93º PERÍODO ORDINARIO DE SESIONES
6 al 16 de agosto 2018
Rio de Janeiro, Brasil

OEA/Ser. Q
CJI/doc.570/18
6 julio 2018
Original: inglés

DERECHO INTERNACIONAL Y OPERACIONES CIBERNÉTICAS DEL ESTADO: MEJORANDO LA TRANSPARENCIA

(presentado por el doctor Duncan B. Hollis)

Antecedentes

1. Las amenazas a la seguridad cibernéticas han ganado ubicuidad. Hoy en día, los ataques cibernéticos por actores estatales y no estatales – incluyendo las disrupciones de infraestructura, el robo de datos y de la propiedad intelectual en grande escala, el hackeo hacia los actores políticos y procesos electivos – están generando pérdidas significativas. Estas pérdidas se producen, además, a través de una variedad de medidas, incluyendo la seguridad nacional, los derechos humanos y la economía.

2. En 2017, algunas de las herramientas más sensibles en el campo del hackeo utilizados por la Agencia Nacional de Seguridad de los Estados Unidos y la Agencial Central de Inteligencia fueron sustraídas y lanzadas en la internet.[1] Esas herramientas fueron reformuladas para lanzar ataques globales de secuestro de datos tales como el WannaCry, que infectó a cientos de miles de redes de computadoras en 150 países, con pérdidas que totalizaron hasta 4.000 millones de dólares.[2] Más notablemente, el WannaCry condujo al cese temporario de las operaciones no emergenciales en los hospitals del Servicio Nacional de Salud del Reino Unido.[3] El ataque cibernético subsecuente llamado NotPetya puede haber sido diseñado para alcanzar a Ucrania (habiendo ocasionado interruciones en sus hospitales, compañías de electricidad, aeropuertos y en el banco central), pero impactó a otros 64 países, incluyendo a varios Estados Miembros de la OEA. Empresas tales como FedEx, Maersk, y Merck experimentaron pérdidas de cientos de millones de dólares, mientras que se vio afectada la infraestructura principal, tales como los puertos de Argentina.[4] Programas malignos tales como el "BlackEnergy" han dejado desconectadas a las estaciones de electricidad en Ucrania, mientras que una variante más reciente conocida como "Triton" o "Trisis" penetraron los controles de seguridad de sistemas industriales de larga escala en Arabia Saudita, de tal manera que, si no fuera por un pequeno error de programación, había llevado a la pérdida de vidas.[5] Mientras tanto, los procesos electorales en los Estados Unidos y Francia han sido afectados por los piratas informáticos *(hackers)* y existe la preocupación de que esta práctica será replicada por todo el continente

[1] Lily Hay Newman. *The Biggest Cybersecurity Disasters of 2017 So Far,* WIRED, Julio 1, 2017.
[2] Jonathan Beer. *"WannaCry" ransomware attack losses could reach $4 billion,* CBS NEWS, Mayo 16, 2017.
[3] *Id.*; Damien Gayle et al., *NHS seeks to recover from global cyber-attack as security concerns resurface*, THE GUARDIAN, Mayo 13, 2017.
[4] Newman, *supra* note 1; Conner Forrest, *NotPetya ransomware outbreak cost Merck more than $300M per quarter*, TECHREPUBLIC, Oct. 30, 2017.
[5] *Ver, por ej.,* Chris Bing. *Trisis has the security world spooked, stumped and searching for answers,* CYBERSCOOP, Jan. 16, 2018*;* Blake Johnson et al, *Attackers Deploy New ICS Attack Framework "TRITON" and cause Operational Disruption to Critical Infrastructure,* FIREEYE BLOG, Dic. 14, 2017; Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, Marzo 3, 2016.

americano.[6] En pocas palabras, el status quo de la seguridad cibernética es precario y se está deteriorando.

