvieran siendo usados para propósitos militares"[93]. Guyana responde con una óptica similar. Tras señalar que borrar, suprimir o corromper datos podría tener consecuencias de gran alcance, se centra en los efectos de la operación cibernética, en vez de abordar la cuestión de si los datos que sean el objetivo del ataque pueden considerarse como un objeto o no[94].

37. En su respuesta, Perú no aborda la posibilidad de que los datos puedan considerarse como un objetivo civil, sino que se centra (de manera afirmativa) en la posibilidad de que puedan considerarse como un objetivo militar. Señala que ciertos "datos" (por ejemplo, "un software que permita la comunicación entre las tropas de un ejército en campaña o sincronice el arsenal de misiles de un país o ayude a localizar una aeronave enemiga") son objetivos militares legítimos,

---

[89] CICR, Documento de posición, nota 62 *supra*, en 8; Informe del CICR de 2019, nota 71 *supra*, en 21 (Además, los datos se han convertido en un componente esencial del dominio digital y una piedra angular de la vida en muchas sociedades. Sin embargo, existen diferentes puntos de vista sobre si los datos civiles deben considerarse como objetos civiles y, por lo tanto, si deben protegerse bajo los principios y normas del DIH que rigen la conducción de las hostilidades. En la opinión del CICR, la conclusión de que este tipo de operación no estaría prohibido por el DIH en el mundo de hoy, cada vez más dependiente de la esfera cibernética –sea porque eliminar o alterar esos datos no constituiría un ataque en el sentido del DIH o porque esos datos no se considerarían objetos respecto de los cuales se aplicaría la prohibición de ataques contra bienes de carácter civil- parece difícil de conciliar con el objetivo y el propósito de este ordenamiento jurídico. En pocas palabras, el reemplazo de archivos en papel y documentos con archivos digitales en forma de datos no debería disminuir la protección que el DIH les brinda"); Informe del CICR en 2015, nota 67 *supra*, en 43.

[90] Véanse la respuesta de Bolivia, nota 1 *supra*, en 5 a 7; la respuesta de Ecuador, nota 1 *supra*, en 2, y la respuesta de Guatemala, nota 1 *supra*, en 3.

[91] Respuesta de Chile, nota 1 *supra*, en 4.

[92] Íd.

[93] Íd.

[94] Respuesta de Guyana, nota 1 *supra*, en 4 (donde dice que, en lo que se refiere a los datos, hay que tener en cuenta si la operación cibernética dirigida contra los datos ha producido una pérdida tal de funcionalidad que pueda constituir un ataque).

mientras que otros sistemas de datos utilizados en conflictos (por ejemplo, "un sistema de datos que permita el funcionamiento de la sala de operaciones de un hospital de campaña en el que se atiende a heridos de guerra o a población civil") no pueden ser el blanco de ataques[95].

38. Varios comentarios de Estados Miembros al Grupo de Trabajo de Composición Abierta afirmaron la importancia de aplicar el derecho internacional humanitario al contexto cibernético. Algunos Estados, como Brasil, subrayaron, además, que esta aplicación debe incluir expresamente los principios fundamentales de "humanidad, necesidad, proporcionalidad y distinción". [96] Sin embargo, ninguna de las contribuciones del Grupo de Trabajo de Composición Abierta abordó la definición de un ataque ni la idea de los datos como objetivo civil (o militar).

Pregunta 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?

39. La soberanía es sin lugar a dudas la característica estructural básica del ordenamiento jurídico internacional actual, que asigna derechos y responsabilidades a los Estados[97]. Es un principio fundacional de algunas de las normas jurídicas internacionales mencionadas (por ejemplo, la prohibición del uso de la fuerza, el derecho de legítima defensa, la responsabilidad del Estado). Asimismo, en ciertos contextos, la soberanía existe no solamente como un principio básico, sino como una norma independiente que regula el comportamiento del Estado (por ejemplo, una aeronave que penetra el espacio aéreo de otro Estado sin autorización viola su soberanía)[98]. Sin embargo, todavía no resulta claro si la soberanía tiene calidad de norma en el ciberespacio. En el *Tallinn Manual 2.0* se señala que es una regla que limita las operaciones cibernéticas de un Estado

---

[95] Respuesta de Perú, nota 1 *supra*, en 6. Perú explica que, en el primer caso, los ataques causarían "un daño militar significativo a las fuerzas de la contraparte", mientras que un ataque contra los datos en el hospital de campaña "no generaría una ventaja militar legítima". Íd.

