Naciones Unidas S/2021/621

Consejo de Seguridad

Distr. general
1 de julio de 2021
Español
Original: inglés

Carta de fecha 1 de julio de 2021 dirigida al Secretario General y a los Representantes Permanentes de los miembros del Consejo de Seguridad por la Presidencia del Consejo de Seguridad

Tengo el honor de adjuntar a la presente una copia de la exposición informativa ofrecida por Izumi Nakamitsu, Alta Representante para Asuntos de Desarme, así como de las declaraciones formuladas por Kaja Kallas, Primera Ministra de Estonia; Mahamadou Ouhoumoudou, Primer Ministro del Níger; Simon Coveney, Ministro de Relaciones Exteriores y Defensa de Irlanda; Bui Thanh Son, Ministro de Relaciones Exteriores de Viet Nam; Joe Mucheru, Secretario del Gabinete de Comunicaciones y Tecnología de la Información, Innovación y Asuntos de la Juventud de Kenya; Linda Thomas-Greenfield, Representante Permanente de los Estados Unidos de América y miembro del Gobierno del Presidente Biden; Harsh Vardhan Shringla, Secretario de Relaciones Exteriores de la India; Keisal M. Peters, Ministra de Estado a cargo de Relaciones Exteriores y Comercio Exterior de San Vicente y las Granadinas; Audun Halvorsen, Viceministro de Relaciones Exteriores de Noruega; Lord Tariq Ahmad de Wimbledon, Ministro de Estado para el Commonwealth, las Naciones Unidas y Asia Meridional del Reino Unido de Gran Bretaña e Irlanda del Norte; y Franck Riester, Ministro Delegado de Comercio Exterior y Atractivo Económico de Francia adscrito al Ministro de Europa y de Relaciones Exteriores de Francia, así como por los representantes de China, México, la Federación de Rusia y Túnez en relación con la videoconferencia sobre el tema “Mantenimiento de la paz y la seguridad internacionales: ciberseguridad” celebrada el martes 29 de junio de 2021.

De conformidad con el entendimiento alcanzado entre los miembros del Consejo en relación con esta videoconferencia, las siguientes delegaciones presentaron declaraciones por escrito, de las que también se adjunta copia: Alemania, Argentina, Australia, Austria, Bahrein, Bélgica, Brasil, Canadá, Chequia, Chile, Comité Internacional de la Cruz Roja, Dinamarca, Ecuador, Egipto, El Salvador, Emiratos Árabes Unidos, Eslovaquia, Eslovenia, Georgia, Grecia, Guatemala, Indonesia, República Islámica del Irán, Italia, Japón, Kazajstán, Letonia, Liechtenstein, Malta, Marruecos, Nueva Zelandia, Organización Internacional de Policía Criminal, Países Bajos, Pakistán, Perú, Polonia, Qatar, República de Corea, Rumania, Senegal, Singapur, Sudáfrica, Suiza, Tailandia, Turquía, Ucrania y Unión Europea.

De conformidad con el procedimiento establecido en la carta de fecha 7 de mayo de 2020 dirigida a los Representantes Permanentes de los miembros del Consejo de Seguridad por la Presidencia del Consejo de Seguridad (S/2020/372), acordada a raíz de las circunstancias extraordinarias relacionadas con la pandemia de enfermedad por coronavirus (COVID-19), las exposiciones informativas y las declaraciones adjuntas se publicarán como documento del Consejo de Seguridad.

(*Firmado*) Nicolas **de Rivière**
Presidente del Consejo de Seguridad

Anexo I

Declaración de la Alta Representante para Asuntos de Desarme, Izumi Nakamitsu

Deseo manifestar mi aprecio a Estonia por organizar esta reunión y por invitarme a ofrecer una exposición informativa en este debate abierto sobre el mantenimiento de la paz y la seguridad internacionales en el ciberespacio.

Al mes de enero de este año, hay más de 4.600 millones de usuarios activos de Internet en todo el mundo. Se calcula que en 2022 habrá 28.500 millones de dispositivos en red conectados a Internet, lo que supone un aumento significativo respecto a los 18.000 millones de 2017.

