94º PERÍODO ORDINARIO DE SESIONES
18-22 de febrero de 2019
Rio de Janeiro, Brasil

OEA/Ser.Q
CJI/doc.578/19
21 enero 2019
Original: inglés

EL DERECHO INTERNACIONAL Y LAS OPERACIONES CIBERNÉTICAS DE LOS ESTADOS: MEJORAR LA TRANSPARENCIA

(Presentado por el profesor Duncan B. Hollis)

1. El tema del derecho internacional y las operaciones cibernéticas de los Estados se planteó por primera vez durante el nonagésimo tercero período ordinario de sesiones del Comité. El autor fue invitado a presentar un informe inicial sobre temas relacionados con la aplicación del derecho internacional en el espacio cibernético, así como ideas sobre la forma en que el Comité podría tratar el tema.

2. Mi informe inicial examina el deficiente estado de la ciberseguridad mundial y los costos financieros, humanitarios y de seguridad nacional de las amenazas cibernéticas, con especial atención a aquellas dirigidas a la infraestructura crítica y a los procesos electorales. El informe también explora la creciente labor de los Estados para desarrollar capacidades a fin de participar directamente en operaciones cibernéticas defensivas *y* ofensivas. Otros Estados parecen haber utilizado actores no estatales "intermediarios" para realizar en operaciones cibernéticas bajo diferentes niveles de control o apoyo estatal.

3. Con toda esta actividad cibernética, mi informe inicial señaló la poca visibilidad que el derecho internacional ha tenido en la regulación de las operaciones cibernéticas del Estado. Si bien los expertos gubernamentales estuvieron de acuerdo en 2013 (y nuevamente en 2015) en que "[e]l derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable al ciberespacio", los intentos por llegar a un acuerdo sobre *cómo* el derecho se aplica se vieron frustrados.[1] Según se informa, un Grupo de Expertos Gubernamentales en 2017 fracasó porque los expertos gubernamentales de algunos Estados clave diferían en cuanto a la aplicación de algunas normas fundamentales del derecho internacional (por ejemplo, legítima defensa, derecho internacional humanitario, medidas de control, diligencia debida) a las operaciones cibernéticas de los Estados.[2]

4. El Comité Internacional de la Cruz Roja ofreció su opinión sobre cómo el derecho internacional se aplica al espacio cibernético en el área específica dentro de su mandato, es decir, el

---

1. *Véase* Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional*, párrafo 19, U.N. Doc. A/68/98 (24 de junio de 2013); Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional*, párrafo 10, U.N. Doc. A/70/174 (22 de julio de 2015).

2. *Véase, por ejemplo,* Arun M. Sukumar, *"The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?"* LAWFARE, 4 de julio de 2017.

derecho internacional humanitario.[3] Además, los dos *Manuales de Tallin* presentan la opinión de un grupo de expertos independiente (aunque financiado por la OTAN) sobre la forma en que el derecho internacional se aplica a las operaciones cibernéticas en general[4]. Ambos manuales son importantes obras de referencia y los gobiernos fueron consultados en su redacción. Pero algunos estudios recientes sugieren que, en la práctica, los Estados han dejado de lado dichos manuales.[5] En efecto, hay poca evidencia de que los Estados estén invocando el derecho internacional en respuesta a incidentes cibernéticos específicos y solo unos pocos Estados realizaron declaraciones públicas sobre la aplicación del derecho internacional en general. [6]

5. Al reflexionar sobre estas experiencias, mi informe presentó tres grupos de problemas con respecto a la regulación del derecho internacional sobre la conducta de los Estados en el espacio cibernético. En primer lugar, hay preguntas existenciales sobre si determinadas normas o doctrinas de derecho internacional tienen alguna influencia en el contexto cibernético. Aunque no lo han hecho en el ámbito público, en el contexto del Grupo de Expertos Gubernamentales, los expertos de algunos Estados se han opuesto a la aplicación de las doctrinas de derecho internacional humanitario, legítima defensa y debida diligencia al espacio cibernético.[7] En segundo lugar, aun si los Estados aceptan la pertinencia de un concepto específico de derecho internacional – tales como la soberanía y el principio de no intervención – los mismos discrepan con respecto a la "interpretación" adecuada en el contexto cibernético.[8] En tercer lugar, existe el anteriormente mencionado problema de la

---

3. CIRC, COMENTARIO (2016) DEL PRIMER CONVENIO DE GINEBRA DE 1949, 91 ¶¶ 253–256, y 158-159 ¶¶ 436-437; y CICR, El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos, Informe, 39-44 (octubre de 2015).