3. Los Estados nacionales, mientras tanto, están desarrollando en forma creciente sus capacidades para introducirse en las operaciones cibernéticas. Estos esfuerzos incluyen medidas defensivas y versiones de espionaje por medios cibernéticos. Pero también se incluyen operaciones cibernéticas "ofensivas" que pueden generar pérdidas de funcionalidad o daños físicos a la infraestructura y a otros sistemas soportados por las redes de computadoras. Actualmente, alrededor de 30 Estados han acometido, según se sabe, el desarrollo de capacidades ofensivas cibernéticas.[7] Los Estados parecen favoracer tales operaciones, tanto como una manera de complementar (o incluso de sustituir) los medios y métodos bélicos tradicionales, pero también como una forma de involucrar de manera consistente a los adversarios que carezcan de conflictos armados cinéticos. En otros casos, los Estados han hecho uso de "procuradores" para asumir las operaciones cibernéticas, a veces bajo el control del Estado mismo o simplemente con señales públicas o privadas adicionales de apoyo estatal.[8]

El derecho internacional y las operaciones cibernéticas

4. ¿Cómo es que el derecho internacional regular las operaciones cibernéticas estatales y patrocinadas por el Estado? Hasta la fecha, se ha producido tan solo un avance limitado en la respuesta a esta pregunta. En 2013, un Grupo de Expertos Gubernamentales de las Naciones Unidas (el "GEG" de la ONU), incluyendo a especialistas de quince gobiernos, adoptó un informe consensual indicando que el "derecho [i]nternacional, y en particular la Carta de las Naciones Unidas, son aplicables y son esenciales para mantener la paz y la estabilidad, y para promover un ambiente de información y comunicación tecnológica (CIT) abierto, seguro, pacífico y accesible."[9] Este punto de vista fue confirmado por otro GEG de la ONU en 2015, que también endosó una serie de normas voluntarias (es decir, no vinculantes legalmente) para una conducta responsable del Estado[10] es decir, que los Estados, durante épocas de paz, tengan bajo su mira las infraestructuras cruciales o el trabajo de los equipos de respuesta a incidentes en el area de la seguridad computacional (CSIRTs).[11]

5. Lamentablemente, buena parte del *momentum* del GEG se perdió en 2017, cuando el ultimo GEG dejó de generar informes. Los veinte especialistas gubernamentales que participaban en el mismo estuvieron aparentemente en desacuerdo sobre si ciertos regímenes de derecho internacional (por ejemplo,

---

[6] *Ver, por ej.,* Adam Nossiter, David E. Sanger, and Nicole Perlroth, *Hackers Came, but the French Were Prepared*, NEW YORK TIMES, Mayo 9, 2017; Kim Willsher, and Jon Henley, *Emmanuel Macron's campaign hacked on eve of French election,* THE GUARDIAN, Mayo 6, 2017.

[7] Steve Ranger. *US Intelligence: 30 Countries Building Cyber Attack Capabilities*, ZD NET, enero 5, 2017.

[8] *Ver en general* Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (2018).

[9] *Ver* del Secretario General de la ONU. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 19, U.N. Doc. A/68/98 (Junio 24, 2013).

[10] Secretario General de la ONU. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 10, U.N. doc. A/70/174 (julio 22, 2015) ["*2015 GGE Report*"]. "El proceso del GEG no es, por supuesto, el único vehículo para la cooperación interestatal en ciberseguridad. En 2015, por ejemplo, el presidente de los EE. UU., Barack Obama, y el presidente chino, Xi Jinping, anunciaron un "entendimiento común" sobre ciberespionaje, es decir, un compromiso político. Acordaron que ni el gobierno de los EE. UU. ni el de China "llevarán a cabo o apoyarán a sabiendas el robo de la propiedad intelectual con fines cibernéticos, incluidos los secretos comerciales u otra información comercial confidencial, con la intención de proporcionar ventajas competitivas a empresas o sectores comerciales". *Ver* OFFICE OF PRESS SEC'Y, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT TO THE UNITED STATES (2015). Este principio fue luego endosado por el G-20. *Ver* G-20 Leaders' Communiqué, *Antalya Summit*, (nov. 15–16, 2015), 26, http://www.mofa.go.jp/files/000111117.pdf.

