96º PERÍODO ORDINARIO DE SESIONES
2 – 6 marzo de 2020
Rio de Janeiro, Brasil

OEA/Ser. Q
CJI/doc. 603/20 rev.1 corr.1
5 marzo 2020
Original: inglés
* Limitado

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

CUARTO INFORME

(Presentado por el profesor Duncan B. Hollis)

1. Este es mi cuarto informe sobre la mejora de la transparencia en la forma en que los Estados Miembros entienden la aplicación del derecho internacional a las operaciones cibernéticas del Estado. Presenta un análisis de las respuestas recibidas hasta la fecha al cuestionario del Comité Jurídico Interamericano (CJI) dirigido a los Estados Miembros sobre el derecho internacional y las operaciones cibernéticas del Estado. De esta forma, el informe procura contribuir a una amplia tendencia en las relaciones internacionales hacia una mayor transparencia en la forma en que los Estados nación entienden la aplicación del derecho internacional al ciberespacio.

2. En mi primer informe puse de relieve la poca visibilidad que el derecho internacional ha tenido en la reglamentación de las operaciones cibernéticas del Estado, a pesar de su proliferación y de sus implicaciones económicas, humanitarias y para la seguridad nacional[1]. Muchos Estados *han* confirmado la aplicabilidad del derecho internacional a su comportamiento en el ciberespacio[2]. Aunque la OEA no lo ha hecho, otras organizaciones internacionales, como la ASEAN, la Unión Europea y las Naciones Unidas, también lo han hecho[3]. No obstante, los intentos realizados hasta la fecha de delinear *la forma* en que los Estados entienden la aplicación del derecho internacional al ciberespacio han tenido poco éxito.

3. Como señalé en mi segundo informe, sigue habiendo controversias y confusión con respecto a si ciertos regímenes jurídicos internacionales —entre ellos la autodefensa, el derecho internacional humanitario, las contramedidas, la soberanía (como norma autónoma) y la diligencia debida— se aplican a las operaciones cibernéticas[4]. Lo que es más importante, los Estados se muestran renuentes a invocar el derecho internacional al formular acusaciones con respecto a las operaciones cibernéticas de otros

---

[1] Véase Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser. Q, CJI/doc. 570/18 (9 de agosto de 2018) ("primer informe de Hollis").

[2] Véanse Naciones Unidas, Nota del Secretario General, *Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, párr. 19, A/68/98 (24 de junio de 2013) ("El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable" al ciberespacio); Nota del Secretario General, *Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, párr. 24, A/70/174 (22 de julio de 2015) (ídem).

[3] Véanse la resolución 266 de la Asamblea General de las Naciones Unidas, A/RES/73/266 (2 de enero de 2019); *ASEAN-United States Leaders' Statement on Cybersecurity Cooperation* (18 de noviembre de 2018); *EU Statement – United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security* (26 de octubre de 2018). Tanto el G7 como el G20 han hecho declaraciones similares. Véanse, por ejemplo, *G7 Declaration on Responsible States Behavior in Cyberspace* (Luca, 11 de abril de 2017); *Comunicado de los dirigentes del G-20, Cumbre de Antalya*, 15 y 16 de noviembre de 2015, párr. 26.

[4] Duncan B. Hollis. *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc. 578/19 (21 de enero de 2019) ("segundo informe de Hollis").

Estados[5]. En una notable excepción, en 2018, cinco Estados (Australia, Canadá, los Países Bajos, Nueva Zelandia y el Reino Unido) acusaron al Servicio de Información Militar (GRU) —la rama de inteligencia militar de Rusia— de una serie de operaciones cibernéticas, entre ellas algunas contra la Organización para la Prohibición de las Armas Químicas (OPAQ) y la Agencia Mundial Antidopaje (AMA). El Secretario de Relaciones Exteriores del Reino Unido señaló que Rusia quería operar sin respetar el derecho internacional ni las normas establecidas, en tanto que los Países Bajos afirmaron, en términos más generales, que las actividades rusas socavaban el estado de derecho internacional[6]. Desafortunadamente, en estas acusaciones no se indicó si todas las presuntas operaciones del GRU o solo algunas violaban el derecho internacional ni se especificaron las normas del derecho internacional que los acusadores creían que se habían infringido.

4. En años recientes, varios Estados han comenzado a ofrecer *algunas* explicaciones de la forma en que se aplica el derecho internacional al ciberespacio. A partir de 2012, Estados Unidos comenzó a expresar sus opiniones en discursos y declaraciones[7]. En 2018, el Ministerio Público del Reino Unido hizo una importante declaración acerca de las opiniones del país[8]. Posteriormente, varios

---

[5] Véanse Dan Efrony y Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-Operations and Subsequent State Practice,* 112 AJIL 583, 594 (2018); Duncan B. Hollis y Martha Finnemore, *Beyond Naming and Shaming: Accusations and International Law in Global Cybersecurity,* en *Euro. J. Int'l L.* (se publicará en 2020).