4. *Véase Michael Schmitt, ed., Manual* de *Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas* (Tallin, Estonia: Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, 2017); Michael Schmitt, ed., *Manual de Tallin sobre el derecho internacional aplicable en la guerra cibernética,* (Tallin, Estonia, Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, 2013).

5. Dan Efrony y Yuval Shany, *A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112, *American Journal of International Law*, 583 (2018).

6. *Véase, por ejemplo,* Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century*, 23 de mayo, 2018 (Reino Unido); Revue stratégie de cyberdéfense 82-84 (febrero 2018) (Francia); Brian Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Law School, 10 de noviembre de 2016 (Estados Unidos); Harold Koh, *International Law in Cyberspace,* 54 HARV. INT'L LAW. J. 1, 7 (2012) (Estados Unidos). Existe una reciente excepción a esta tendencia. En octubre de 2018, el Reino Unido acusó al Departamento Central de Inteligencia (GRU) – la sección de inteligencia militar de Rusia – de su responsabilidad en una serie de operaciones cibernéticas, entre las que se incluye la intervención en la Organización para la Prohibición de las Armas Químicas (la cual estaba investigando el uso de un agente neurotóxico contra un ex espía ruso y su hija en Salisbury, Reino Unido). El Secretario de Relaciones Exteriores del Reino Unido calificó la conducta de Rusia como el reflejo de "un deseo de obrar sin tener en cuenta el derecho internacional ni las normas establecidas", mientras que un comunicado de prensa relacionado describió las operaciones del Departamento Central de Inteligencia (GRU) como una "flagrante violación del derecho internacional". Comunicado de prensa, Ministerio de Relaciones Exteriores y Asuntos del Commonwealth, *UK exposes Russian cyber attacks*, 4 de octubre de 2018; Centro Nacional de Seguridad Cibernética (NCSC), *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 4 de octubre de 2018.

7. *Véase, por ejemplo,* Sukumar, *supra* nota 2.

8. Por ejemplo, con respecto a la soberanía, el Manual de Tallin 2.0 concibe la soberanía como una regla que los Estados podrían violar directamente a través de sus operaciones cibernéticas. Véase, Manual de Tallin 2.0, supra, nota 4, regla 4 ("Un Estado no debe efectuar operaciones cibernéticas que violen la soberanía de otro Estado"). El Gobierno holandés parece apoyar este enfoque. Bert Koenders, Ministro de Relaciones Exteriores, Países Bajos, Remarks at The Hague Regarding Tallinn Manual 2.0 (13 de febrero de 2017). Por el contrario, el Procurador General del Reino Unido cuestionó ese enfoque (así como también el

"aplicación", dado que los Estados han actuado relativamente poco para aplicar el derecho internacional en incidentes cibernéticos reales.[9] En consecuencia, es muy poca la responsabilidad legal internacional por la conducta de los Estados en el espacio cibernético.

6. El Comité recibió favorablemente el primer informe. Estuvo de acuerdo en que el tema era importante y correspondía al mandato del Comité, agregándolo a su temario y designando al actual autor como Relator. Ahora bien, el enfoque del Comité en las operaciones cibernéticas sigue siendo relativamente limitado; en lugar de formular las opiniones del Comité sobre la forma de aplicar el derecho internacional al ciberespacio, el Comité considera que un primer paso más fructífero consistiría en aumentar la transparencia sobre los puntos de vista de los Estados Miembros de la OEA en el tema. En resumen, el Comité apoya la idea de que los Estados Miembros formulen y den a conocer sus opiniones sobre estos asuntos.