[96] Comentarios de Brasil, *supra,* nota 5

[97] *Island of Palmas (Netherlands v. United States of America)*, 2 R.I.A.A. 829, 839 (1928) ("La soberanía en las relaciones entre Estados significa independencia. La independencia con respecto a la porción del mundo que ocupan es el derecho a ejercer dentro de ella, con exclusión de cualquier otro Estado, las funciones de un Estado [...]. La soberanía territorial, como ya se dijo, implica el derecho exclusivo a realizar las actividades de un Estado. Este derecho tiene como corolario un deber: la obligación de proteger, dentro del territorio, los derechos de otros Estados, en particular su derecho a la integridad y la inviolabilidad en tiempos de paz y de guerra" [traducción del CJI]).

[98] Véase, por ejemplo, Michael N. Schmitt y Liis Vihul, *Respect for Sovereignty in Cyberspace,* 95 en *Texas L. Rev.* 1639, 1640 (2017). Además de la prohibición del uso de la fuerza enunciada en el artículo 2.4, en el derecho internacional hay amplio acuerdo sobre el deber de no intervención que se aplica al ciberespacio. Véanse, por ejemplo, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Jurisdicción y Admisibilidad) [2006] ICJ Rep. 6, [46]-[48]; *Nicaragua Case*, nota 23 *supra*, párr. 205; Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas, de 24 de octubre de 1970, que contiene la Declaración relativa a los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas. El GEG de 2015 refrendó este principio entre las normas del derecho internacional que se aplican al ciberespacio. 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/70/174 (22 de julio de 2015) párrafos. 26 y 28.b. La regla 66 del manual *Tallinn 2.0* postula que "un Estado no puede intervenir, incluso por medios cibernéticos, en los asuntos internos o externos de otro Estado". *Tallinn 2.0,* nota 20 *supra*, en 312 (traducción del CJI). Sin embargo, igual que ocurre con el uso de la fuerza, subsisten dudas con respecto a si este deber existe en el espacio cibernético y qué operaciones cibernéticas prohíbe o reglamenta.

que no dan lugar al uso de la fuerza ni constituyen una intervención prohibida[99]. No obstante, en 2018, el Fiscal General del Reino Unido opinó que la soberanía no era una norma de derecho internacional en sí, sino un principio que servía de base para otras normas[100]. Posteriormente, el Ministerio de Defensa de Francia y el Gobierno de Holanda han expresado apoyo a la soberanía como norma autónoma[101].

40. La finalidad de la octava pregunta era recabar las opiniones de los Estados Miembros sobre la cuestión de la soberanía como principio en contraposición a la soberanía como norma. La pregunta se centra en la función limitante de la soberanía, es decir, si limita la capacidad de un Estado para realizar operaciones cibernéticas fuera de su territorio y de qué forma. Lo interesante es que muchos de los Estados que respondieron tomaron la pregunta como una invitación para reafirmar la función habilitadora de la soberanía; por ejemplo, de acuerdo con la autoridad del Estado para reglamentar las TIC dentro de su propia jurisdicción territorial. Bolivia y Guyana dicen que la soberanía autoriza a los Estados a ejercer jurisdicción sobre la infraestructura o las actividades cibernéticas en su territorio[102]. Ecuador, en cambio, arroja dudas sobre la capacidad de los Estados para ejercer su soberanía en el ciberespacio en vista de su "intangibilidad" y, al mismo tiempo, afirma que los Estados tienen soberanía sobre la "infraestructura cibernética" y las actividades relacionadas con dicha infraestructura en su territorio[103]. Chile y Estados Unidos también se hacen eco del poder que la soberanía confiere a los Estados sobre las TIC en su

---

[99] *Tallinn 2.0,* nota 20 *supra*, regla 4 ("Un Estado no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado" [traducción del CJI]).

[100] Véase, por ejemplo, Jeremy Wright, QC, MP. *Cyber and International Law in the 21st Century* (23 de mayo de 2018) en https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("las opiniones del Reino Unido"). ("Algunos han tratado de demostrar la existencia de una norma orientada específicamente al espacio cibernético que se aplica a la 'violación de la soberanía territorial' [...]. Por supuesto, la soberanía es fundamental para el sistema internacional basado en normas, pero no estoy convencido de que en la actualidad podamos extrapolar de ese principio general una norma específica o una prohibición de actividades cibernéticas además de una intervención prohibida. Por lo tanto, la posición del Gobierno del Reino Unido es que no hay una norma de ese tipo en el derecho internacional vigente".