[6] Foreign Commonwealth Office, Press Release, *UK exposes Russian cyber-attacks* (4 de octubre de 2018); NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (4 de octubre de 2018); Netherlands Ministry of Defense, *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW* (4 de octubre de 2018).
La acusación de Canadá contenía ambas formulaciones. Press Release, Global Affairs Canada, *Canada Identifies Malicious Cyber-Activity by Russia* (4 de octubre de 2018) (donde se señala que la actividad de Rusia demuestra un desconocimiento del derecho internacional y socava el orden internacional basado en normas). En cambio, Australia y Nueva Zelandia acusaron a Rusia de llevar a cabo una actividad cibernética maliciosa, sin hacer referencia alguna al derecho internacional. Véanse, por ejemplo, Press Release, Government Communications Security Bureau, *Malicious Cyber Activity Attributed to Russia* (4 de octubre de 2018); Media Release, Prime Minister of Australia, *Attribution of a Pattern of Malicious Cyber Activity to Russia* (4 de octubre de 2018).

[7] Véanse, por ejemplo, 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).

[8] Jeremy Wright, QC, MP. *Cyber and International Law in the 21st Century* (23 de mayo de 2018) ("las opiniones del Reino Unido").

Estados —entre ellos Australia[9], Estonia[10], Francia[11] y los Países Bajos[12]— comenzaron a presentar sus propios puntos de vista de manera pormenorizada. Aunque se trata de un avance, el número y la especificidad de estas declaraciones (todavía) no han sido suficientes para usarlas como evidencia en la práctica general de los Estados o la *opinio juris*[13].

5. Varios agentes no estatales han tratado de suplir esta falta de información con sus propias opiniones sobre la manera en que el derecho internacional consuetudinario regula las operaciones cibernéticas del Estado. Las dos voces más prominentes son, sin lugar a dudas, las del Comité Internacional de la Cruz Roja (CICR) y el grupo independiente de expertos que escribió los manuales de Tallin[14]. No obstante, es evidente que no todos los Estados consideran que su contenido refleja el derecho internacional[15].

6. Con el apoyo del Comité, en mi segundo informe detallé un plan para abordar la *transparencia* con respecto a la forma en que los Estados entienden la aplicación del derecho internacional a las operaciones cibernéticas. Específicamente, propuse distribuir un cuestionario a los Estados Miembros de la OEA sobre algunas de las cuestiones jurídicas internacionales más pertinentes, y el Comité lo aprobó. El proyecto tiene tres objetivos:

a. Indicar áreas de convergencia en la forma en que los Estados entienden qué normas jurídicas internacionales se aplican y de qué manera. Su uniformidad de puntos de vista, combinada con las declaraciones de Estados extrarregionales, podría proporcionar más pruebas para delinear las normas pertinentes del derecho internacional consuetudinario.

b. Indicar opiniones divergentes sobre las normas del derecho internacional que se aplican y la forma en que se aplican. Eso podría facilitar el establecimiento de un punto de partida para un

---

[9] Australian Mission to the United Nations. *Australian Paper—Open Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security* (septiembre de 2019) ("las opiniones de Australia").

[10] Kersti Kaljulaid, Presidente de Estonia. *Speech at the opening of CyCon 2019* (29 de mayo de 2019) ("las opiniones de Estonia").

[11] Ministère des Armées. *Droit international appliqué aux operations dans le cyberspace* (9 de septiembre de 2019) ("las opiniones del Ministerio de Defensa de Francia"). No las llamo "opiniones de Francia" porque por lo menos un experto ha señalado que el autor del documento es el Ministerio de Defensa de Francia, y su contenido no puede atribuirse al Estado francés en conjunto. Véase Gary Corn, *Punching on the Edges of the Gray Zone, Iranian Cyber Threats and State Cyber Responses*, en *Just Security* (11 de febrero de 2020) (donde dice que, a pesar de las numerosas afirmaciones en contrario, el documento francés no dice que es la posición oficial del Gobierno de Francia. Fue escrito y publicado por el Ministerio de Defensa. Análogamente, el *Law of War Manual*, del Departamento de Defensa de Estados Unidos, no refleja necesariamente las opiniones del gobierno en conjunto).

[12] *Letter from Minister of Foreign Affairs to President of the House of Representatives on the international legal order in cyberspace*, 5 de julio de 2019, apéndice 1 ("las opiniones de los Países Bajos").

[13] Véase, por ejemplo, Egan, nota 7 *supra*, 817.

[14] Véanse, por ejemplo, CICR, Documento de posición sobre *Derecho internacional humanitario y ciberoperaciones durante conflictos armados* (noviembre de 2019) ("Documento de posición del CICR"); 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*, 70 años de los Convenios de Ginebra (Nov. 2019) ("Informe del CICR de 2019");
CICR, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja (octubre de 2015) 39-43 ("Informe del CICR de 2015").

[15] Egan, nota 7 *supra*, 817 ("Es posible que las interpretaciones o aplicaciones del derecho internacional propuestas por grupos no gubernamentales no reflejen la práctica o las opiniones jurídicas de muchos de los Estados o de la mayoría. El relativo silencio de los Estados podría llevar a la imprevisibilidad en el ámbito cibernético, que podría sembrar la incertidumbre entre los Estados con respecto a las opiniones de los demás con respecto al marco jurídico aplicable. En el contexto de un incidente cibernético particular, esta incertidumbre podría dar lugar a percepciones erróneas y errores de cálculo de los Estados, lo cual, a su vez, podría llevar a una escalada y, en el peor de los casos, a un conflicto" [traducción del CJI]).

diálogo ulterior, sea para conciliar posiciones divergentes, aclarar el contenido del derecho o incluso tratar de cambiarlo. Además, una mayor transparencia de las opiniones de un Estado puede llevar a otros Estados a adaptar su comportamiento para limitar el riesgo de escalada involuntaria o conflicto.