7. Hacerlo tendría evidentes beneficios. En el ámbito legal, comprender cómo los Estados perciben el derecho internacional y el espacio cibernético permitirá un mapeo de las prácticas estatales, e identificará las áreas en las cuales los Estados poseen una visión general y uniforme sobre lo que el derecho internacional requiere. Con suficiente apoyo, estas opiniones pueden ayudar a determinar cómo el derecho internacional consuetudinario regula las operaciones cibernéticas del Estado. Pero, aunque los Estados tengan puntos de vista diferentes, o incluso contradictorios, es igualmente importante dar a conocer esas diferencias. De lo contrario, existe el riesgo de que los Estados con diferentes interpretaciones básicas sobre lo que establece el derecho internacional puedan, sin querer, dar lugar al escalamiento de un conflicto (es decir, el Estado A supone que su operación no cruza el umbral del ataque armado, pero el Estado B víctima lo interpreta como habiendo hecho exactamente eso). Conocer los aspectos sobre los cuales los Estados no están de acuerdo pondría de relieve los aspectos en los que se necesita un mayor diálogo, ya sea para cerrar esas brechas, expresar aclaraciones o buscar modificaciones que garanticen que el derecho internacional sea más efectivo en la regulación de la conducta de los Estados en el espacio cibernético.

8. La labor del Comité en materia de derecho internacional y espacio cibernético se centrará en la *transparencia* – en solicitar, recopilar y publicar las opiniones de los Estados Miembros de la OEA sobre cómo se aplica el derecho internacional en el contexto cibernético. El Comité autorizó al autor a preparar un cuestionario para obtener las opiniones de los Estados Miembros sobre algunos de los aspectos más importantes del derecho internacional relacionados con el espacio cibernético hasta la fecha.

9. El 15 de agosto de 2018, el autor presentó el proyecto sobre transparencia del Comité durante su reunión con asesores jurídicos de los Ministerios de Relaciones Exteriores de los Estados Miembros de la OEA. El proyecto fue recibido muy positivamente por todos los asistentes. Se hicieron sugerencias para abreviar la lista de preguntas planteadas (el informe original había adjuntado veinte posibles preguntas). Además, el representante de un asesor jurídico sugirió que el

---

abogado principal del *U.S. Cyber Command*, aunque lo hizo escribiendo a título personal). Véase, Wright, supra, nota 6 ("Algunos han tratado de argumentar la existencia de una regla cibernética específica sobre "violación de la soberanía territorial"…la soberanía es, por supuesto, fundamental en el sistema internacional basado en normas. Pero no estoy convencido de que actualmente podamos extrapolar ese principio general a una regla específica o una prohibición adicional para la actividad cibernética más allá de una intervención prohibida. La posición del Gobierno del Reino Unido es, por lo tanto, que no existe tal norma en el derecho internacional vigente".) Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, Just Security (15 de febrero de 2017).

9. *Véase supra* nota 6 y texto adjunto.

Comité procurara, ante todo, recopilar todas las declaraciones públicas anteriores realizadas por los Estados Miembros de la OEA relacionadas con la aplicación del derecho internacional en general.

10. Desde las reuniones del Comité en agosto, se han desarrollado nuevas iniciativas en foros multilaterales y de múltiples partes interesadas que continúan subrayando la aplicación del derecho internacional en el ciberespacio, incluido el hecho de que los derechos humanos que existen en el entorno "off-line" también deben aplicarse en el entorno en línea[10]. Al menos dos organizaciones regionales, la ASEAN y la Unión Europea, han afirmado que el derecho internacional se aplica al espacio cibernético y manifestaron su apoyo para que se explique más detalladamente cómo ello se realiza[11]. Además, la Unión Europea respaldó la idea de que *todos* los Estados Miembros de la ONU "deben presentar aportes nacionales sobre el tema de cómo se aplica el derecho internacional al uso de las [tecnologías de la información y la comunicación] por los Estados" para promover "el entendimiento mundial sobre los enfoques nacionales lo cual es fundamental para mantener la paz y la seguridad a largo plazo y reducir el riesgo de conflicto en el espacio cibernético" [12]. Por lo tanto, el enfoque del Comité está de acuerdo con las opiniones de otras organizaciones regionales.

11. Mientras tanto, la Asamblea General de las Naciones Unidas ha respaldado la conclusión de anteriores Grupos de Expertos Gubernamentales en el sentido de que el derecho internacional se aplica al ciberespacio.[13] También acordó comenzar dos nuevos procesos relacionados con la seguridad cibernética mundial: (i) un nuevo Grupo de Trabajo de Composición Abierta para analizar la seguridad cibernética en un foro relativamente abierto y permanente, y (ii) un nuevo Grupo de Expertos Gubernamentales que se formará y comenzará a reunirse a finales de la primavera