[11] *Ver 2015 GGE Report, supra* note 13(h), (k).

el derecho internacional humanitario, las contramedidas, la diligencia debida) eran aplicables a las operaciones cibernéticas de los Estados.[12] Según el especialista de los EE.UU. en las negociaciones,

> "a [p]esar de años de discusiones y estudio, algunos participantes … parecen querer retroceder en lo que hace a los avances en los informes previos del GEG. Llego a la lamentable conclusión de que aquellos que no desean afirmar la aplicabilidad de estas normas legales y principios internacionales, creen que sus Estados tienen libertad de actuar en o a través del ciberespacio para conseguir sus fines políticos sin limitación o restricción alguna en lo que hace a sus actos.[13]

6. Con el retroceso del GEG, los esfuerzos para identificar cómo se aplica el derecho internacional a la conducta de los Estados en el ciberespacio se han trasladado a otros foros. Algunos esfuerzos enfocan la necesidad de una nueva legislación, tal como el llamado del Presidente de la Microsoft, Brad Smith, con relación a una "Convención Digital de Ginebra"[14]. Más recientemente, una *Comisión Global sobre la Estabilidad del Ciberespacio* ha propuesto varias "normas" innovadoras convocando a los Estados para que prometan no interferir con el "núcleo público" de la internet o con procesos electorales de otros estados.[15]

7. Hasta la fecha, sin embargo, los Estados han trabajado relativamente poco en forma colectiva para articular cómo el derecho internacional regula en la *actualidad* la conducta del Estado en el ciberespacio. Una reunión del "grupo independiente de especialistas" patrocinado por la OTAN en Tallim, Estonia, produjo dos manuales sobre derecho internacional y ciberespacio. El primer *Manual de Tallinn* abordó cómo el derecho internacional se aplica a la guerra cibernética (esto es, la prohibición del uso de la fuerza y el derecho internacional humanitario).[16] El segundo, *Manual de Tallinn 2.0*, expandió el tratamiento para abordar otras áreas del derecho internacional que regulan las ciberoperaciones estatales, incluyendo el deber de no intervención, soberanía y diligencia debida.[17] Ambos manuales constituyen importantes obras de referencia y los gobviernos fueron consultados durante su preparación. Pero a pesar de todas las opiniones especializadas producidas, los *Manuales Tallinn* permanecen como la obra de individuos privados. Como máximo, son una fuente "subsidiaria" de derecho internacional y no pueden ser considerados fuentes primarias tales como los tratados, la costumbre y los principios generales del derecho.

8. Además, por más valiosos que sean, los contenidos de los *Manuales Tallin* son con frecuencia objeto de controversia o ambiguos. Por ejemplo, el *Tallinn 2.0* describe a la "soberanía" no solo como un principio que establece la autoridad del Estado de controlar su territorio y población, sino

---

[12] Arun M. Sukumar. *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well,* LAWFARE, julio 4, 2017.

[13] Michele Markoff. U.S. Expert to the Group of Governmental Experts, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security* (Junio 23, 2017), https://usun.State.gov/remarks/7880.

[14] *Ver* Brad Smith. *The Need for a Digital Geneva Convention*, MICROSOFT BLOG (Feb. 14, 2017). En interés de una amplia publicación, estoy ahora consultando con la Microsoft sobre este Proyecto. Por tanto, sin embargo, mi actual proopuesta enfoca la clarificación de las normas existentes del derecho internacional para el ciberespacio y no propuestas de nueva legislación, ya que veo esto como proyectos separados. Como tal, no creo existir conflicto de intereses en mi actividad sobre este tema en el CJI. Habiendo dicho esto, por supuesto voy a adherirme a las opiniones del Comité en caso de conflict de intereses.