[101] Véase Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (9 de septiembre de 2019), en: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("Opinión del Ministerio de Defensa de Francia") en 6 ("Toda penetración no autorizada de sistemas franceses por un Estado o todo acto que surta efectos en el territorio francés por medio de un vector digital podría constituir, como mínimo, una violación de la soberanía" [traducción al inglés del Relator]); *Letter to the parliament on the international legal order in cyberspace,* 5 de julio de 2019, apéndice 1 en https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("Opinión de los Países Bajos") ("Según algunos países y juristas, el principio de soberanía no constituye una norma independientemente vinculante del derecho internacional que la separa de las demás normas derivadas del mismo. Los Países Bajos no están de acuerdo con este punto de vista, ya que creen que el respeto de la soberanía de otros países es una obligación por sí misma, cuya violación podría a su vez constituir un acto internacionalmente ilícito" [traducción del CJI]). En un análisis académico reciente se cuestiona si Francia se encuadra claramente en el bando de la soberanía como norma. Véase Gary Corn, *Punching on the Edges of the Gray Zone: Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (11 de febrero de 2020) ("aunque el Ministerio de Defensa afirma que los ciberataques, tal como define el término, contra sistemas digitales franceses o todo efecto producido en territorio francés por medios digitales podrían constituir una violación de la soberanía en sentido general, en ningún momento dice sin lugar a dudas que una violación del principio de soberanía constituye un incumplimiento de una obligación internacional. Por el contrario, los autores del documento, obviamente conscientes del debate, son deliberadamente vagos al respecto y reafirman simplemente el derecho de Francia a responder a los ciberataques con la gama completa de opciones que tenga a su alcance de acuerdo con el derecho internacional")

[102] Respuesta de Bolivia, nota 1 *supra*, en 5 a 7; respuesta de Guyana, nota 1*supra*, en 5.

[103] Respuesta de Ecuador, nota 1 *supra*, en 2.

territorio, pero observan que ese poder debe actuar dentro de ciertos límites. Ambos señalan la necesidad de que los Estados ejerzan la soberanía de conformidad con el derecho internacional de los derechos humanos[104]. Colombia respaldó este último punto en sus comentarios al Grupo de Trabajo de Composición Abierta.[105]

41. Con respecto a la pregunta de si la soberanía opera como norma autónoma en el ciberespacio, tres Estados —Bolivia, Guatemala y Guyana— respondieron que sí[106]. Guyana, por ejemplo, afirma que las protecciones de la soberanía "no se limitan a las actividades que representen un uso injustificado de la fuerza, un ataque armado o una intervención prohibida"[107]. Opina que el Estado "no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado", y la existencia de una violación de ese tipo depende "del grado de infracción y de si ha habido interferencia en las funciones del gobierno"[108]. Guatemala adopta una posición similar y señala que "un Estado que participa en operaciones cibernéticas específicas viola la soberanía de un país si al momento de realizar un ataque cibernético se capta cierta información en el ciberentorno de otro Estado, aun cuando no causare ningún daño que repercuta en algún equipo o en los derechos humanos de alguna o algunas personas"[109].

42. Las respuestas de otros Estados son bastante ambiguas. Perú dice simplemente que la soberanía "es uno de los pilares fundamentales de la sociedad internacional", sin opinar sobre su condición de norma independiente[110]. Ecuador indica que la "norma" que autoriza a los Estados a controlar su propia infraestructura cibernética "no prohíbe a un Estado [...] participar en operaciones cibernéticas", pero no opina sobre si podría reglamentar la forma en que lo hace en relación con otros Estados soberanos[111].