---

10. Véase, *Llamado de París para la confianza y la seguridad en el ciberespacio*, 12 de noviembre de 2018 ("Reafirmamos también que el derecho internacional, incluidos la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional consuetudinario, se aplica al uso de las tecnologías de la información y la comunicación (TIC) por los Estados. Reafirmamos que los mismos derechos que las personas gozan en sus comunicaciones en persona deben protegerse en línea, y reafirmamos también la aplicabilidad del derecho internacional de los derechos humanos en el espacio cibernético."); sírvase observar que, además de mi calidad de miembro del Comité, también presto servicios como consultor externo de Microsoft sobre temas de derecho internacional y ciberespacio, incluido el trabajo con el Gobierno de Francia para dar inicio al Llamado de París.

11. *Véase* ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (18 de noviembre de 2018) ("Reafirmar que el derecho internacional y, en particular, la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones, y reconocer la necesidad de que "se continúe estudiando la forma en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones por los Estados"); Declaración de la Unión Europea – Primera Comisión de Naciones Unidas, *Thematic Discussion on Other Disarmament Measures and International Security* (Discusión Temática sobre Otras Medidas de Desarme y Seguridad Internacional) (26 de octubre de 2018) (la Unión Europea recuerda que el derecho internacional, en particular la Carta de la OEA, es aplicable y fundamental para mantener la paz y la estabilidad y promover un entorno de TIC abierto, seguro y pacífico y accesible).

12. Declaración de la Unión Europea, *supra* nota 11.

13. Resolución 266 de la Asamblea General de Naciones Unidas, U.N. Doc. A/RES/73/266 (2 enero 2019) ("Confirmando las conclusiones del Grupo de Expertos Gubernamentales, en sus informes de 2013 y 2015, de que el derecho internacional y, en particular, la Carta de las Naciones Unidas, son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones").

o a principios del verano de 2019. [14] Con respecto al nuevo Grupo de Expertos Gubernamentales, la Asamblea General de las Naciones Unidas solicitó:

> [A]l Secretario General que, con la asistencia de un grupo de expertos gubernamentales… "continúe estudiando…la forma en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones por los Estados, y que le presente, en su septuagésimo sexto período de sesiones, un informe sobre los resultados del estudio, incluido un anexo que contenga las aportaciones nacionales de los expertos gubernamentales participantes sobre la cuestión de cómo se aplica el derecho internacional al uso de las tecnologías de la información y las comunicaciones;[15]

12. En su conjunto, parece que existe un impulso cada vez mayor para que los Estados expresen sus opiniones sobre la aplicación del derecho internacional en el ciberespacio. Ese apoyo, incluso en las Naciones Unidas, refuerza la importancia y la oportunidad de la labor del Comité sobre este tema. El Grupo de Expertos Gubernamentales estará compuesto por expertos de 20 a 25 Estados como máximo. Solo unos pocos de ellos serán Estados Miembros de la OEA. Por lo tanto, el Comité tendrá la oportunidad de estudiar y reunir un conjunto de opiniones más amplio y diverso entre *todos* los Estados Miembros de la OEA que lo que permite el proceso del Grupo de Expertos Gubernamentales. Además, a medida que otras organizaciones regionales alientan a sus Estados Miembros para formular puntos de vista sobre la aplicación del derecho internacional, es importante que los Estados Miembros de la OEA tengan la oportunidad de promover sus puntos de vista, para que otras regiones no tengan una voz exagerada para delinear los límites y contenidos del derecho internacional en el contexto cibernético. Por lo tanto, es fundamental que el Comité reúna y comparta las opiniones de los Estados Miembros de la OEA no solo dentro de la región sino también con otras organizaciones internacionales regionales y dentro del sistema de las Naciones Unidas.

13. Además, cabe señalar que la importante labor del Grupo de Expertos Gubernamentales se verá restringida, por su mandato, a determinados temas limitados. Como producto de la Primera Comisión, el Grupo de Expertos Gubernamentales se concentrará únicamente en cuestiones de derecho internacional en relación con los aspectos de desarme y seguridad. Por el contrario, el mandato del Comité es más amplio, y las respuestas de los Estados a su cuestionario pueden abordar una gama más extensa de temas, incluidos todos los asuntos de derecho internacional público y privado relacionados con las operaciones cibernéticas del Estado. Por lo tanto, el Comité puede mejorar la transparencia en toda la gama de temas de derecho internacional.