c. Dar a los Estados Miembros de la OEA una voz apropiada en las conversaciones mundiales sobre la aplicación del derecho internacional. El año pasado, la Asamblea General de las Naciones Unidas encomendó a un nuevo Grupo de Expertos Gubernamentales (GEG) que recabara opiniones nacionales sobre el derecho internacional[16]. En vista de que solo cuatro Estados Miembros de la OEA participan en el GEG (Brasil, México, Estados Unidos y Uruguay), el trabajo del Comité ofrece a otros Estados Miembros la oportunidad de presentar una gama más completa de opiniones de toda la región. Eso concuerda con el llamamiento de la Unión Europea a *todos* los Estados Miembros de las Naciones Unidas para que presenten contribuciones nacionales sobre la forma en que se aplica el derecho internacional al uso de la tecnología de la información y las comunicaciones por los Estados[17].

Al mismo tiempo, es importante reiterar lo que *no* se procura hacer con este proyecto. No es su finalidad codificar o desarrollar gradualmente el derecho internacional (ni siquiera presentar las mejores prácticas u orientación general). Tampoco es su finalidad ofrecer una perspectiva integral o fundamental de los asuntos jurídicos internacionales en el contexto cibernético. El objetivo es más moderado. El propósito de las preguntas era recabar las opiniones de los Estados sobre la forma en que el derecho internacional se aplica al ciberespacio en las áreas en las cuales han surgido más discusiones (y discordia) hasta el momento. Por lo tanto, lo que se busca con este proyecto es proporcionar a los Estados Miembros de la OEA una base para que sean más transparentes en lo que respecta a la forma en que entienden la relación del derecho internacional con el ciberespacio y la tecnología de la información y las comunicaciones (TIC) de la cual deriva.

7. Con la autorización del Comité, preparé un cuestionario sobre estos temas con aportes del Departamento de Derecho Internacional de la OEA y el Comité Internacional de la Cruz Roja. El cuestionario se distribuyó a los Estados Miembros en enero de 2019. En mi tercer informe presenté una actualización del contenido del cuestionario y pedí una prórroga del plazo para responder[18].

8. Después de mi tercer informe, tuve la oportunidad de participar en consultas organizadas por la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), de la OEA, con la Oficina de Asuntos de Desarme de las Naciones Unidas los días 15 y 16 de agosto de 2019. En esa oportunidad hablé a los participantes sobre el trabajo del Comité en este campo. En diciembre participé (en calidad de académico) en la reunión intersesional informal 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. Allí mantuve varias consultas informales con los Estados y otros interesados y describí el interés del Comité en promover la transparencia en la forma en que los Estados entienden la aplicación del derecho internacional al ciberespacio. En ambos contextos recibí comentarios siempre positivos y aliento, lo cual muestra que hay gran interés en ofrecer a los Estados un foro o más de uno para que expresen sus opiniones y sigan fortaleciendo el estado de derecho en el ciberespacio.

9. En este informe presento una breve reseña de las respuestas a las diez preguntas del Comité sobre el derecho internacional y el ciberespacio. Hasta ahora, el Comité ha recibido nueve respuestas.

---

[16] Véase la resolución 266 de la Asamblea General de las Naciones Unidas, nota 3 *supra*, párr. 3 (sobre el mandato del GEG). Además del nuevo GEG, hay un grupo de trabajo de composición abierta patrocinado por las Naciones Unidas cuyo objetivo es llevar a la práctica el trabajo de GEG anteriores y, en algunos casos, rever o incluso revisar los resultados de ese trabajo. Véase A/RES/73/27.

[17] *EU Statement*, nota 3 *supra*.

[18] Véase Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency: Third Report*, OEA/Ser.Q, CJI/doc 594/19 (24 de julio de 2019) ("tercer informe de Hollis").

Ocho son de fondo, ya que Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana y Perú proporcionaron respuestas específicas[19], mientras que Estados Unidos remitió al Comité a sus declaraciones anteriores de 2012 a 2016[20]. La novena respuesta (de Brasil) no fue de fondo, sino que destacó el trabajo de Brasil en el GEG de las Naciones Unidas (que su experto preside) como foro donde planeaba abordar algunos aspectos de la aplicación del derecho internacional al ciberespacio[21].

10. Antes de examinar las respuestas correspondientes a cada pregunta, debo recalcar tres reacciones generales. Ante todo, es evidente que los Estados que respondieron tienen un interés duradero en el estado de derecho, incluido el papel que el derecho internacional puede desempeñar en la reglamentación del comportamiento de los Estados en el ciberespacio. Esto es sin duda un avance y es muy prometedor para la cooperación y la coordinación futuras de los Estados Miembros en lo que se refiere a los asuntos jurídicos internacionales en este contexto.