43. En su respuesta, Chile describe la soberanía como un principio que "[l]os Estados que llevan a cabo operaciones cibernéticas deben siempre tener en cuenta"[112]. Por lo tanto, "cada vez que un Estado contempla realizar una operación cibernética, debe tener en consideración no afectar la soberanía de otro"[113]. La referencia a un "principio" orientador puede sugerir algo diferente de una regla concreta, aunque el uso del verbo "deben" crea expectativas con un carácter más obligatoria. Por otro lado, Chile afirma lo siguiente:

> cada Estado está obligado a respetar la integridad territorial e independencia política de otros Estados y debe cumplir fielmente con sus obligaciones internacionales, incluyendo el principio de no intervención. Por ende, las operaciones

---

[104] Respuesta de Chile, nota 1 *supra*, en 4 y 5 (donde reconoce que la soberanía autoriza al Estado a proteger y defender "su infraestructura crítica de la información, [...] siempre y cuando estas medidas no vayan en contra de una norma de derecho internacional, como por ejemplo aquellas presentes en el derecho internacional de los derechos humanos o el derecho internacional humanitario"); escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 737 a 738 (donde se señala que el ejercicio de la jurisdicción de un Estado territorial no es ilimitado, sino que debe concordar con el derecho internacional aplicable, incluidas las obligaciones internacionales en materia de derechos humanos, y se mencionan en particular la libertad de expresión y la libertad de opinión).

[105] Comentarios de Colombia, nota 5 *supra.*

[106] Respuesta de Bolivia, nota 1 *supra*, en 5 a 7; respuesta de Guatemala, nota 1 *supra*, en 3; respuesta de Guyana, nota 1 *supra*, en 5.

[107] Respuesta de Guyana, nota 23 *supra*, en 5

[108] Íd.

[109] Respuesta de Guatemala, nota 1 *supra*, en 3.

[110] Respuesta de Perú, nota 1 *supra*, en 6 y 7.

[111] Respuesta de Ecuador, nota 1 *supra*, en 2.

[112] Respuesta de Chile, nota 1 *supra*, en 5.

[113] Íd.

cibernéticas que impiden el ejercicio de soberanía por parte de otro Estado constituyen una violación de dicha soberanía y están prohibidas por el derecho internacional[114].

La última oración parece indicar que la soberanía podría constituir una norma autónoma salvo que la referencia a la intervención en el ejercicio de la soberanía de otro Estado se entienda como el equivalente del *domaine reservé* protegido por el deber de no intervención[115].

44. La posición de Estados Unidos es menos clara aún. En 2014, el entonces asesor jurídico Harold Koh afirmó que "la soberanía del Estado [...] debe tenerse en cuenta en la realización de actividades en el ciberespacio, incluso fuera del contexto del conflicto armado"[116]. Sin embargo, no resulta claro si tener en cuenta la soberanía del Estado indica el reconocimiento por Estados Unidos de la soberanía como norma autónoma. En su discurso de 2016, el entonces asesor jurídico Brian Egan dejó en claro que "las operaciones cibernéticas remotas con computadoras u otros dispositivos en red situados en el territorio de otro Estado no constituyen de por sí una violación del derecho internacional"[117]. Al mismo tiempo, admitió que, "en ciertas circunstancias, las operaciones cibernéticas no consensuales de un Estado en el territorio de otro podrían violar el derecho internacional, incluso si no llegan al umbral para el uso de la fuerza". De todas maneras, Egan indicó que "el momento preciso en que una operación cibernética no consensual viola la soberanía de otro Estado es una cuestión que los abogados del Gobierno de Estados Unidos siguen estudiando minuciosamente y, en última instancia, se resolverá por medio de la práctica y la *opinio juris*"[118]. Sin embargo, más recientemente, el Asesor Jurídico del Departamento de Defensa de los Estados Unidos indicó que "en relación a las operaciones cibernéticas que no constituirían una intervención prohibida o uso de la fuerza [es decir, aquellas que podrían estar cubiertas por una regla de soberanía], el Departamento cree que no existe una práctica estatal suficientemente extendida y consistente como resultado de un sentido de obligación legal de concluir que el derecho internacional consuetudinario generalmente prohíbe tales operaciones cibernéticas no consensuales en el territorio de otro Estado[119].

45. En un debate entre 16 representantes de Estados Miembros celebrado de acuerdo a las "Reglas de Chatham House" [120] el 23 de junio de 2020, se reforzó la actual diversidad de opiniones sobre la cuestión de la soberanía. Varios participantes solicitaron que se afirmara la opinión de la soberanía como norma para el espacio cibernético, con lo cual la violación de la misma conllevaría una responsabilidad jurídica internacional. Otros, sin embargo, expresaron mayor escepticismo con respecto al valor de dicha labor; un participante sugirió que podrían existir muchos significados del término "soberanía" para atribuirle el rango de regla. Otro participante consideró que la "el debate

---

[114] Íd.