A medida que los avances en las tecnologías digitales siguen revolucionando la vida humana, debemos permanecer atentos al uso malicioso de dichas tecnologías que podría poner en peligro la seguridad de las generaciones futuras.

Las tecnologías digitales están tensionando cada vez más las normas jurídicas, humanitarias y éticas existentes, la no proliferación, la estabilidad internacional y la paz y la seguridad.

También están reduciendo las barreras de acceso y abriendo nuevos dominios potenciales para el conflicto y la capacidad de los actores estatales y no estatales para llevar a cabo ataques, incluso a través de las fronteras internacionales.

En lo que respecta específicamente a las tecnologías de la información y las comunicaciones (TIC), hemos asistido a un aumento espectacular de la frecuencia de los incidentes maliciosos en los últimos años. Estos incidentes han adoptado muchas formas, desde la desinformación hasta la disrupción de las redes de computadoras. Estos actos contribuyen a la disminución de la confianza entre los Estados.

Estos avances también suponen un riesgo específico para la infraestructura crítica que es habilitada por las TIC, como el sector financiero, las redes de suministro eléctrico y las instalaciones nucleares. El Secretario General ha dirigido la atención sobre los ciberataques a instalaciones de salud durante la pandemia, y ha hecho un llamamiento a la comunidad internacional para que haga más por prevenir y poner fin a estas nuevas formas de agresión, que pueden causar más daños graves a la población civil[1].

Estas amenazas de las TIC también tienen un impacto de género y deben ser examinadas a través de esta lente. El extremismo violento y la trata de personas en línea tienen un impacto diferenciado, que suele pasarse por alto, en las mujeres, los hombres y los niños, al igual que otras amenazas relacionadas con las TIC, como el ciberacoso, la violencia de pareja y la difusión no consentida de información e imágenes íntimas. Por eso también debemos hacer todo lo posible para garantizar la participación igualitaria, plena y efectiva de mujeres y hombres en la toma de decisiones en el ámbito digital.

[1] Véase www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered.

Las amenazas de las TIC están aumentando, pero también se están realizando esfuerzos para hacerles frente. A lo largo de la última década y media en las Naciones Unidas, una serie de cinco Grupos de Expertos Gubernamentales han estudiado las amenazas existentes y emergentes de las TIC para la seguridad internacional y han recomendado medidas para afrontarlas. Otros dos procesos de las Naciones Unidas, un Grupo de Trabajo de Composición Abierta y un sexto Grupo de Expertos Gubernamentales, ambos creados en 2018, han concluido recientemente y con éxito sus respectivos trabajos, dando importantes pasos adelante en el tema mediante la adopción de recomendaciones concretas y orientadas a la acción.

Estos dos Grupos afirmaron un conjunto de normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados, reconociendo que podrían desarrollarse normas adicionales con el tiempo. También reafirmaron que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el entorno de las TIC. Los Grupos recomendaron medidas de fomento de la confianza, creación de capacidad y de cooperación, con base en el trabajo de los procesos anteriores. Además, el Grupo de Trabajo de Composición Abierta, de acuerdo con su mandato, formuló conclusiones y recomendaciones sobre el establecimiento de un diálogo institucional regular sobre la cuestión de las TIC.

Como señaló el Grupo de Expertos Gubernamentales más reciente en su informe, las medidas recomendadas por los anteriores Grupos de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta representan, en conjunto, un marco inicial para el comportamiento responsable del Estado en el uso de las TIC[2].

Un nuevo y segundo Grupo de Trabajo de Composición Abierta acaba de celebrar su período de sesiones de organización y comenzará su labor sustantiva a finales de este año.

A nivel regional, las organizaciones regionales están llevando a cabo esfuerzos clave en materia de TIC. Los enfoques regionales han adoptado diversas formas según las diferentes prioridades y necesidades. Algunas regiones han hecho mayor hincapié en la aplicación de normas voluntarias y no vinculantes de comportamiento responsable de los Estados mediante esfuerzos de creación de capacidad, mientras que otras han sido pioneras en sus propias medidas regionales de fomento de la confianza para reducir los riesgos de conflicto derivados de las actividades de las TIC o han adoptado otras herramientas regionales para hacer frente a las amenazas de las TIC. También existen varios instrumentos regionales que abordan aspectos específicos de las TIC.