11. Sin embargo, al mismo tiempo debo expresar una *segunda* reacción, menos positiva, a las respuestas del cuestionario. Consideradas en conjunto, revelan una *falta de uniformidad* de la capacidad actual de los Estados Miembros. Cuando hablo de "capacidad" me refiero no solo a las diferencias en la capacidad operacional de los Estados para realizar operaciones cibernéticas, aunque esas diferencias son muy reales, sino también a la medida en que los Estados Miembros de la OEA parecen comprender las cuestiones técnicas y jurídicas pertinentes que han suscitado mucha atención en otros contextos geopolíticos, como las Naciones Unidas. Claro está, varios Estados ponen de manifiesto en su respuesta un profundo conocimiento de las diversas formas en que pueden recurrir a operaciones cibernéticas como sustituto de otras cosas que han hecho anteriormente y como herramienta novedosa para alcanzar objetivos, escalas o efectos nunca antes vistos. Al mismo tiempo, otros Estados parecen tener una comprensión más limitada de lo que se puede lograr en el ciberespacio. Su comprensión se complica con la falta de un lenguaje compartido, ya que los Estados utilizan términos y definiciones muy diferentes en sus respuestas[22]. Asimismo, en lo que se refiere al derecho internacional, varios Estados evidentemente conocen las diversas líneas divisorias que han dominado la conversación en los últimos años, mientras que otros demuestran un conocimiento mucho menor de las normas jurídicas internacionales subyacentes y de las cuestiones particulares que su aplicación suscita en el contexto cibernético.

12. En vista de estas disparidades, sería conveniente que el Comité considerara si, además de sondear las opiniones de los Estados, la OEA debería trabajar para aumentar más la capacidad jurídica y

---

[19] Nota del Estado Plurinacional de Bolivia, Ministerio de Relaciones Exteriores, Misión Permanente ante la Organización de los Estados Americanos, MPB-OEA-NV104-19 (17 de julio de 2019) (que contiene las respuestas del Comando en Jefe de las Fuerzas Armadas del Estado, Inspectoría General de las Fuerzas Armadas, al cuestionario del CJI) ("respuesta de Bolivia"); Respuesta de 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").

[20] Véase la nota 7.

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

[22] Por ejemplo, los Estados usan definiciones diferentes de ciberespacio. Compárese la respuesta de Guyana, nota 19 *supra*, en 2 (donde se usa una definición tomada del sitio web de la Academia Naval de Estados Unidos) con la respuesta de Perú, nota 19 *supra*, en 2 (donde se usa una definición tomada de Kristen Eichensehr, *The Cyber-Law of Nations* 103, en *Georgetown L. J.* 323, 324 [2015], que, a su vez, proviene del *Oxford English Dictionary*).

técnica. El CICTE, de la OEA, ya tiene una trayectoria excelente de ayuda a los Estados Miembros para aumentar la capacidad con la formulación de estrategias "nacionales" de ciberseguridad y el establecimiento de equipos de respuesta a incidentes de seguridad informática (CSIRT)[23]. En la región también se han llevado a cabo varios programas para capacitar a los ministerios de relaciones exteriores de los Estados Miembros sobre las cuestiones jurídicas pertinentes y los términos de los debates en curso[24]. No obstante, las respuestas actuales indican que se puede y se debe hacer más. Asimismo, esta opinión se refleja en las respuestas de varios Estados Miembros. La respuesta de Costa Rica fue particularmente elocuente en ese sentido:

> la necesidad urgente de espacios de estudio y análisis para poder atender con éxito y efectividad toda la problemática que podría[n] generar las operaciones cibernéticas, no solo en atención a los ataques y su forma de contrarrestarlos, prevenirlos, sancionarlos, sino también de la responsabilidad de los Estados, aún frente a sujetos no estatales.
>
> En ese sentido, expresamos con todo respeto la necesidad de unir esfuerzos para abrir los espacios idóneos, para que países como Costa Rica y otros se involucren en el estudio de esta temática y hagan propuestas, no solo en orden al Derecho internacional sino también de derecho interno, que puedan dar un paso en la atención de una realidad virtual con implicaciones transfronterizas, con capacidad de afectar derechos fundamentales de los ciudadanos del mundo[25].

Teniendo en cuenta estos puntos de vista, invitaría al Comité a opinar si la OEA podría aumentar la capacidad jurídica internacional en este espacio y de qué forma. Me interesan en particular las formas de asegurar que los Estados Miembros posean los conocimientos jurídicos y técnicos básicos necesarios para participar en las discusiones y los debates en curso y sacar sus propias conclusiones fundamentadas.

13. *Tercero*, la tasa de respuesta al cuestionario del Comité sigue siendo subrepresentativa de la región en conjunto. Agradecemos el tiempo y el esfuerzo dedicados por los Estados a las respuestas de fondo, que son sumamente valiosas. Sin embargo, las respuestas recibidas hasta ahora representan menos de 25% de los Estados Miembros de la OEA. Para tener una idea más exacta de la forma en que la región entiende la aplicación del derecho internacional al ciberespacio se necesitan respuestas de más Estados Miembros. Invito al Comité a que opine sobre si sería útil o factible tratar de obtener estas respuestas.

14. Con estas salvedades en mente, a continuación copio cada pregunta del Comité seguida de un resumen de las respuestas recibidas hasta ahora.

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.

15. 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 ocho 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

---

[23] Véase más información sobre las actividades del CICTE en http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

[24] Canadá y México, por ejemplo, fueron coanfitriones de un taller con la OEA el 30 de mayo de 2019, dirigido a Estados Miembros, en el cual se examinó la aplicación del derecho internacional al ciberespacio.

[25] Respuesta de Costa Rica, nota 19 *supra*, en 2.

reuniones del Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional[26].