14. Posteriormente a la producción de mi primer informe, realicé una convocatoria sumaria para los Estados Miembros de la OEA sobre este tema junto con una lista revisada y más corta de preguntas. El cuestionario del Comité terminó con 10 preguntas:

- La primera pregunta responde a la sugerencia de uno de los asesores jurídicos del Ministerio de Relaciones Exteriores de que el Comité solicite y compile las declaraciones existentes sobre el derecho internacional y el ciberespacio.
- La segunda pregunta está orientada hacia preguntas existenciales: solicitar a los Estados que confirmen o nieguen si ciertas normas vigentes del derecho internacional se aplican (o no) al contexto cibernético.

---

14. Véase, U.N. Doc. A/RES/73/27 (en referencia al Grupo de Trabajo de Composición Abierta, que estará abierto a todos los Estados Miembros de las Naciones Unidas con planes que incluyan consultas con la industria); U.N. Doc. A/RES/73/266 (2 enero de 2019) (en referencia al Grupo de Expertos Gubernamentales).

15. U.N. Doc. A/Res/73/266, párrafo 3.

- La tercera pregunta se refiere al empleo de la fuerza (el *jus ad bellum*), con especial atención a los criterios que utiliza un Estado para determinar si una operación cibernética corresponde al uso de fuerza o a un ataque armado.
- Las preguntas cuarta y quinta se refieren a cómo los Estados entienden la adjudicación de responsabilidad legal internacional por el comportamiento de actores no estatales.
- La sexta y séptima preguntas abordan el derecho internacional humanitario y dos de los aspectos críticos más importantes, a saber, la definición de un "ataque" en el contexto cibernético y la pregunta sobre si las operaciones cibernéticas dirigidas solamente a datos constituirían un ataque (nota: estas preguntas fueron corregidas sustancialmente con respecto a la propuesta original de acuerdo con las sugerencias y los comentarios presentados por el Comité Internacional de la Cruz Roja).
- La octava pregunta solicita las opiniones de los Estados sobre si la soberanía comprende su propia norma para la conducta del Estado en el ciberespacio o si es, en cambio, un principio de fondo que informa el contenido de otras normas.
- La novena pregunta realiza una investigación similar con respecto a la diligencia debida.
- Finalmente, la décima pregunta invita a los Estados a determinar áreas adicionales del derecho internacional en las que el Comité debería centrarse para mejorar la transparencia en el contexto cibernético.

15. El cuestionario revisado se finalizó con la asistencia de la Secretaría del Comité. Se preparará un informe sobre las respuestas pertinentes al Cuestionario del Comité con anterioridad al próximo período ordinario de sesiones del Comité.

Una vez que se haya recibido un número suficiente de respuestas, el Comité deberá decidir si se formularán más preguntas o simplemente se aprobará su distribución a la Asamblea General con una recomendación de que apruebe su distribución dentro y fuera de la región.

* * *

COMITÉ JURÍDICO INTERAMERICANO
CUESTIONARIO PARA LOS ESTADOS MIEMBROS
EL DERECHO INTERNACIONAL Y LAS OPERACIONES CIBERNÉTICAS DE LOS ESTADOS: MEJORAR LA TRANSPARENCIA

El ciberespacio se ha convertido en un componente integral de la vida civil en todos sus aspectos sociales, económicos, culturales y políticos. Al mismo tiempo, las "amenazas cibernéticas" a las tecnologías de la información y la comunicación (TIC) se han vuelto omnipresentes. Las operaciones cibernéticas han generado importantes pérdidas financieras, violado los derechos humanos y amenazado la seguridad nacional. Los Estados han respondido mediante la regulación del delito cibernético y la creación de capacidad, ya sea directamente o a través de representantes, para participar en operaciones cibernéticas defensivas *y* ofensivas. El aumento de las capacidades y las actividades de los Estados en el ciberespacio ha dado lugar a convocatorias generalizadas para aclarar cuáles son las normas que rigen el comportamiento del Estado. En 2013 y 2015, un Grupo de Expertos Gubernamentales (GEG) convocado por la Primera Comisión de la Asamblea General de las Naciones Unidas confirmó que "el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable" al ciberespacio[1]. A principios del presente año, la Asamblea General de las Naciones Unidas respaldó esta conclusión.[2]

Lamentablemente, sin embargo, los Estados no han podido ponerse de acuerdo sobre *cómo* se aplica el derecho internacional. Solo algunos Estados ofrecieron opiniones públicas sobre el tema.[3] Y si bien algunos expertos independientes (especialmente a través de dos Manuales de Tallin[4]) han

---

1. Secretario General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, ¶ 19, U.N., Naciones Unidas A/68/98 (24 de junio de 2013); Naciones Unidas, Secretario General, *Informe del Grupo de Expertos Gubernamentales sobre avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, ¶ 10, U.N. Doc. A/70/174 (22 de julio de 2015).

