95º PERÍODO ORDINARIO DE SESIONES
31 julio - 9 agosto de 2019
Rio de Janeiro, Brasil

OEA/Ser. Q
CJI/doc.594/19
24 julio 2019
Original: inglés

TERCER INFORME

DERECHO INTERNACIONAL Y OPERACIONES CIBERNÉTICAS DEL ESTADO: MEJORANDO LA TRANSPARENCIA

(Presentado por el doctor Duncan B. Hollis)

1. El presente es mi Tercer Informe sobre el tema de mejora de la transparencia con respecto a la forma en que los Estados Miembros comprenden la aplicación del derecho internacional a las operaciones cibernéticas del Estado. En mi primer informe examiné el número creciente de incidentes cibernéticos ocurridos en relación con los Estados y sus representantes, así como sus consecuencias económicas, humanitarias y para la seguridad nacional.[1] Dicho informe puso de relieve la escasa visibilidad que ha tenido el derecho internacional en la reglamentación de las operaciones cibernéticas de los Estados. Es cierto que numerosos Estados han reafirmado la aplicabilidad del derecho internacional a sus actuaciones en el espacio cibernético.[2] Además, aun cuando la OEA no lo ha hecho, tres importantes organizaciones internacionales (la Asociación de Naciones del Sudeste Asiático-ASEAN, la Unión Europea y la Organización de las Naciones Unidas) también la han reafirmado.[3] No obstante, hasta la fecha los esfuerzos realizados para delinear *cómo* se aplica el derecho internacional al espacio cibernético han sido poco fructíferos.

2. En mi segundo informe puse de relieve varias áreas en las cuales las preguntas de cómo se aplica el derecho internacional a las operaciones cibernéticas han generado polémica o confusión,

---

[1] *Véase* Duncan B. Hollis, *Derecho internacional y operaciones cibernéticas del Estado: Mejorando la transparencia*, OEA/Ser. Q, CJI/doc. 570/18 (9 agosto 2018) ("Hollis, Primer Informe").

[2] *Véase* ONU, Secretario General, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, p. 19, ONU Doc. A/68/98 (24 junio 2013) ("El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable" al espacio cibernético); ONU, Secretario General, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, p. 24, ONU Doc. A/70/174 (22 de julio de 2015) (lo mismo).

[3] *Véase* ONU Res. 266, Doc. A/RES/73/266 (2 de enero de 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"); Declaración de ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (18 de noviembre de 2018) (Reafirmar 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 y reconocer la necesidad de profundizar en el estudio de cómo se aplica el derecho internacional a la utilización por los Estados de las tecnologías de la información y las comunicaciones); Declaración de la Unión Europea, ONU Primera Comisión, Thematic Discussion on Other Disarmament Measures and International Security (26 de octubre de 2018) (La Unión Europea recuerda 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.)

incluido el uso de la fuerza y las medidas de autodefensa, el derecho internacional humanitario, las contramedidas, la soberanía y la diligencia debida.[4] Los Estados han sido en gran medida reticentes a explicar sus opiniones en cuanto a si éstas y otras áreas del derecho internacional son aplicables al espacio cibernético y de qué forma. De hecho, los Estados parecen bastante renuentes a invocar textos del derecho internacional al formular acusaciones acerca de las operaciones cibernéticas de otros Estados.[5] Un pequeño grupo de Estados han emitido declaraciones generales sobre tales temas, entre los que se mencionan los comentarios más recientes del Presidente de Estonia.[6] Pero el número y especificidad de tales declaraciones no han sido suficientes para esgrimirlas como pruebas de la práctica de los Estados o de *opinio juris* en esta importante esfera.

3. Con el apoyo del Comité, en mi segundo informe detallé un plan para centrar la atención en la *transparencia* con respecto a la manera en que los Estados entienden la aplicación del derecho internacional a las operaciones cibernéticas. El Comité me apoyó para pedir a los Estados sus opiniones sobre algunas de las cuestiones jurídicas internacionales más importantes, pues hacerlo tiene varios beneficios claros para la región. Esquematizar los puntos de vista de los Estados Miembros de la OEA sobre el derecho internacional y las operaciones cibernéticas puede ser útil para determinar el grado de convergencia (o divergencia) que existe en cuanto a cuestiones clave, que van desde la autodefensa hasta la soberanía y las contramedidas. Saber en qué aspectos concuerdan los Estados puede aportar una evidencia muy necesaria para delinear las responsabilidades de los Estados en materia de derecho internacional consuetudinario en el espacio cibernético. Al mismo tiempo, la identificación de los desacuerdos puede ser igualmente importante. El hecho de divulgar públicamente dichas diferencias puede atenuar el riesgo de que los Estados operen a partir de diferentes supuestos básicos en formas que pudieran escalar hasta generar un conflicto (por ejemplo, cuando una parte considera que su operación cibernética es una contramedida no contundente, pero el Estado contra el cual se dirige la operación lo percibe como un ataque armado, que lo faculta para responder con actos enérgicos de autodefensa). También pondría de relieve las áreas en las que habría mayor necesidad de diálogo, ya sea para conciliar posiciones encontradas, aclarar el contenido de la legislación o incluso tratar de instituir reformas.