16. Otros Estados dijeron que no estaban al tanto de posiciones anteriores sobre la aplicación del derecho internacional en el contexto cibernético[27]. 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 TIC[28].

17. La escasez de declaraciones oficiales anteriores 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?

18. Aunque una resolución reciente de la Asamblea General de las Naciones Unidas[29] 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[30]. 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.

19. 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

---

[26] Con respecto a las citas, véase la nota 7 *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").

[27] Véase, por ejemplo, la respuesta de Ecuador, nota 19 *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 19 *supra*, en 1 (ídem).

[28] Respuesta de Bolivia, nota 19 *supra*, en 1 (donde se cita una nueva ley de 2015); respuesta de Chile, nota 19 *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 19 *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 19 *supra*, en 1.

[29] Véase la resolución 266 de la Asamblea General de las Naciones Unidas, nota 3 *supra*.

[30] 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).

la responsabilidad internacional de los Estados"[31]. Otros Estados que confirmaron la aplicación del derecho internacional fueron Ecuador, Perú y Estados Unidos[32]. Junto 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."[33]. 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[34].

20. 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[35]. 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*.

21. 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"[36]. 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[37]. 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[38].

---

[31] Respuesta de Chile, nota 19 *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").

[32] Respuesta de Ecuador, nota 19 *supra*, en 1 ("se aplica[n] las ramas del derecho internacional al ciberespacio"); respuesta de Perú, nota 19 *supra*, 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 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 7 *supra*, 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).

[33] Respuesta de Perú, nota 19 *supra*, en 1.

[34] Escrito presentado por Estados Unidos al GGE en 2014, nota 7 *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 7 *supra*, en 815 (ídem). Sobre la aplicación de los derechos humanos, véanse Koh, nota 7 *supra*, en 598; Egan, nota 7 *supra*, en 820; escrito presentado por Estados Unidos al GGE en 2016, nota 7 *supra*, en 824.

[35] Respuesta de Bolivia, nota 19 *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.

[36] Respuesta de Guatemala, nota 19 *supra*, en 1 y 2.

[37] Respuesta de Guyana, nota 19 *supra*, en 1 y 2.

[38] Íd.

22. 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.

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?

23. 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?[39] 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.

24. 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"[40]. 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

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

[40] Respuesta de Bolivia, nota 19 *supra*, en 2 a 7; respuesta de Chile, nota 19 *supra*, 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"); Guatemala, nota 19 *supra*, en 2; respuesta de Perú, nota 19 *supra*, en 1 a 3; Koh, nota 7 *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 7 *supra*, en 734; Egan, nota 7 *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 19 *supra*, en 1.

derecho de legítima defensa ante un ataque u operación cibernética que atente contra la soberanía de un país[41].

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[42]. 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)[43]. 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[44].

25. 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[45]. Asimismo, afirma que un ataque armado implica el uso de armamento y que una operación cibernética, que no implica el uso de armamento físico, no puede considerarse como un ataque armado que genere el ejercicio de la legítima defensa[46]. Al mismo tiempo, Guyana recalca que es posible que se usen operaciones cibernéticas en conflictos armados, que estarían regidas por el derecho internacional humanitario[47].

26. Con respecto a si una operación cibernética puede cruzar el umbral del uso de la fuerza (o de un ataque armado[48]) 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[49]. 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[50].

27. 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"[51]. Sin embargo, se

---

[41] Guatemala, nota 19 *supra*, en 2; respuesta de Perú, nota 19 *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).
[42] Koh, nota 7 *supra*, en 597.
[43] Véase *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)* [1986] ICJ Rep. 14, párrs. 176 y 191 (27 de junio) (donde se describen los ataques armados como las formas más graves de uso de la fuerza).
[44] Escrito presentado por Estados Unidos al GEG en 2014, nota 7 *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.
[45] Respuesta de Guyana, nota 19 *supra*, en 2.
[46] Íd.
[47] Véase íd. en 3 y 5.
[48] Esto parte del supuesto de que podría haber dos umbrales diferentes, contrariamente a la opinión de Estados Unidos. Véanse las notas 42 y 43 *supra* y el texto acompañante.
[49] Respuesta de Chile, nota 19 *supra*, en 2.
[50] Íd. en 2.
[51] Respuesta de Perú, nota 19 *supra*, en 3.

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)[52]. 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"[53]. 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"[54].

28. 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"[55]. Indica que, en el contexto cibernético, las consecuencias que producen "muerte, zozobra, pobreza" deberían considerarse violentas[56].

29. 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 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"[57].

30. 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[58].

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[59]. 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

---

[52] Íd.
[53] Íd. en 2.
[54] Íd. en 3.
[55] Guatemala, nota 19 *supra*, en 2.
[56] Íd.
[57] Respuesta de Bolivia, nota 19 *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).
[58] Koh, nota 7 *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" [traducción del CJI]). Estados Unidos ha mantenido este punto de vista desde entonces. Véase el escrito presentado al GEG en 2014, nota 7, en 734. Este escrito se anexó al de 2016, lo cual indica que su contenido seguía siendo válido.
[59] Koh, nota 7 *supra*, en 595.

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[60]. 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?

31. 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[61]. 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 utilizar estos agentes no estatales como sustitutos para llevar a cabo diversas operaciones cibernéticas.

32. 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[62]. 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)[63]. 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[64]. Posteriormente, la Corte Penal Internacional refrendó la norma del "control general"[65].