2. Resolución 266 de la Asamblea General de Naciones Unidas, U.N. Doc. A/RES/73/266 (2 enero 2019) ("Confirmando las conclusiones del Grupo de Expertos Gubernamentales, en sus informes de 2013 y 2015, de que el derecho internacional y, en particular, la Carta de las Naciones Unidas, son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones").

3. *Véase. por ejemplo,* Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century*, 23 de mayo de 2018 (Reino Unido; Revue stratégie de cyberdéfense 82-84 (Feb. 2018) (Francia); Brian Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Law School, 10 de noviembre de 2016 (Estados Unidos); Harold Koh, *International Law in Cyberspace,* 54 HARV. INT'L LAW. J. 1, 7 (2012) (Estados Unidos). El Comité Internacional de la Cruz Roja también expresó su opinión sobre la aplicación del derecho internacional humanitario al ciberespacio. Véase, CICR, COMENTARIO DEL PRIMER CONVENIO DE GINEBRA DE 1949, ¶¶ 253–256, y 158-159 ¶¶ 436-437; y CICR, El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos, Informe, 39-44 (octubre de 2015).

4. MICHAEL SCHMITT (ED.), MANUAL DE TALLIN 2.0 SOBRE EL DERECHO INTERNACIONAL APLICABLE A LAS OPERACIONES CIBERNÉTICAS (CENTRO DE EXCELENCIA PARA LA CIBERDEFENSA COOPERATIVA DE LA OTAN, 2017); MICHAEL SCHMITT (ED.), MANUAL DE TALLIN 2.0 SOBRE EL DERECHO INTERNACIONAL APLICABLE A LA GUERRA CIBERNÉTICA (CENTRO DE EXCELENCIA PARA LA CIBERDEFENSA

tratado de llenar este vacío de información, los Estados no lo han hecho. Hasta la fecha, los Estados se han abstenido de invocar el derecho internacional tanto en general como en respuesta a incidentes cibernéticos específicos.

Más adelante, en 2019, se convocará un nuevo Grupo de Expertos Gubernamentales de las Naciones Unidas. Su mandato alentará a los expertos a ampliar la información sobre cómo sus Estados entienden la aplicación del derecho internacional al ciberespacio[5]. Sin embargo, el nuevo Grupo de Expertos Gubernamentales constará de un número reducido de miembros con solo un grupo limitado de voces de las Américas. El Comité Jurídico Interamericano (CJI) apoya el trabajo pasado y futuro del GEG de las Naciones Unidas. No obstante, cree que se puede realizar un mayor esfuerzo para aumentar la transparencia de sobre la forma en que los Estados conciben la aplicación del derecho internacional al ciberespacio. Además, esta opinión es compartida por otras organizaciones regionales, incluidas la ASEAN y la Unión Europea.[6]

El cuestionario adjunto representa el primer paso en la labor del CJI de solicitar, compilar y publicar las opiniones de los Estados Miembros sobre la aplicación del derecho internacional a las operaciones cibernéticas. Refleja algunos de los temas más importantes o más discutidos que han surgido hasta la fecha. No está previsto que el Comité presente sus propios puntos de vista sobre estos temas. Más bien, el objetivo es aportar un foro en el que se puedan recopilar y divulgar las opiniones de los Estados con el fin de promover el entendimiento mutuo en la región. En la medida en que las respuestas de los Estados Miembros se ajusten a las declaraciones existentes sobre el derecho internacional presentadas por el Grupo de Expertos Gubernamentales de las Naciones Unidas o en cualquier otro lugar, estas respuestas serían una contribución importante para explicar las normas jurídicas internacionales vigentes. Sin embargo, es igualmente importante determinar los aspectos con respecto a los cuales existen discrepancias entre las opiniones de los Estados. Al hacerlo, los Estados podrán apreciar cómo otros Estados perciben las operaciones cibernéticas ofensivas y defensivas, establecer expectativas para sus futuros intercambios y proporcionar una base para continuar el diálogo.