Aunque los Estados son los principales responsables del mantenimiento de la seguridad internacional, las TIC son parte integrante de nuestras sociedades y otros interesados tienen un papel y un interés clave, así como una responsabilidad, en la seguridad del ciberespacio.

[2] Véase el párr. 21 del informe del Grupo de Expertos Gubernamentales. Se encuentra disponible una copia anticipada en https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

Se han creado muchas y excelentes ciberiniciativas dirigidas por el sector privado, como el Acuerdo Tecnológico de Ciberseguridad liderado por Microsoft, la Carta de Confianza dirigida por Siemens y la Conferencia de Múnich sobre Seguridad, y la Iniciativa de Transparencia Global de Kaspersky Lab.

El Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio de 2018 reunió a la industria, los Estados, la sociedad civil y el mundo académico en un compromiso con nueve principios para la ciberseguridad. Estos principios abarcan una serie de cuestiones que van desde el desarrollo de medios para evitar la proliferación de herramientas y prácticas maliciosas de las TIC, hasta la promoción de la aceptación generalizada y la puesta en práctica de normas internacionales de comportamiento responsable, así como medidas de fomento de la confianza en el ciberespacio.

Las perspectivas del sector privado, la sociedad civil y el mundo académico aportan una parte única e importante de la solución colectiva a la ciberseguridad que busca la comunidad internacional.

Las Naciones Unidas, por su parte, están dispuestas a apoyar a los Estados, junto con otros interesados, en la promoción de un entorno pacífico para las TIC. El Secretario General convocó un panel de alto nivel sobre la cooperación digital, que publicó su informe en 2019. A través de una serie de mesas redondas posteriores con los Estados y otros interesados clave, se elaboró una hoja de ruta, que recomendaba nuevas acciones para hacer avanzar la cooperación en áreas clave del espacio digital.

En el contexto de la paz y la seguridad, el Secretario General también puso en marcha una agenda para el desarme que hace hincapié en la comprensión y el tratamiento de las tecnologías de nueva generación que plantean posibles desafíos a las normas legales, humanitarias y éticas existentes; la no proliferación; y la paz y la seguridad.

En su agenda, el Secretario General se compromete a participar y a trabajar con los científicos, los ingenieros y la industria para fomentar la innovación responsable de la ciencia y la tecnología y garantizar su aplicación con fines pacíficos.

También asume un segundo compromiso de participar con Estados Miembros para ayudar a fomentar una cultura de rendición de cuentas y respeto a las normas, las reglas y los principios emergentes de un comportamiento responsable en el ciberespacio.

Si bien el espacio digital ha llegado a apuntalar casi todos los aspectos de nuestra vida cotidiana, la escala y la omnipresencia de la “inseguridad” de las TIC también se reconoce ahora como una preocupación importante. La dificultad política y técnica de atribuir y asignar la responsabilidad de los ataques de las TIC podría tener consecuencias significativas, incluso en respuestas armadas no deseadas y su escalada.

Estas dinámicas pueden animar a los Estados a adoptar posturas ofensivas para el uso hostil de estas tecnologías. También puede permitir a los grupos armados y criminales no estatales y a los individuos que buscan desarrollar o acceder a capacidades potencialmente desestabilizadoras con un alto grado de impunidad. Dadas estas repercusiones para el mantenimiento de la paz y la seguridad

internacionales derivadas de las amenazas de las TIC, el compromiso del Consejo de Seguridad en esta cuestión es primordial.

Por lo tanto, celebro esta oportunidad de dirigirme al Consejo, y espero con interés el debate que tendrá lugar a continuación.

Anexo II

Declaración de la Primera Ministra de Estonia, Kaja Kallas

Las Naciones Unidas fueron creadas con el futuro en mente. Aunque nos enfrentamos a una serie de nuevos desafíos, los valores y principios convenidos en la Carta de las Naciones Unidas hace 76 años siguen siendo igual de válidos hoy en día. Mantenerlos en nuestro futuro cada vez más digital se ha convertido en una de las tareas globales más urgentes. Hoy quiero hablar de las oportunidades, de las amenazas y de los mecanismos que tenemos para afrontarlas.