[15] *Ver, por ej.*, Global Comm'n on the Stability of Cyberspace, *Global Commission Proposes Call to Protect the Public Core of the Internet* (Nov. 21, 2017), disponible en https://cyberstability.org/news/global-commission-proposes-action-to-increase-cyberspace-stability/. Para detalles sobre la composición y mission del GCSC, ver https://cyberstability.org/.

[16] *Ver* Michael Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: NATO CCD COE, 2013).

[17] Michael Schmitt, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn, Estonia: NATO CCD COE, 2017).

como una "regla" que puede ser violada por las ciberoperaciones de otro Estado.[18] *Si* la soberanía constituye una regla, debería establecer bases para que un Estado promueva una queja cuando otro Estado (o actores por los cuales el Estado se responsabiliza) llevan a cabo ciberoperaciones que afecten a sus ciudadanos o a suas propiedades. Por ejemplo, ello constituiría la base para pensar que el cibersecuestro de datos tales como el WannaCry o los *malwares* tales como Triton/Trisis efectivamente infringieron la soberanía de los Estados víctimizados.

9. Parece, sin embargo, que varios Estados no aceptan (aun) la visión de la soberanía como uma regla, prefiriendo identificarla como um principio que informa el contenido de otras reglas (por ejemplo, el deber de no intervención), mas no como un medio directo de regulación de la conducta de un Estado. El Abogado General del Reino Unido adoptó esta posición en un discurso proferido en Mayo de 2018.[19] El abogado en jefe del Cibercomando de los EEUU también apoyó la idea de la soberanía como principio (aunque refiriéndose a ella como una capacidad privada).[20] Como tal, existe una cuestión abierta sobre si la soberanía se aplica incluso en la restricción de las ciberoperaciones de los Estados. Han surgido debates "existenciales" similares sobre la disponibilidad de otras "reglas" propuestas para las ciberoperaciones (por ej., el derecho internacional humanitario, la diligencia debida, las contramedidas).

10. Pero aunque existe acuerdo sobre la aplicación de una regla específica a las ciberoperaciones, sus contornos y significado son con frecuencia ambiguos. Por ejemplo, los especialistas de los *Manuales Tallinn*, a pesar de que concuerdan con la soberanía como uma regla, no pudieron llegar a un acuerdo si una ciberoperación que causa remotamente uma pérdida de funcionalidad en la infraestructura cibernética viola la regla en caso de que no requiera el reemplazo físico de cualquier parte de la computadora o de la infraestructura que lo apoya. Han surgido cuestiones similares sobre cómo regular las ciberoperaciones que afectan la funcionalidad sin provocar efectos físicos en las interpretaciones opuestas sobre lo que constituye un "ataque" para los fines del derecho internacional humanitario (es decir, la exigencia de que los Estados en un conflicto armado deben abstenerse de "atacar" a los civiles, debiendo solo "atacar" a los objetivos militares, donde cualesquiera pérdidaa civiles son proporcionales a las ventajas militares obtenidas). Algunos, incluyendo a la mayoría de los especialistas de los *Manuales Tallinn*, interpretan que el umbral del "ataque" exige el daño físico o la destrucción equivalente de los tipos de operaciones cinéticas que han previamente calificado como ataques.[21] Otros, tales como el Comité Internacional de la Cruz Roja, argumentan que el concepto de "ataque" debe expandirse, dadas las novedosas caracteristicas de las tecnologías de la información y de la comunicación, de incluir las pérdidas de funcionalidad aún cuando no se produzcan daños físicos (por ej., en lugar de hacer volar una red energética, hackearla de manera temporaria, interrumpiendo así el sistema).[22]

---

[18] *Id.*, en la Regla 4 ("Un Estado no debe realizer ciberoperaciones que violan la soberanía de otro Estado.").

[19] *Ver, por ej.,* Jeremy Wright QC, MP, *Cyber and International Law in the 21st Century*, Mayo 23, 2018, en https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[20] *Ver* Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017).