[115] Véase la nota 99.

[116] Koh, nota 1 *supra*, en 596 (traducción del CJI); escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 737; escrito presentado por Estados Unidos al GEG en 2016, nota 1 *supra*, en 825.

[117] Egan, *supra* note 1, en 818 (traducción del CJI). Entre otras cosas, Egan dijo que Estados Unidos recopilaba inteligencia en el exterior y que esas actividades podrían violar las leyes internas de otros Estados, pero no estaban prohibidas de por sí en el derecho internacional consuetudinario. Íd.

[118] Íd. en 819

[119] *Véase* Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 de marzo, 2020, en, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference. Sin embargo, no queda claro si Ney estaba expresando la opinión de los Estados Unidos en su totalidad o si se trataba solamente de la posición de los militares estadounidenses, una ambigüedad que existe también con respecto a las opiniones del Ministerio de Defensa de Francia. Véase nota 101 *supra*.

[120] Chatham House, *La Regla de Chatham House:* https://www.chathamhouse.org/chatham-house-rule (Cuando una reunión, o una parte de la reunión, se convoca bajo la Regla de Chatham House, los participantes tienen derecho a utilizar la información que reciben, pero no pueden revelar la identidad ni la afiliación del orador, ni de ningún otro participante.)

sobre soberanía es una distracción", y un tercer participante sugirió explícitamente la necesidad de replantearse su significado en el contexto cibernético.

Pregunta 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?

46. La diligencia debida es un principio del derecho internacional según el cual un Estado debe responder a las actividades que sepa (o que razonablemente deba saber) que se han originado en su territorio o en otras zonas bajo su control y que violan los derechos de otro Estado[121]. Es una obligación de esfuerzo y no de resultado: en los casos en que un Estado tenga conocimiento de la conducta o deba tenerlo, debe emplear "todos los medios que estén razonablemente a su alcance" para corregirla[122]. Como principio, la diligencia debida regula actualmente el comportamiento del Estado en varios contextos, en particular el derecho ambiental internacional, donde constituye la base del requisito de que los Estados frenen en su territorio la contaminación que sea una fuente de daños transfronterizos para el territorio de otros Estados.

47. Igual que en el caso de la soberanía, hay opiniones contrarias sobre si la diligencia debida es un requisito del derecho internacional en el ciberespacio. En el informe del GEG de 2015 se la menciona entre las normas "voluntarias" del comportamiento responsable de los Estados, en vez de incluirla en los principios aplicables del derecho internacional[123]. Los Ministerios de Defensa de los Países Bajos y de Francia la han descrito como una norma jurídica que se aplica al ciberespacio[124]. Sin embargo, los Países Bajos observan que no todos los países están de acuerdo en que el principio de la diligencia debida constituye una obligación en sí en el marco del derecho internacional, y se cree que Estados Unidos es uno de los países que ponen en tela de juicio esa condición[125]. Por lo tanto, con la novena pregunta se trató de recabar la opinión de los Estados Miembros sobre la condición de la diligencia debida con respecto a las obligaciones de un Estado de conformidad con el derecho internacional en el ciberespacio.

48. Chile, Ecuador, Guatemala, Guyana y Perú adoptan la posición de que el principio de la diligencia debida forma parte del derecho internacional que los Estados deben aplicar en el

---

[121] Véanse, por ejemplo, *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)* [1949] ICJ Rep., párr. 22 (9 de abril); *Trail Smelter Case (United States-Canada)*, UNRIAA, vol. III, 1905 (1938, 1941).

[122] Véase *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia v. Serbia)* (Judgment) [2007] ICJ Rep. 1, párr. 430.

[123] GEG de 2015, nota 1 *supra*, párrs. 13 y 26 a 28.