33. 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

---

[60] Íd.

[61] 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), A/56/10 55 [3]; *Tallinn 2.0,* nota 14 *supra*, regla 15.

[62] Artículos sobre la responsabilidad del Estado, nota 61 *supra*, art. 11; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* 52 (2012).

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

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

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

efectivo" en otros contextos[66]. 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.

34. En su respuesta, varios Estados Miembros ponen de relieve la dificultad de la atribución en el ciberespacio[67]. 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[68]. En ese sentido, Perú comenta que "la inercia de un 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"[69]. 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[70]. 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"[71].

35. 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[72].

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[73].

---

[66] *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).

[67] Guatemala, nota 19 *supra*, en 3 (donde se indica que "es sumamente complicado" determinar una clara responsabilidad por un ataque cibernético); Perú, nota 19 *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").

[68] Ecuador, nota 19 *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"); Guatemala, nota 19 *supra*, en 3 (donde responde desde la óptica de la debida diligencia del Estado anfitrión en vez del grado de control ejercido sobre agentes sustitutos).

[69] Respuesta de Perú, nota 19 *supra*, en 4 (donde se cita el artículo 11 de los artículos sobre la responsabilidad del Estado).

[70] Bolivia, nota 19 *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.

[71] Escrito presentado por Estados Unidos al GEG en 2014, nota 7 *supra*, en 738 (traducción del CJI).

[72] Artículos sobre la responsabilidad del Estado, nota 61 *supra*, art. 8; respuesta de Chile, nota 19 *supra*, en 2; respuesta de Guyana, nota 19 *supra*, en 3; respuesta de Perú, nota 19 *supra*, en 4. Las respuestas de Chile y Perú también parecen basarse en el artículo 5 de los artículos sobre 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 19 *supra*, en 2, y la respuesta de Perú, nota 19 *supra*, en 4.

[73] Artículos sobre la responsabilidad del Estado, nota 61 *supra*, en 48 (comentario sobre el artículo 8).

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"[74]. 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[75].

36. 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"[76]. Asimismo, opina que las normas relativas a la responsabilidad del Estado son las mismas en el contexto de los conflictos armados[77].

37. 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"[78] 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".

38. 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"[79]. 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[80].

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?

39. 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)

---

[74] Koh, nota 7 *supra*, en 595; escrito presentado por Estados Unidos al GEG en 2014, nota 7 *supra*, en 738 (ídem); Egan, nota 7 *supra*, en 821; escrito presentado por Estados Unidos al GEG en 2016, nota 7 *supra*, en 826.
[75] Egan, nota 7 *supra*, en 821; escrito presentado por Estados Unidos al GEG en 2016, nota 7 *supra*, en 826.
[76] Respuesta de Chile, nota 19 *supra*, en 2.
[77] Íd. en 3.
[78] Respuesta de Perú, nota 19 *supra*, en 4 y 5.
[79] Respuesta de Guatemala, nota 19 *supra*, en 3.
[80] Véanse, por ejemplo, la respuesta de Bolivia, nota 19 *supra*, en 4 a 7, y la respuesta de Guyana, nota 19 *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 19 *supra*, en 2.

y la autorización de otros (por ejemplo, los dirigidos contra objetivos militares)[81]. 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 para la aplicabilidad de estas normas y la protección que confieren a los civiles y a la infraestructura civil[82]. 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[83].

40. 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"[84]. 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"[85]. 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"[86]. 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[87]. 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*[88].

41. 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[89]. 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[90]. El CICR, por su parte, ha argumentado que, en un conflicto

---

[81] 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.

[82] Documento de posición del CICR, nota 14 *supra*, en 7.

[83] 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 81 *supra*, art. 57.1; *Tallinn 2.0,* nota 14 *supra*, en 476.

[84] Protocolo adicional I, nota 81 *supra*, art. 49.

[85] *Tallinn 2.0*, nota 14 *supra*, en 415 (traducción del CJI).

[86] Véase el Documento de posición del CICR, nota 14 *supra*, en 7 (traducción del CJI).

[87] Informe de actividad: la labor del CICR en 2015, nota 14 *supra*, en 41.

[88] Íd.

[89] *Tallinn 2.0,* nota 14 *supra*, en 417.

[90] Informe de actividad: la labor del CICR en 2015, nota 14 *supra*, en 43. Véase también el Informe del CICR de 2019, supra nota 18, en 21 ("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

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[91].

42. 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" se aplica a las operaciones cibernéticas sobre la base de la pérdida de funcionalidad, en vez de los conceptos más tradicionales de daño físico o destrucción.

43. 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[92]. 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[93]. 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"[94]. 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"[95]. Perú responde que, para que haya un "ataque", se deben causar "daños físicos" a "personas" o "bienes públicos o privados"[96]. 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[97]. Eso implica que, si una operación cibernética produce efectos no cinéticos o reversibles, no constituye un ataque armado[98], 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.

---

cibernéticas que afectan la funcionalidad de la infraestructura civil están sujetas a las normas que rigen los ataques en virtud del DIH ".)

[91] Véanse el Documento de posición del CICR, nota 14 *supra*, en 7, y el Informe de actividad: la labor del CICR en 2015, nota 14 *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 cual se infiere que la neutralización de objetos está comprendida en el ámbito del derecho internacional humanitario).