[21] *Ver Tallinn 2.0, supra* nota 17, en 417 (mayoría aceptó la idea de que una pérdida de funcionalidad constituye daño solo si el mismo "require reemplazo de components físicos").

[22] *Ver, por ej.,* International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* 32nd International Conference of the Red Cross and Red Crescent (Oct. 2015) 40-41 ("2015 ICRC Report").

11. Deesta forma, parecen existir dos grupos de problemas distintos con la actual aplicación del derecho internacional al ciberespacio. En primer lugar, existen "problemas de aplicación" donde no resulta claro qué reglas se aplican a las ciberoperaciones de los Estados. En segundo lugar, existen "problemas interpretativos" donde se aplica la presunción de una regla, siendo sus contornos y significado oscuros o conflictivos.

12. Mas un tercer problema es inminente también con relación a la aplicación del derecho internacional al ciberespacio – al cual yo denominaría de un "problema relativo a la obligatoriedad de rendir cuentas". Recientemente, los Estados y otros actores han comenzado a responsabilizar a los Estados por ciertas ciberoperaciones (previamente, la atribución de los ciberataques era considerada como siendo o demasiado difícil técnicamente o que no valía los costos de la divulgación pública).[23] Los Estados Unidos acusaron a Corea del Norte de ser responsables en el caso del hackeamiento de Sony Pictures.[24] Se unieron luego al Reino Unido para acusar también a Corea del Norte de ser responsable del WannaCry.[25] Junto con algunos otros Estados, estos dos Estados acusaron a la Federación Rusa de ser responsable por el NotPetya.[26]

13. Al formular estas acusaciones, sin embargo, los Estados han evitado a todas luces invocar el derecho internacional. Ninguna de las acusaciones menciona ni al menos trata de verificar cómo regula el derecho internacional tal tipo de conducta.[27] De resultas de ello, existe hoy en día un escaso deber de rendir cuentas en el caso de la conducta de un Estado con relación al ciberespacio.

13a. Tomados en su conjunto, estos problemas sobre la aplicación, interpretación y responsabilidad complican cualquier tentativa de aplicar el derecho internacional a las operaciones cibernéticas. Incluso si un Estado posee sus propios puntos de vista sobre qué leyes se aplican y lo que ellas significan con relación a sus ciberoperaciones, no resulta claro que el Estado alcanzado por dicha operación vaya a compartir tales puntos de vista. Esto da lugar a una possible sucesión de conflictos no intencionados (por ejemplo, donde un Estado comprende que sus operaciones no constituyen un uso de la fuerza, mientras que el Estado en foco sí lo considera y responde en defensa propia). Por otro lado, dicho silencio estatal torna difícil el desarrollo del derecho consuetudinario internacional. Como los Estados se niegan a articular sus puntos de vista y plasmarlos en una *opinio juris* para casos específicos, se hace difícil identificar las reglas consuetudinarias, y menos aún aplicarlas.

Una modesta propuesta: preguntando a los Estados sobre sus puntos de vista con relación al derecho internacional

14. El hecho de que los Estados se muestren reacios a identificar sus puntos de vista sobre el derecho internacional con respecto a casos específicos, no significa que deban guardar silencio sobre la aplicación del derecho internacional al ciberespacio de manera más general. Ya sea que uno esté de acuerdo con el Procurador General del Reino Unido o no, es útil saber cómo el Reino Unido considera las reclamaciones de soberanía como regla para las operaciones cibernéticas. Del mismo modo, en 2012, los Estados Unidos ofrecieron una serie de respuestas a preguntas básicas sobre la aplicación del derecho

---

[23] *Ver* Duncan B. Hollis. *An e-SOS for Cyberspace,* 52 HARVARD INT'L L. J. 374 (2011).

[24] David E. Sanger and Nicole Perlroth. *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES, Dic. 17, 2014.