Por lo tanto, el Comité invitaría a todos los Estados Miembros a responder a las siguientes preguntas. Sería ideal que los Estados Miembros respondieran a las diez preguntas planteadas. Sin embargo, los Estados Miembros pueden optar por presentar un conjunto de respuestas más limitado si hay preguntas específicas sobre las que sus Gobiernos todavía no han formulado una opinión (o su opinión no está pronta para hacerse pública). Como lo indica la pregunta final, el Comité también agradecería las opiniones de los Estados Miembros sobre preguntas o temas adicionales en los cuales una mayor transparencia beneficiaría la aplicación del derecho internacional al ciberespacio.

COOPERATIVA DE LA OTAN, 2013). Aunque fue financiado por el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, el Manual Tallin constituye la labor de un grupo de expertos independientes.

5. *Véase* Res. 266 de la Asamblea General de Naciones Unidas, U.N. Doc. A/Res/73/266, ¶3 (2 de enero de 2019).

6. *Véase* ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (18 noviembre 2018) ("Reafirmar que el derecho internacional, y, en particular, la Carta de las Naciones Unidas, son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones" y reconocer la necesidad de que "se continúe estudiando la forma en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones por los Estados").

PREGUNTAS:

1. ¿Ha hecho público su Gobierno algún documento oficial, discurso o declaración similar que resuma cómo entiende que el derecho internacional se aplica a las operaciones cibernéticas? Se ruega proporcionar copias o enlaces a dichas declaraciones.

2. ¿Se aplican las ramas del derecho internacional actual (incluidos la prohibición del uso de la fuerza, el derecho de legítima defensa, el derecho internacional humanitario y los derechos humanos) al ciberespacio? ¿Existen áreas en las cuales la novedad del ciberespacio excluye la aplicación de un conjunto específico de derechos u obligaciones legales internacionales?

3. ¿Puede una operación cibernética por sí misma constituir un uso de fuerza? ¿Puede constituir un ataque armado que genere un derecho de legítima defensa en virtud del artículo 51 de la Carta de las Naciones Unidas? ¿Puede una operación cibernética calificarse como uso de fuerza o ataque armado sin causar los efectos violentos que se han utilizado para marcar dichos umbrales en conflictos cinéticos pasados?

4. Fuera de los conflictos armados, ¿cuándo sería un Estado responsable por las operaciones cibernéticas de un actor no estatal? ¿Qué grado de control o participación debe tener un Estado en las operaciones del actor no estatal para desencadenar la responsabilidad legal internacional de ese Estado?

5. ¿Son las normas de responsabilidad del Estado las mismas u otras en el contexto de un conflicto armado tal como se define ese término en los artículos 2 y 3 comunes a los Convenios de Ginebra de 1949?

6. De acuerdo al derecho internacional humanitario, ¿puede una operación cibernética calificarse como un "ataque" de acuerdo a las normas que rigen la conducción de las hostilidades si no causa muerte, lesión ni daño físico directo al sistema informático en cuestión o a la infraestructura que apoya? ¿Podría una operación cibernética que produce solo una pérdida de funcionalidad, por ejemplo, calificarse como un ataque? Si es así, ¿en qué casos?

7. ¿Estaría una operación cibernética que solamente ataca datos regulada por la obligación de derecho internacional humanitario de dirigir ataques solamente contra objetivos militares y no contra objetivos civiles?

8. ¿Es la soberanía una norma discreta del derecho internacional que prohíbe a los Estados participar en operaciones cibernéticas específicas? Si es así, ¿esa prohibición cubre las operaciones cibernéticas que se encuentran por debajo del umbral de uso de la fuerza y que, aparte de eso, no violan el principio de no intervención?

9. ¿Es la diligencia debida una norma de derecho internacional que los Estados deben acatar en el ejercicio de su soberanía sobre las tecnologías de la información y la comunicación en sus territorios o bajo el control de sus nacionales?

10. ¿Existen otras reglas de derecho internacional que su Gobierno considere importante tener en cuenta al evaluar la regulación de las operaciones cibernéticas por parte de los Estados o actores por las que un Estado tenga responsabilidad en el ámbito internacional?