En primer lugar, las oportunidades: el último año y medio de trabajo, estudio y vida a distancia ha demostrado claramente que nuestra dependencia de las tecnologías digitales y de la comunicación no hará más que crecer con el tiempo. Somos responsables de construir un futuro en el que todos los actores sigan ciertas obligaciones en su comportamiento en el ciberespacio.

Por eso, el debate de hoy no es sobre la tecnología, sino sobre cómo se puede utilizar el ciberespacio. Steve Jobs lo describió bien: “La tecnología no es nada. Lo importante es tener fe en las personas, que son básicamente buenas e inteligentes, y si les das herramientas, harán cosas maravillosas con ellas”.

Como sociedad digital próspera, Estonia lo ha experimentado de primera mano. Un ciberespacio libre, abierto, estable y seguro forma parte de nuestra vida. Hemos ahorrado entre un 2 % y un 3 % más de nuestro producto interno bruto cada año gracias a la puesta en línea de la mayoría de los servicios públicos. Nuestra administración pública de rutina lleva más de 15 años sin usar papel. Estonia también ha producido el mayor número de unicornios tecnológicos per cápita.

En segundo lugar, las amenazas: debemos reconocer que también existe un lado oscuro en la rápida digitalización.

Los actores maliciosos pueden utilizar el ciberespacio como otro dominio a través del cual causar estragos. Por ejemplo, imagine lo que ocurriría si en medio de una sequía, la cadena de suministro de agua de un país dejara de funcionar o si durante los fríos meses de invierno, la red eléctrica de una nación se interrumpiera.

En el último año, hemos visto cómo las ciberactividades dañinas dirigidas al sector de salud pueden suponer una amenaza real y tangible. Los efectos humanitarios de la manipulación de la infraestructura crítica podrían ser devastadores.

Aunque podemos poner altas barreras y vallas alrededor de nuestras centrales eléctricas y otra infraestructura crítica, esto nunca puede ser parte de la solución en el ciberespacio. En cambio, debemos asumir colectivamente el papel de guardianes.

Por último, cómo hacer frente a estas amenazas: afortunadamente, como también expuso nuestra distinguida ponente, la Sra. Nakamitsu, tenemos una base sólida sobre la que trabajar.

Durante la última década, los Estados Miembros han acordado un marco normativo eficaz para la ciberestabilidad y la prevención de conflictos. Consiste en el derecho internacional vigente, 11 normas voluntarias no vinculantes para un comportamiento responsable de los Estados, medidas de fomento de la confianza y la creación de capacidad.

Estonia apoya la sólida opinión de que el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica al comportamiento de los Estados en el ciberespacio.

Permítanme subrayar que los Estados son responsables de cualquier acto cometido contrario a las obligaciones que hayan contraído en virtud del derecho internacional.

Para garantizar la protección de la población y los bienes civiles en situaciones de conflicto armado en particular, que el Consejo de Seguridad también examina periódicamente, es fundamental que cualquier uso de las cibercapacidades en este contexto esté sujeto a las obligaciones derivadas del derecho internacional humanitario.

Las 11 normas de comportamiento responsable de los Estados que hemos acordado reflejan las expectativas de la comunidad internacional y fijan importantes directrices adicionales para las actividades de los Estados en el ciberespacio.

Esta primavera, la comunidad internacional ha reafirmado con fuerza este marco normativo. Nos sentimos alentados y guiados por los exitosos resultados del consenso tanto del último Grupo de Expertos Gubernamentales como del Grupo de Trabajo de Composición Abierta. La implementación de este marco es un objetivo importante para la comunidad internacional.

Los esfuerzos globales también deben ir acompañados de actividades regionales y de creación de capacidad. A este respecto, destacamos la importante labor realizada por las organizaciones regionales para aumentar la confianza y avanzar en la cooperación. Estonia también da prioridad a los esfuerzos para cerrar la brecha digital, que deben ir acompañadas de la creación de capacidad en materia de ciberresiliencia y de la protección de los derechos humanos en línea.

También debemos reconocer que abordamos las ciberamenazas junto con el sector privado, la sociedad civil y el mundo académico. Las compañías, en particular, desempeñan un papel importante en invertir en ciberseguridad y ayudar a eliminar las vulnerabilidades.