4. Aparte de sus efectos regionales, la elaboración de los puntos de vista de numerosos Estados Miembros de la OEA puede igualmente contribuir a iluminar el estado del derecho internacional en todo el mundo. La difusión pública de dichos puntos de vista coincidirá con el trabajo que se realiza en el ámbito mundial en la Primera Comisión de las Naciones Unidas, específicamente en la próxima reunión del Grupo de Expertos Gubernamentales (GEG) de la ONU, que será presidido por un experto gubernamental de Brasil.[7] Entre otras cosas, se informa que el nuevo GEG invitará a sus

---

[4].Duncan B. Hollis, *Derecho internacional y operaciones cibernéticas del Estado: Mejorando la transparencia*, OEA/Ser. Q, CJI/doc. 570/18 (21 enero 2019) ("Hollis, Segundo Informe").

[5].*Véase, p. ej.,* Dan Efrony y Yuval Shany, *A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112 AM. J. INT'L L. 583 (2018). La excepción más notable fue que el Reino Unido estuvo dispuesto a sugerir que las operaciones cibernéticas rusas constituyeron una "violación flagrante del derecho internacional." No obstante, el Reino Unido no especificó exactamente a cuáles operaciones cibernéticas se refería (en su acusación menciona varias atribuidas a la Federación de Rusia) ni qué derechos internacionales fueron vulnerados. *Véase* Comunicado de prensa del Ministerio de Relaciones Exteriores de la Mancomunidad, *UK exposes Russian cyber attacks*, 4 octubre 2018; NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 4 octubre 2018.

[6].*Véase* Kersti Kaljulaid, Presidente de Estonia, Opening Remarks for CyCon 2019, 29 mayo 2019; *véase también* Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century*, 23 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 noviembre 2016 (Estados Unidos); Harold Koh, *International Law in Cyberspace,* 54 HARV. INT'L DERECHO. J. 1, 7 (2012) (Estados Unidos).

[7].Véase ONU Doc. A/RES/73/266 (2 enero 2019) párrafo 3 (sobre el mandato del EGE). Además del nuevo EGE, también habrá un Grupo de Trabajo de Composición Abierta (GTCA) patrocinado por las Naciones Unidas que

respectivos expertos gubernamentales a ofrecer los pareceres nacionales sobre el derecho internacional en el contexto de la seguridad de la información. Cuatro de los 25 miembros del Grupo de Expertos Gubernamentales provienen de la región: Brasil, México, Estados Unidos y Uruguay. El trabajo del Comité permitirá que otros Estados hagan valer sus opiniones sin competencia ni conflicto con el trabajo del Grupo. De hecho, el esfuerzo del Comité debería complementar y apoyar el proyecto del GEG, dar lugar a una gama más amplia de puntos de vista de toda la región sobre los temas jurídicos internacionales y mejorar la comprensión que se tiene del derecho internacional en el entorno cibernético y su eficacia en la reglamentación de las relaciones entre los Estados que operan en dicho entorno. Este enfoque es, además, coherente con el que han propuesto otras organizaciones regionales. Por ejemplo, la Unión Europea ha propuesto que *todos* los Estados Miembros de la ONU "deberían presentar contribuciones nacionales sobre el tema de cómo se aplica el derecho internacional a la utilización por los Estados [de las tecnologías de la información y las comunicaciones]."[8]

5. Como indiqué en mi Segundo Informe, con la asistencia del Departamento de Derecho Internacional de la OEA y el aporte del Comité Internacional de la Cruz Roja, procedí a preparar un cuestionario para los Estados Miembros, el cual fue distribuido por dicho Departamento de Derecho Internacional en enero de 2019. El cuestionario plantea 10 preguntas, a saber:

