Naciones Unidas S/2021/540

Consejo de Seguridad

Distr. general
8 de junio de 2021
Español
Original: inglés

Carta de fecha 8 de junio de 2021 dirigida al Secretario General por el Representante Permanente de Estonia ante las Naciones Unidas

Estonia, que ocupa la Presidencia del Consejo de Seguridad durante el mes de junio, tiene la intención de celebrar el martes 29 de junio de 2021 a las 8.00 horas (hora de verano de Nueva York) un debate abierto de alto nivel sobre el tema “Mantener la paz y la seguridad internacionales en el ciberespacio”, en relación con el asunto “Mantenimiento de la paz y la seguridad internacionales”.

A fin de orientar la discusión sobre el tema, Estonia ha preparado la nota conceptual adjunta (véase el anexo).

Le agradecería que tuviera a bien hacer circular la presente carta y su anexo como documento del Consejo de Seguridad.

(*Firmado*) Sven **Jürgenson**
Embajador y
Representante Permanente

21-07545 (S) 10621 150621

Anexo de la carta de fecha 8 de junio de 2021 dirigida al Secretario General por el Representante Permanente de Estonia ante las Naciones Unidas

Nota conceptual para el debate abierto del Consejo de Seguridad sobre el tema “Mantener la paz y la seguridad internacionales en el ciberespacio”, que se celebrará el 29 de junio de 2021

I. Objetivo

1. Con este debate abierto se pretende contribuir a que se entiendan mejor los crecientes riesgos que plantean las actividades maliciosas en el ciberespacio y su repercusión para la paz y la seguridad internacionales, así como abordar las iniciativas mundiales encaminadas a promover la paz y la estabilidad en el ciberespacio. Será una oportunidad para que los Estados Miembros reafirmen su adhesión al derecho internacional y al marco de comportamiento responsable de los Estados como elementos clave de la prevención de conflictos y el mantenimiento de la paz y la seguridad en el ciberespacio.

II. Antecedentes

2. De conformidad con la Carta de las Naciones Unidas, la responsabilidad primordial del Consejo de Seguridad es mantener la paz y la seguridad internacionales. En consonancia, el Consejo ha seguido de cerca la evolución de los desafíos para la seguridad internacional abordando diversos factores complejos nuevos que pueden desestabilizar a los países y empeorar o prolongar los conflictos. A lo largo de los años el Consejo ha celebrado tanto debates temáticos amplios sobre los desafíos nuevos para la paz y la seguridad internacionales como reuniones dedicadas a cuestiones concretas, como el cambio climático, los recursos naturales, las pandemias, la hambruna, la delincuencia organizada transnacional, el tráfico de drogas y la piratería.

3. Aunque el Consejo de Seguridad tratará por primera vez la ciberseguridad como tema aparte en este debate abierto, ya ha tratado el tema en diversas sesiones oficiosas y en el marco de un debate más amplio sobre la seguridad internacional. Estas sesiones han dejado patente que para muchos países las ciberamenazas son motivo de preocupación y un desafío importante en materia de seguridad. Por ejemplo, en diciembre de 2017, durante la presidencia del Japón, el Consejo celebró un debate abierto sobre cómo hacer frente a los complejos desafíos contemporáneos para la paz y la seguridad internacionales, durante el cual el Secretario General señaló que la ciberseguridad era un peligro en auge para la paz y la seguridad internacionales (véase S/PV.8144). Posteriormente, en agosto de 2019, Polonia organizó un debate abierto sobre los desafíos para la paz y la seguridad en Oriente Medio y sugirió a los miembros que consideraran “[d]e qué manera se pueden contrarrestar las ciberamenazas, como las amenazas a las infraestructuras de energía, en lo que respecta a la promoción de mecanismos de cooperación para evitar que se produzcan incidentes cibernéticos importantes en Oriente Medio y responder a ellos” (véase S/2019/643), cuestión que trataron varios participantes en sus intervenciones. Más recientemente, en abril de 2021, durante la presidencia de Viet Nam, se celebró un debate de alto nivel sobre “La protección de los civiles en los conflictos armados: bienes de carácter civil indispensables” (véase S/2021/415), en el que los ponentes y varios participantes mencionaron las amenazas que las ciberactividades maliciosas planteaban para la infraestructura crítica, y en particular las instalaciones médicas.