[25] Nate Lanxon & Tim Ross. *U.K. Blames North Korea for WannaCry Attack on Health Service*, BLOOMBERG, Oct. 26, 2017; *U.S. blames North Korea for 'WannaCry' cyber attack*, REUTERS, Dic. 18, 2017.

[26] Sarah Marsh. *US joins UK in blaming Russia for NotPetya cyber-attack*, THE GUARDIAN, Feb. 15, 2018.

[27] Con relación al hackeo de Sony Pictures, el Presidente Obama declinó clasificar al incidente como violación del derecho internacional, pero se refirió al mismo como un ataque de "cibervandalismo." Brian Fung. *Obama called the Sony hack an Act of "Cyber-Vandalism*, WASH. POST, Dic. 22, 2014. Un reciente studio académica de los incidentes cibernéticos más significativos afirma la negative consistente de los estados en aplicar el derecho internacional a las ciberoperaciones por las cuales un Estado puede ser responsabilizado. *Ver* Dan Efrony and Yuval Shany. *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, SSRN (2018).

internacional al ciberespacio, en un discurso que fue ampliamente divulgado por el entonces asesor jurídico del Departamento de Estado, Harold Koh[28]. Dichas declaraciones pueden contribuir a identificar y comprender las reglas de derecho internacional relevantes para los Estados con relación al ciberespacio. Mejoran la transparencia de cómo los Estados individuales ven el derecho internacional, lo cual -si compartido por un número suficiente de Estados adicionales- puede conducir a la identificación del derecho internacional consuetudinario. Al mismo tiempo, estas declaraciones tienen importancia práctica: señalan a otros Estados cómo un Estado trata de administrar y desplegar sus propias operaciones cibernéticas o cómo responder a las de otros Estados. Dicha transparencia puede mitigar potencialmente las consecuencias involuntarias o escaladas derivadas de operaciones cibernéticas por parte de Estados, o de aquellos cuyo comportamiento des atribuíble a un Estado.

15. Por lo tanto, quien les habla y escribe, propondría que el CJI emprendiese un nuevo proyecto: solicitar, recopilar y publicitar las opiniones de los Estados Miembros sobre la aplicación del derecho internacional a las operaciones cibernéticas. Esto se basaría en declaraciones *ad hoc* que han sido emitidas por funcionarios del gobierno hasta la fecha. Pero en lugar de diseminar estos puntos de vista en el tiempo y en el lugar, nuestro Comité bien podría compilar una colección de respuestas de los Estados Miembros sobre algunas de las cuestiones jurídicas internacionales más importantes en un área - la ciberseguridad - que se ha convertido en una prioridad nacional para todos los Estados de la región.

16. Creo, además, que la OEA se encuentra en una posición única entre las organizaciones internacionales para llevar a cabo tal proyecto. Como se ha señalado, los esfuerzos globales en las Naciones Unidas han vacilado porque ciertos Estados tienen visiones fundamentalmente diferentes sobre el ciberespacio y el papel de los Estados en el mismo. Otras organizaciones regionales, como la OSCE (Organización para la Seguridad y la Cooperación en Europa) y el Consejo de Europa, se han estancado debido a desacuerdos similares entre los Estados Miembros. Por el contrario, los Estados Miembros de la OEA comparten un compromiso con los valores democráticos y el estado de derecho. Como tal, la OEA es quizás la única organización internacional regional que podría ofrecer un conjunto de puntos de vista sobre cómo el derecho internacional se aplica a las operaciones cibernéticas. En la medida en que las respuestas de los Estados Miembros se ajusten a las declaraciones existentes sobre derecho internacional ofrecidas en el GEG de las Naciones Unidas o en otro foro, estas respuestas aportarían una contribución importante al señalar que tales declaraciones cuentan con un amplio respaldo. Y allí donde Estados Miembros de la OEA ofrezcan puntos de vista consistentes sobre asuntos legales internacionales, que no se han expresado previamente, podrán presentar argumentos sólidos para tratar tales opiniones como un reflejo del derecho internacional consuetudinario no solo en la región, sino en todo el mundo.