- La primera pregunta solicita la presentación de las actuales declaraciones nacionales de cada Estado Miembro sobre el derecho internacional y el espacio cibernético.
- La segunda pregunta pide que los Estados Miembros confirmen si han identificado ciertas normas vigentes del derecho internacional que sean (o no) aplicables en el contexto cibernético.
- La tercera pregunta se refiere al uso de la fuerza (el *jus ad bellum*), consultando cuáles son los criterios que utiliza el Estado para identificar una operación cibernética como uso de la fuerza o ataque armado.
- Las preguntas cuarta y quinta consultan sobre cómo entienden los Estados la asignación de la responsabilidad jurídica internacional por el comportamiento de los agentes no estatales, en particular el grado de "control" requerido por el Estado.
- Las preguntas sexta y séptima abordan el derecho internacional humanitario (el *jus in bello*) y dos de sus temas cruciales pendientes, a saber, la definición de un "ataque" en el contexto cibernético y la cuestión de si las operaciones cibernéticas que solo involucran datos constituyen tal ataque.
- La octava pregunta recaba las opiniones de los Estados en cuanto a si la soberanía comprende su propia normativa de comportamiento del Estado en el espacio cibernético o si, por el contrario, es un principio de fondo que fundamenta el contenido de otras normas. Existen actualmente opiniones divididas entre los Estados sobre este tema.
- La novena pregunta formula una consulta similar con respecto a la diligencia debida.
- Por último, la décima pregunta invita a los Estados a identificar áreas adicionales de derecho internacional en las que el Comité debería centrar su atención para lograr una mejor transparencia en el contexto cibernético.

6. Hasta la fecha, el Comité ha recibido las respuestas de seis países a su cuestionario, a saber, Bolivia, Brasil, Costa Rica, Ecuador, Guatemala y Perú. La respuesta de Brasil puso de relieve el trabajo que dicho país tiene pendiente en el Grupo de Expertos Gubernamentales de la ONU (que

---

tratará de poner en práctica el trabajo de anteriores grupos de expertos gubernamentales y, en algunos casos, revisar o incluso enmendar los resultados de esa labor. *Véase* ONU Doc. A/RES/73/27.

[8] Declaración de la Unión Europea, *supra* nota 3.

será presidido por un experto brasileño). A su vez, en su respuesta, Costa Rica destacó la necesidad de reforzar más la capacidad respecto a la manera como el derecho internacional se aplica a las operaciones cibernéticas, así como a la posibilidad de que el Comité emprenda el trabajo de elaborar reglamentos jurídicos internos para hacer frente a las amenazas cibernéticas. Las otras cuatro respuestas se refirieron específicamente a las preguntas formuladas por el Comité. He adjuntado las seis respuestas a este informe para su examen por el Comité.

7. En este Tercer Informe, no ofrezco ningún análisis sustantivo o sumatorio de las respuestas recibidas hasta la fecha. Lo que pretendo, antes bien, es simplemente poner al día al Comité sobre la situación actual. También quisiera invitar a los miembros del Comité que representan a los Estados que todavía no han respondido al cuestionario antes aludido a que alienten a sus gobiernos nacionales a hacerlo.

8. Según entiendo, otros Estados están trabajando en la preparación de sus respuestas. En tal sentido, creo que sería mejor tener un conjunto más completo de respuestas antes de emprender el análisis de cómo interpretan los Estados Miembros de la OEA la forma en que se aplica el derecho internacional en general al espacio cibernético, o a las operaciones cibernéticas en particular. Además, la Secretaría Ejecutiva del Comité Interamericano contra el Terrorismo (CICTE) de la OEA celebrará consultas con la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA) los días 15 y 16 de agosto de 2019.[9] En tales consultas probablemente se aborden la utilidad del trabajo del Comité, así como algunos de los temas jurídicos internacionales de fondo en los que procura aumentar la transparencia. A tal efecto, dichas consultas aportan una justificación adicional para esperar antes de ofrecer un análisis detallado de los puntos de vista de los Estados Miembros.

9. En mi próximo informe, me propongo sintetizar el modo en que los Estados Miembros que emitan respuestas comprenden que se aplica el derecho internacional a las operaciones cibernéticas de los Estados. Procuraré hacerlo teniendo presente la continua labor de la ONU (incluido el GEG, que comenzará a reunirse formalmente en diciembre, pero también un nuevo Grupo de Trabajo de Composición Abierta (GTCA), que iniciará funciones en septiembre de 2019), planteando la pregunta de cómo dicha labor puede influir, si es que lo hace, en nuestra comprensión de las respuestas de los Estados Miembros.

10. Según lo expresado al comienzo, no preveo que este proyecto se traduzca en un esfuerzo para codificar o desarrollar gradualmente el derecho internacional (y ni siquiera en un intento de definir las mejores prácticas o directrices generales). El objetivo sigue siendo más bien uno modesto: ofrecer a los Estados Miembros de la OEA una plataforma para una acción más transparente sobre cómo entienden ellos que se aplica el derecho internacional al entorno cibernético y a las tecnologías de la información y las comunicaciones de las cuales se deriva. Espero con interés escuchar los puntos de vista del Comité y aportar sugerencias sobre cómo asegurar una mayor transparencia en lo que hoy en día se reconoce ampliamente como una de las principales prioridades de los Estados nacionales.

[9]. Esta consulta es una de las varias que celebrará la UNODA este verano [boreal] con varios organismos regionales de todo el mundo, incluidas la Organización para la Seguridad y la Cooperación en Europa (OSCE), la ASEAN y la UE.