[92] Véanse, por ejemplo, respuesta de Bolivia, nota 19 *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 19 *supra*, en 3; respuesta de Guyana, nota 19 *supra*, en 3; respuesta de Perú, nota 19 *supra*, en 1; Koh, nota 7 *supra*, en 595 (opinión de Estados Unidos).

[93] Respuesta de Guyana, nota 19 *supra*, en 4.

[94] Respuesta de Chile, nota 19 *supra*, en 3.

[95] Íd.

[96] 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 19 *supra*, en 6.

[97] Escrito presentado por Estados Unidos al GEG en 2014, nota 7 *supra*, en 736.

[98] Egan, nota 7 *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" (traducción del CJI). Íd.

44. 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"[99]. 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"[100].

45. 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"[101]. 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"[102]. Guyana observa que, cuando una operación cibernética produce una pérdida de funcionalidad, puede o no constituir un ataque[103]. 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[104]. 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"[105]. 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?

46. 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[106]. 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?

47. 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

---

[99] Respuesta de Guatemala, nota 19 *supra*, en 3.
[100] Respuesta de Ecuador, nota 19 *supra*, en 3.
[101] Respuesta de Bolivia, nota 19 *supra*, en 4 a 7.
[102] Íd.
[103] Guyana, nota 19 *supra*, en 3.
[104] Íd. (traducción del CJI).
[105] Íd. (donde se cita el artículo 54.2 del Protocolo adicional I [traducción del CJI]).
[106] 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 81 *supra*.

incluye los datos, por lo menos en el derecho actual"[107]. 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[108]. 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 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"[109]. 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.

48. 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[110]. 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"[111]. 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[112] 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"[113]. 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

---

[107] *Tallinn 2.0*, nota 14 *supra*, en 437 (traducción del CJI).
[108] Íd. en 416 (traducción del CJI).
[109] CICR, Documento de posición, nota 14 *supra*, en 8; Informe del CICR de 2019, nota 18 *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 14 *supra*, en 43 (traducción del CJI).
[110] Véanse la respuesta de Bolivia, nota 19 *supra*, en 5 a 7; la respuesta de Ecuador, nota 19 *supra*, en 2, y la respuesta de Guatemala, nota 19 *supra*, en 3.
[111] Respuesta de Chile, nota 19 *supra*, en 4.
[112] Íd.
[113] Íd.

vez de abordar la cuestión de si los datos que sean el objetivo del ataque pueden considerarse como un objeto o no[114].

49. 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, 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[115].

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?

50. La soberanía es sin lugar a dudas la característica estructural básica del ordenamiento jurídico internacional actual, que asigna derechos y responsabilidades a los Estados[116]. 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 es algo más que un principio básico: es 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)[117]. 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 que no dan lugar al uso de la fuerza ni constituyen una intervención

---

[114] Respuesta de Guyana, nota 19 *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).

[115] Respuesta de Perú, nota 19 *supra*, en 6. Perú explica que, en el primer caso, los ataques causarían "un daño militar significativo a la fuerzas de la contraparte", mientras que un ataque contra los datos en el hospital de campaña "no generaría una ventaja militar legítima". Íd.

[116] *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]).

[117] 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 43 *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. Informe del GEG de 2015, nota 2 supra, párrs. 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 14 *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.

prohibida[118]. 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[119]. Posteriormente, el Ministerio de Defensa de Francia y el Gobierno de Holanda han expresado apoyo a la soberanía como norma autónoma[120].

51. 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[121]. 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[122]. Chile y Estados Unidos también se hacen eco del poder que la soberanía confiere a los Estados sobre las TIC en su 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[123].

---

[118] *Tallinn 2.0,* nota 14 *supra*, regla 4 ("Un Estado no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado" [traducción del CJI]).

[119] Véase, por ejemplo, la opinión del Reino Unido*,* nota 8 *supra* ("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" [traducción del CJI]).

[120] Véanse la opinión del Ministerio de Defensa de Francia, nota 11 *supra*, 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 del CJI]); opinión de los Países Bajos, nota 12 *supra*, apéndice, en 2 ("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 Corn, nota 11 *supra* ("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" [traducción del CJI]).

[121] Respuesta de Bolivia, nota 19 *supra*, en 5 a 7; respuesta de Guyana, nota 19 *supra*, en 5.

[122] Respuesta de Ecuador, nota 19 *supra*, en 2.

[123] Respuesta de Chile, nota 19 *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 7 *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

52. 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[124]. 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"[125]. 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"[126]. 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"[127].

53. 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[128]. 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[129].

54. 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"[130]. Por lo tanto, "cada vez que un Estado contempla realizar una operación cibernética, debe tener en consideración no afectar la soberanía de otro"[131]. 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 obligatori. 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 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[132].

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[133].

55. 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"[134]. 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 materia de derechos humanos, y se mencionan en particular la libertad de expresión y la libertad de opinión).

[124] Respuesta de Bolivia, nota 19 *supra*, en 5 a 7; respuesta de Guatemala, nota 19 *supra*, en 3; respuesta de Guyana, nota 19 *supra*, en 5.

[125] Respuesta de Guyana, nota 19 *supra*, en 5 (traducción del CJI).

[126] Íd. (traducción del CJI).

[127] Respuesta de Guatemala, nota 19 *supra*, en 3.

[128] Respuesta de Perú, nota 19 *supra*, en 6 y 7.