4. El carácter gratuito, abierto e interoperable del ciberespacio, gestionado y apoyado por la comunidad de múltiples interesados, ha permitido sin duda a los Estados derivar un valor económico considerable y promover el progreso social a nivel mundial. Las tecnologías digitales han sido un importante catalizador del progreso y el desarrollo humanos. Además, la tecnología ha sido una importante plataforma para promover el respeto de los derechos humanos, ya que ha dado voz a los grupos vulnerables y marginados de la sociedad. El desarrollo digital sostenible puede contribuir notablemente también a promover la estabilidad en zonas que salen de conflictos regionales.

5. Sin embargo, al tiempo que se han ido incrementando la dependencia del ámbito digital y los diversos beneficios de la transformación digital, también han aumentado lamentablemente las ciberactividades maliciosas y las amenazas sistémicas que afectan al funcionamiento de la infraestructura y los servicios digitales críticos. El uso indebido del ciberespacio puede repercutir en sectores económicos fundamentales y servicios esenciales para el público, como la atención de la salud y la energía, lo que podría tener un impacto humanitario devastador y efectos desestabilizadores que podrían suponer una amenaza a la paz y la seguridad internacionales. La pandemia de enfermedad por coronavirus (COVID-19) ha hecho que se dependa en mayor medida de la infraestructura digital crucial, lo que pone de manifiesto la importancia de que los Estados se comporten de manera responsable en el ciberespacio de conformidad con los principios del derecho internacional.

6. A fin de reducir el uso malicioso de las capacidades cibernéticas y construir un ciberespacio más estable, es fundamental atenerse a los mecanismos preventivos pertinentes en los planos mundial, regional y nacional. En la última década, los Estados Miembros de las Naciones Unidas han hecho progresos notables en la formulación de los elementos de un marco normativo de comportamiento responsable de los Estados en el ciberespacio, tomando como base el derecho internacional vigente, otras normas pertinentes, medidas de fomento de la confianza y la creación de capacidad.

7. El derecho internacional vigente, y en particular la Carta, brinda a los Estados orientación suficiente para llevar a cabo ciberactividades. Los principios de derecho internacional que han guiado con éxito el comportamiento de los Estados en otros ámbitos son también un marco de referencia primordial para el comportamiento de los Estados en el ciberespacio. Además del derecho internacional, las normas de tiempos de paz, voluntarias y no vinculantes, sobre el comportamiento responsable de los Estados y las medidas de fomento de la confianza también son determinantes para guiar la conducta de los Estados en el ciberespacio; con ellas, mejoran la transparencia, la claridad y la previsibilidad. Los Estados deben cumplir sus obligaciones en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional.

8. Los sucesivos Grupos de Expertos Gubernamentales establecidos en el marco de la Primera Comisión de la Asamblea General han discutido la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional y han elaborado informes aprobados por consenso en 2010, 2013, 2015 y 2021[1]. En la Asamblea General, los Estados Miembros han acordado por consenso guiarse por las normas del comportamiento responsable de los Estados al usar las tecnologías de la información y las comunicaciones, así como por el derecho internacional y las medidas de fomento de la confianza[2]. El hecho de que en 2021 los procesos de la Primera Comisión se celebraran satisfactoriamente por medios

[1] A/65/201, A/68/98 y A/70/174 recibieron el respaldo de la Asamblea General; el informe discutido el 28 de mayo de 2021 está pendiente de publicación.

[2] Resolución 70/237 de la Asamblea General.

cibernéticos añade impulso para seguir aplicando el marco de comportamiento responsable de los Estados en el ciberespacio. En el informe aprobado por consenso en el 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, que recibió el respaldo de la Asamblea General, se reafirmó la aplicación del derecho internacional en el ciberespacio, las normas, las medidas de fomento de la confianza y la creación de capacidad[3]. El informe resultante de la reunión más reciente del Grupo de Expertos Gubernamentales sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional contribuyó en gran medida a profundizar los conocimientos sobre la aplicabilidad del derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados y ofrece más orientación sobre la implementación de las normas y el fomento de la confianza y la creación de capacidad en relación con el ciberespacio.