[124] Opinión del Ministerio de Defensa de Francia, nota 101 *supra*, en 10 ("De acuerdo con la obligación de actuar con la debida diligencia, los Estados deben asegurar que su ámbito soberano en el ciberespacio no se use para cometer actos internacionalmente ilícitos. Si un Estado no cumple esta obligación, eso no es motivo para una excepción a la prohibición del uso de la fuerza, contrariamente a la opinión de la mayoría de los integrantes del grupo de expertos que redactaron el Manual de Tallinn"; opinión de los Países Bajos, nota 101 *supra*, apéndice, en 4 ("el principio de la debida diligencia requiere que los Estados tomen medidas con respecto a las actividades cibernéticas realizadas por personas en su territorio o para las cuales se usen redes que se encuentren en su territorio o bajo su control, que violen un derecho de otro Estado y de cuya existencia tengan conocimiento o deban tenerlo" [traducción del CJI]). Estonia, aunque no describe la debida diligencia como norma específica del derecho internacional, ha catalogado su contenido como requisito para el comportamiento del Estado. Kersti Kaljulaid, Presidente de Estonia, President *of the Republic at the opening of CyCon 2019* (mayo de 2019), en: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("Las opinión de Estonia)("los Estados tienen que hacer un esfuerzo razonable para asegurar que su territorio no se use con el fin de perjudicar los derechos de otros Estados. Deben buscar medios para ofrecer apoyo cuando el Estado lesionado lo solicite para identificar, atribuir o investigar operaciones cibernéticas maliciosas. Esta expectativa depende de la capacidad nacional, la disponibilidad de información y su accesibilidad" [traducción del CJI]).

[125] Opinión de los Países Bajos, nota 101 *supra*, apéndice, en 4.

ciberespacio[126]. Como explica Chile, "desde el punto de vista de las operaciones cibernéticas, un Estado debe ejercer la debida diligencia para no permitir que su territorio soberano, incluida la infraestructura cibernética bajo su control, sea utilizado para llevar a cabo operaciones cibernéticas que afecten los derechos o pudieran producir consecuencias adversas sobre otro Estado"[127]. Guatemala adopta una posición similar y agrega que, como "ciberespacio" es un término muy amplio, actuar con la diligencia debida puede ser sumamente complicado[128]. Aun así, en la medida en que la diligencia debida "deriva del principio de soberanía", Guatemala opina que "cada Estado debe tener el control para detener la actividad nociva que se produce desde su territorio, obligándose a tomar medidas preventivas, estableciendo un CERT, adoptar políticas de seguridad de la información, y elevar la conciencia sobre seguridad de la información"[129].

49. La respuesta de Bolivia es más ambigua. Sin referirse a la condición jurídica de la diligencia debida, opina que no se puede responsabilizar a un Estado por un ataque cibernético si no tiene la infraestructura tecnológica necesaria para controlar a un agente no estatal[130]. Esta opinión podría ser compatible con el principio de la diligencia debida como norma jurídica internacional para las operaciones cibernéticas, ya que, por lo general, requiere que los Estados "tengan conocimiento" de las actividades en cuestión, lo cual no sería posible en el caso de los Estados que no tengan la infraestructura técnica necesaria[131]. Por otro lado, la imposibilidad de "controlar" actividades cibernéticas de las cuales se tenga conocimiento podría indicar que Bolivia no se adhiere a la doctrina de la diligencia debida en el ciberespacio. Sin una aclaración de la respuesta, es difícil llegar a una conclusión. Asimismo, en las declaraciones públicas anteriores de Estados Unidos no se abordó la condición jurídica de la diligencia debida de forma directa. Cabe señalar, no obstante, que Estados Unidos ha tendido a describir toda obligación de responder a solicitudes de asistencia en términos no vinculantes[132]. El hecho de que Estados Unidos no haya refrendado públicamente el principio de la diligencia debida como norma jurídica en el GEG ni en otros contextos podría indicar dudas con respecto a la condición jurídica de este principio.

50. En el debate de Chatham House de junio de 2020, varios Estados Miembros expresaron su apoyo a la debida diligencia como una norma (importante) del derecho internacional en el contexto cibernético. Sin embargo, un representante de un Estado Miembro expresó dudas con respecto al respaldo de la debida diligencia, dado el riesgo de incumplimiento que podría ocurrir para los Estados que no pueden responder adecuadamente a los ataques cibernéticos por falta de capacidad técnica.

Pregunta 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?

51. En la décima y última pregunta se pidió a los Estados que indicaran otras áreas del derecho internacional en las cuales el Comité debería concentrarse para mejorar la transparencia en el contexto cibernético. En las respuestas se abordan distintos asuntos. Bolivia pide que se preste

---

[126] Respuesta de Chile, nota 1 *supra*, en 6 y 7; respuesta de Ecuador, nota 1*supra*, en 2; respuesta de Guatemala, nota 1 *supra*, en 4; respuesta de Guyana, nota 1 *supra*, en 5; respuesta de Perú, nota 1 *supra*, en 7.