17. Dicho esto, no me es posible anticipar que los Estados Miembras ofrezcan siempre respuestas similares a las preguntas clave pendientes sobre el derecho internacional y las operaciones cibernéticas. No obstante, existe incluso suficiente valor en identificar casos en que los Estados Miembros ofrecen puntos de vista no compatibles. Será posible mapear áreas de convergencia y divergencia. Sabiendo en qué discrepan los Estados, se pueden resaltar áreas que necesitan mayor diálogo o atención, ya sea para cerrar estas brechas, articular aclaraciones o buscar modificaciones para asegurar que la ley internacional pueda ser más efectiva en la regulación del comportamiento real del Estado en el ciberespacio.

18. En resumen, solicito la aprobación del Comité para redactar y enviar un cuestionario a los Estados Miembros, solicitando sus puntos de vista oficiales sobre algunas de las cuestiones clave que han surgido con respecto a la aplicación del derecho internacional a operaciones en ciberespacio por Estados o por aquellos actores respecto de los cuales un Estado podría ser internacionalmente responsable. También estoy buscando la aprobación del Comité para plantear este tema con los Asesores Legales del Ministerio de Relaciones Exteriores durante nuestra reunión del 15 de agosto de 2018. La receptividad de estos

[28] *Ver* Harold Hongju Koh. Asesor Legal del Departamento de Estado de los EE.UU. *International Law in Cyberspace,* USCYBERCOM Inter-Agency Legal Conference, Sept. 18, 2012, *disponible en* https://2009-2017.State.gov/s/l/releases/remarks/197924.htm.

asesores legales a la idea de un cuestionario será un indicador importante del éxito de la propuesta de proyecto en su conjunto. Dicho diálogo puede también identificar ciertos temas que son (o no) fructíferos para la atención como parte de cualquier esfuerzo para mejorar la transparencia de la aplicación del derecho internacional en el ciberespacio.

19. Para facilitar el debate, adjunto un proyecto de lista de 20 preguntas que propongo que el Comité someta a la consideración de los Estados Miembros. Son similares al tipo de preguntas sobre las cuales ya algunos Estados (por ejemplo, los Estados Unidos) han ofrecido puntos de vista. Sin embargo, son más detalladas y numerosas que las generalmente producidas por el Comité. No obstante, creo que vale la pena formular estas preguntas. Sin embargo, será importante comunicar a los Estados Miembros que sus propias respuestas constituyen el producto deseado del trabajo del Comité. El valor de este proyecto radica en que los Estados sean más transparentes en la forma en que entienden el derecho internacional para operar en este espacio. Por lo tanto, tendremos que trabajar como Comité, en conjunto con el Departamento de Derecho Internacional, para dar a luz a más (y más detalladas) respuestas que las que hemos recibido en otros contextos.

20. Si el Comité aprueba este tema, quien les habla se ofrece a trabajar con la Secretaría para identificar una serie de preguntas apropiadas que podrían plantearse a los Estados Miembros durante este otoño, de modo que el Comité pueda recopilar y analizar las respuestas el próximo año y, con la aprobación de la Asamblea General, publicar los resultados dentro de la región y más allá de ella.

[PROYECTO]

20 PREGUNTAS PARA LOS ESTADOS MIEMBROS

SOBRE EL DERECHO INTERNACIONAL Y LAS CIBEROPERACIONES

La aplicación del derecho internacional en general

1. ¿Se aplican las reglas existentes del derecho internacional al ciberespacio?
2. ¿Existen áreas donde la novedad del ciberespacio excluye la aplicación del derecho internacional?

Las ciberoperaciones y el uso de la fuerza

3. ¿Puede una ciberoperación ser considerada por sí sola como uso de la fuerza o una amenaza de uso de la fuerza? ¿Bajo qué condiciones son las ciberoperaciones consideradas cómo "fuerza"?