[129] Respuesta de Ecuador, nota 19 *supra*, en 2.

[130] Respuesta de Chile, nota 19 *supra*, en 5.

[131] Íd.

[132] Íd.

[133] Véase la nota 117.

[134] Koh, nota 7 *supra*, en 596 (traducción del CJI); escrito presentado por Estados Unidos al GEG en 2014, nota 7 *supra*, en 737; escrito presentado por Estados Unidos al GEG en 2016, nota 7 *supra*, en 825.

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"[135]. 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*"[136]. 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[137]. Sin embargo, no está claro cuán ampliamente compartida es esta opinión en el gobierno de los EE. UU en su conjunto.

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?

56. 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[138]. 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[139]. 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.

57. 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[140]. Varios Estados, entre ellos Francia y los Países Bajos, la han descrito como una norma jurídica que se aplica al ciberespacio[141]. Sin embargo,

---

[135] Egan, *supra* note 7, 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.

[136] Íd. en 819 (traducción del CJI).

[137] *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=%20%20

[138] 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).

[139] 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.

[140] GEG de 2015, nota 2 *supra*, párrs. 13 y 26 a 28.

[141] Opinión del Ministerio de Defensa de Francia, nota 11 *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" [traducción del CJI]); opinión de los Países Bajos, nota 12 *supra*, apéndice, en 4 ("el principio de la debida diligencia requiere que los Estados tomen medidas con respecto a

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[142]. 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.

58. 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 ciberespacio[143]. 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"[144]. Guatemala adopta una posición similar y agrega que, como "ciberespacio" es un término muy amplio, actuar con la diligencia debida puede ser sumamente complicado[145]. 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"[146].

59. 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[147]. 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[148]. 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.

60. 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

---

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. Opinión de Estonia, nota 10 *supra* ("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]).

[142] Opinión de los Países Bajos, nota 12 *supra*, apéndice, en 4.

[143] Respuesta de Chile, nota 19 *supra*, en 6 y 7; respuesta de Ecuador, nota 19 *supra*, en 2; respuesta de Guatemala, nota 19 *supra*, en 4; respuesta de Guyana, nota 19 *supra*, en 5; respuesta de Perú, nota 19 *supra*, en 7.

[144] Respuesta de Chile, nota 19 *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 19 *supra*, en 2.

[145] Respuesta de Guatemala, nota 19 *supra*, en 4.

[146] Íd. en 2 y 4.

[147] Respuesta de Bolivia, nota 19 *supra*, en 3 a 7.

[148] Véase *Tallinn 2.0*, nota 14 *supra*, en 40.

vinculantes[149]. 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.

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?

61. 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 más atención a la protección de los "derechos fundamentales de sus ciudadanos en cualquier dimensión en la que actúen", incluso en el ciberespacio[150]. Algunas respuestas se centran en la ciberdelincuencia y, en particular, el Convenio de Budapest, elaborado por el Consejo de Europa[151]; otras destacan la contribución de los Manuales de Tallinn[152].

62. 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"[153]. 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 diferentes[154].

* * *

63. Si el Comité lo autoriza, propongo publicar mi informe (y las respuestas) para que los Estados de la región y de todo el mundo puedan beneficiarse de las posiciones y los puntos de vista que contiene. Sería también una oportunidad para recabar la opinión de los Estados que todavía no han respondido el cuestionario.

64. Como de costumbre, agradeceré las opiniones y las observaciones del Comité sobre las respuestas recibidas hasta la fecha y su indicación de si valdría la pena tratar de obtener más respuestas. Agradecería también los comentarios del Comité sobre la forma en que podríamos abordar la capacidad técnica y jurídica desigual que se ha observado en el marco de este proyecto.

---

[149] Escrito presentado por Estados Unidos al GEG en 2014, nota 7 *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" [traducción del CJI]).

[150] Respuesta de Bolivia, nota 19 *supra*, en 6 y 7.

[151] Respuesta de Guatemala, nota 19 *supra*, en 4; respuesta de Bolivia, nota 19 *supra*, en 6 y 7.

[152] Respuesta de Costa Rica, nota 19 *supra*, en 2 (donde se expresa el interés de Costa Rica en adherirse al Convenio de Budapest); respuesta de Guatemala, nota 19 *supra*, en 4 (donde se cita el Convenio de Budapest).

[153] Respuesta de Ecuador, nota 19 *supra*, en 3.

[154] Respuesta de Guyana, nota 19 *supra*, en 5 y 6 (donde se indica que el anonimato es una dificultad particular para la aplicación del derecho actual).

65. Por último, valoraría los aportes del Comité sobre los próximos pasos de este proyecto, si considera que debe haberlos. Por una parte, simplemente podría recibir comentarios de los Estados Miembros sobre este informe y revisarlo según sea necesario antes de su aprobación final. Otra posibilidad es que, en mi próximo informe, trate de ampliar el análisis con la respuesta de más Estados Miembros o, si no se reciben más respuestas, con una comparación de las opiniones de los Estados Miembros con las de Estados extrarregionales. En medida creciente contamos con más opiniones que antes y sería útil compararlas con las respuestas examinadas en este informe. ¿O debería mantener el foco original del proyecto y prestar atención solo a la transparencia de los Estados Miembros de la OEA en cuestiones relativas a la aplicación del derecho internacional a las operaciones cibernéticas?