[127] Respuesta de Chile, nota 1 *supra*, en 6 y 7. Ecuador dijo simplemente que "la diligencia debida es aplicable a lo que sucede en los recursos tecnológicos dentro de su territorio nacional". Respuesta de Ecuador, nota 1 *supra*, en 2.

[128] Respuesta de Guatemala, nota 1 *supra*, en 4.

[129] Íd. en 2 y 4.

[130] Respuesta de Bolivia, nota 1 *supra*, en 3 a 7.

[131] Véase *Tallinn 2.0*, nota 20 *supra*, en 40.

[132] Escrito presentado por Estados Unidos al GEG en 2014, nota 1 *supra*, en 739 ("Un Estado *debería* cooperar, de una manera acorde con el derecho interno y las obligaciones internacionales, con los pedidos de asistencia de otros Estados para investigar delitos cibernéticos, obtener pruebas electrónicas y mitigar las actividades cibernéticas maliciosas en su territorio".

más atención a la protección de los "derechos fundamentales de sus ciudadanos en cualquier dimensión en la que actúen", incluso en el ciberespacio[133]. Algunas respuestas se centran en la ciberdelincuencia y, en particular, el Convenio de Budapest, elaborado por el Consejo de Europa[134]; otras destacan la contribución de los Manuales de Tallinn[135].

52. Dos Estados —Ecuador y Guyana— indican que podría ser necesario un nuevo derecho internacional en el contexto cibernético. Ecuador recalca la necesidad de establecer la forma de regular "los ataques a objetivos militares y/o civiles que afecten masivamente a la población, como es el caso de la infraestructura crítica, los hospitales, medios de transporte masivo y otra infraestructura que afecte a la seguridad del Estado"[136]. Guyana dice que sería prudente contar con un conjunto de principios del derecho internacional adaptados a la índole especial del ciberespacio y observa que los principios jurídicos actuales fueron elaborados para una época y un contexto diferente[137].

53. En las consultas de Chatham House de junio de 2020, varios Estados Miembros solicitaron que se preste mayor atención al principio de no injerencia (y al tema de qué actividades cibernéticas constituyen coerción). Varios participantes se hicieron eco del llamado para prestar mayor atención a los temas jurídicos "por debajo" del umbral del uso de fuerza establecido por la prohibición del artículo 2 (4) de la Carta de las Naciones Unidas. Otros sugirieron menor atención a los temas de paz y seguridad internacional en favor de una mayor atención a la aplicación del derecho internacional de los derechos humanos al espacio cibernético. Otros temas que recibieron atención fueron el derecho diplomático, el principio de buena fe, las contramedidas y los estándares de prueba para la atribución de operaciones cibernéticas a un Estado.

54. Por último, al menos un participante solicitó que se desarrollara una perspectiva latinoamericana sobre la gobernabilidad internacional y el marco jurídico del espacio cibernético. El participante señaló que mayoría de las ideas sobre derecho internacional en el espacio cibernético fueron elaboradas por los Estados europeos o por especialistas del Norte Global. En lugar de duplicar los esfuerzos existentes (por ejemplo, GEG de Naciones Unidas, Grupo de Trabajo de Composición Abierta de Naciones Unidas, etc.), los países de América Latina podrían basarse en estos principios para elaborar un marco latinoamericano a fin de entender el derecho internacional en el espacio cibernético, basándose en una cultura política común de instituciones democráticas e historia iberoamericana. La OEA fue citada como el lugar ideal para coordinar dicha visión conjunta.

---

[133] Respuesta de Bolivia, nota 1 *supra*, en 6 y 7.
[134] Respuesta de Guatemala, nota 1 *supra*, en 4; respuesta de Bolivia, nota 1 *supra*, en 6 y 7.
[135] Respuesta de Costa Rica, nota 1 *supra*, en 2 (donde se expresa el interés de Costa Rica en adherirse al Convenio de Budapest); respuesta de Guatemala, nota 1 *supra*, en 4 (donde se cita el Convenio de Budapest).
[136] Respuesta de Ecuador, nota 1 *supra*, en 3.
[137] Respuesta de Guyana, nota 1 *supra*, en 5 y 6 (donde se indica que el anonimato es una dificultad particular para la aplicación del derecho actual).