4. ¿Puede una ciberoperación ser considerada por sí sola como un ataque armado, justificando una respuesta como autodefensa según el Artículo 51 de la Carta de la ONU o el Artículo 22 de la Carta de la OEA?

   i. ¿Bajo qué condiciones puede una ciberoperación ser considerada un ataque armado?

   ii. ¿Podría ser así considerada si [la ciberoperación] interrumpiese una infraestructura crucial sin causar los tipos de efectos violentos que califican como ataque armado en el contexto cinético?

5. ¿Puede la ciberoperación de un actor de un Estado que no es parte ser considerada como uso de la fuerza o como ataque armado? ¿Qué nivel de control o participación debe presentar un Estado a fin de ser considerado responsable de tal operación, en conformidad con el derecho internacional?

Las ciberoperaciones el derecho iternacional humanitario (DIH)

6. ¿Pueden las ciberoperaciones constitutir por sí solas un conflicto armado? ¿Existe algún nivel de intensidad requerido para que una ciberoperación así lo constituya?

7. ¿Allí donde existe un conflicto armado, son de aplicación las reglas del DIH a las ciberoperaciones de un Estado?

8. ¿Cuándo son aplicables las reglas del DIH a las ciberoperaciones realizadas por un actor no estatal?

9. ¿Cuándo se considera que una ciberoperación constituye un ataque según el DIH?

   i. ¿Puede una ciberoperación ser considerada un ataque cuando no causa ningún daño físico directo al sistema computacional o a la red de que es objeto?

   ii. ¿Podría, por ejemplo, considerarse como ataque un cibersecuestro de datos?

   iii. ¿Puede una pérdida de funcionalidad por sí sola constituir un ataque?

   iv. ¿Acaso los datos por sí solos son considerados como objetivo militar sujetos a un ataque según las normas del DIH?

10. ¿En qué casos pueden un sistema computacional o una red ser considerados un objetivo militar? ¿Puede ser considerados un objetivo militar un sistema computacional o una red principalmente utilizados para fines civiles?

El deber de no intervención

11. ¿Es aplicable el deber de no intervención a las ciberoperaciones de un Estado o de los actores respecto de los cuales un Estado sería internacionalmente responsable?

12. ¿Qué tecnología de la información y de la comunicación o infraestructura están protegidos por el deber de no intervención (es decir, cuáles de ellos son considerados *domain réservé*)?

13. ¿En qué casos una ciberoperación constituiría una coerción según el deber de no intervención?

14. ¿Pueden las ciberoperaciones que tienen como blanco a las campañas políticas o a los procesos electorales de un estado violar el deber de no intervención? ¿En qué circunstancias podrían ser violatorias de tales campañas o procesos?

Soberanía

15. ¿Constituye la soberanía una regla del derecho internacional que prohíbe a los Estados se involucrarse en ciberoperaciones específicas?

16. En caso positivo, ¿qué ciberoperaciones podrían ser limitadas por esta regla? ¿Podrían, no obstante, las operaciones que no poseen efectos físicos directos en el territorio de un Estado violar su soberanía?

17. Caso la soberanía sea considerada como una regla del derecho internacional ¿puede la ciberacción de un actor no estatal violar la soberanía de un Estado?

Diligencia debida

18. ¿Puede acaso la diligencia debida ser considerada como regla del derecho internacional que los Estados deben respetar en el ejercicio de su soberanía sobre su territorio y sus nacionales?

19. En caso positivo, ¿bajo qué circunstancias podría esperarse que un Estado ejercite la diligencia debida con relación a una conducta de (a) otros Estados en su territorio; (b) actores no estatales, incluyendo (c) sus propios nacionales?

Otras reglas del derecho internacional

20. ¿Existen otras reglas del derecho internacional que deban destacarse al evaluar las ciberoperaciones realizadas por parte de los Estados o de los actores por los cuales un Estado es responsable internacionalmente?

*** * ***