9. Algunas organizaciones regionales, como la Organización de los Estados Americanos, la Organización para la Seguridad y la Cooperación en Europa, la Unión Africana y la Asociación de Naciones de Asia Sudoriental y su Foro Regional, han avanzado bastante en este ámbito: han aprobado acuerdos regionales en materia de ciberseguridad y han concebido y aplicado medidas de fomento de la confianza cibernética cuyo fin es contribuir a la estabilidad y reducir las posibilidades de que los desencuentros deriven en conflictos. Al mismo tiempo, diversas iniciativas de creación de capacidad y una amplia gama de programas mundiales y regionales están siendo clave para fortalecer la resiliencia cibernética. Además, como los Estados no suelen gestionar ellos mismos toda su infraestructura crítica, sino que para ello cooperan con el sector privado, han surgido varias iniciativas público-privadas sobre ciberseguridad. Teniendo en cuenta que el ciberespacio es un ámbito de múltiples interesados, es conveniente seguir alentando toda oportunidad de incluir al sector privado, el mundo académico y la sociedad civil en las discusiones que se celebren a escala mundial, regional y nacional.

III. Preguntas orientativas

10. Tal vez los Estados Miembros deseen tratar las siguientes cuestiones en sus intervenciones:

a) ¿Cuáles son las ciberamenazas a la paz y la seguridad internacionales actuales y de nueva aparición? ¿Qué efectos podría tener en el futuro el uso malicioso del ciberespacio en relación con los conflictos?

b) ¿Qué mecanismos normativos mundiales, regionales y nacionales existen para mitigar las ciberamenazas y promover el comportamiento responsable de los Estados, y cómo pueden los Estados Miembros de las Naciones Unidas alentar su aplicación?

c) ¿Cómo se puede mejorar el cumplimiento del derecho internacional vigente y la aplicación de las normas de comportamiento responsable de los Estados en el ciberespacio acordadas por los Estados Miembros de las Naciones Unidas?

d) ¿Cómo se puede fomentar la confianza, reducir los malentendidos y evitar acontecimientos que puedan dar lugar a efectos humanitarios devastadores a raíz de ciberactividades maliciosas?

[3] Decisión 75/564 de la Asamblea General.

e) Durante los conflictos armados, ¿cómo se pueden mitigar los posibles efectos humanitarios del uso malicioso de las tecnologías de la información y las comunicaciones?

f) Dado que el ciberespacio es un ámbito de múltiples interesados, ¿cómo puede la comunidad en general, incluidos el sector privado, la sociedad civil y el mundo académico, ayudar a prevenir los conflictos, llegar a un entendimiento común y aumentar la resiliencia cibernética?

g) En el caso de situaciones graves derivadas de ciberactividades que pudieran desembocar en un conflicto internacional o dar pie a controversias, ¿qué opciones existen para responder a ellas y lograr una solución pacífica?

IV. Ponentes

11. Se ha invitado a informar al Consejo a la Alta Representante para Asuntos de Desarme.

V. Formato

12. El debate abierto de alto nivel se celebrará el 29 de junio de 2021 por videoconferencia pública. Presidirá la sesión la Primera Ministra de la República de Estonia, Kaja Kallas.

13. Se invita a los Estados Miembros de las Naciones Unidas que no son miembros del Consejo de Seguridad y a los Observadores Permanentes ante las Naciones Unidas a que participen presentando sus declaraciones por escrito mediante el módulo eSpeakers. Los Estados Miembros deberán remitir sus declaraciones en formato de Microsoft Word y acompañarlas de una carta de presentación, debidamente firmada por el Representante Permanente o el Encargado de Negocios y dirigida a la Presidencia del Consejo de Seguridad, a más tardar en la fecha de la sesión, es decir, el 29 de junio de 2021. Las declaraciones se publicarán en un documento recopilatorio oficial que incluirá las intervenciones presentadas en relación con esta videoconferencia pública.