Estoy seguro de que el debate de hoy dejará una huella en la historia del Consejo de Seguridad al abordar las cuestiones que serán más relevantes para el mantenimiento de la paz y la estabilidad internacionales en los próximos años.

Nuestro futuro digital solo estará asegurado si seguimos unas reglas de procedimiento comunes.

Anexo III

Declaración del Primer Ministro de la República del Níger, Ouhoumoudou Mahamadou

[Original: francés]

En primer lugar, permítanme expresar mi agradecimiento a Estonia por incluir la cuestión de los riesgos de seguridad relacionados con el ciberespacio en la agenda del Consejo. Asimismo, quisiera dar las gracias a la Sra. Izumi Nakamitsu por su intervención y su firme compromiso sobre esta cuestión.

Durante los dos últimos decenios, la penetración de Internet y la utilización de tecnologías de la información y las comunicaciones (TIC) han experimentado un crecimiento fulgurante. El ciberespacio se ha convertido hoy en día en un tablero geopolítico que permite a las distintas naciones avanzar en su esfera de influencia a nivel tanto económico como político y cultural.

Esta revolución digital que tanto nos ha acercado eliminando nuestras fronteras también ha abierto la vía a nuevos desafíos de soberanía debido a la naturaleza extraterritorial de las leyes en la materia. Del mismo modo que este espacio puede reforzar nuestras democracias, brindando una plataforma y un soporte a todas las voces para hacerse oír, incluso las voces disidentes, también puede ser un lugar de refugio para actores y grupos delictivos cuyo único objetivo es desestabilizar nuestras naciones.

La pandemia de enfermedad por coronavirus (COVID-19) nos ha mostrado las dos facetas de este espacio: por un lado, nuestra dependencia creciente de las tecnologías digitales —esta reunión en formato virtual es una prueba de ello— y, por otro lado, la fragilidad de nuestros sistemas frente a las posibilidades de ciberdelincuencia y ciberespionaje, demostrada por los ataques delictivos con programas secuestradores llevados a cabo contra los sistemas de salud y las campañas de desinformación que tienen como objetivo minar la moral de los ciudadanos de nuestros países contra los esfuerzos de vacunación.

Además, el auge de las redes sociales y otras plataformas de debate ha dado lugar a la proliferación de determinados tipos de discurso que incitan a actos de insurrección, terrorismo y ataque a nuestros valores morales y a las bases de nuestras democracias.

Habida cuenta de todo lo anterior, permítanme formular algunas recomendaciones susceptibles, desde mi punto de vista, de propiciar el refuerzo del respeto del derecho internacional y el establecimiento de normas de actuación responsable de los Estados en el ciberespacio.

En primer lugar, es necesario cerrar la brecha digital que existe entre las naciones, y principalmente con el continente africano, donde tres cuartas partes de los habitantes tienen un acceso insuficiente o nulo a Internet.

Esta situación, como han mencionado los expertos, es un factor que agrava el empobrecimiento de las poblaciones y cuya incidencia afecta a todo el mundo y a todos los componentes de la sociedad, desde la sanidad al bienestar económico pasando por la educación, y hace a estos últimos más vulnerables a las campañas de

desinformación y a otras amenazas propiciadas por las tecnologías de la información y las comunicaciones. No podemos esperar un ciberespacio saludable y protegido sin garantizar la equidad digital.

Sobre esta base, mi segunda recomendación es el desarrollo de una arquitectura mundial a través de un enfoque integrado y coordinado que permitiría definir, de manera clara, las normas de derecho internacional aplicables al ciberespacio, en ámbitos tan amplios como la salud, el derecho internacional humanitario, el proceso electoral y las actividades económicas, por mencionar solo algunos.

Pero al hacerlo, también debemos ser conscientes de que esta arquitectura debe ser equitativa, tanto en su aplicación como en los beneficios que van a cosecharse, para evitar crear nuevos mecanismos de doble rasero que no harían más que profundizar las desigualdades entre las naciones, obligándolas a afrontar otros efectos perversos.

Con esta lógica, convendría que toda nueva arquitectura reglamentaria a nivel mundial se inspire en las ya establecidas a nivel regional, que se supone que armonizan las reglamentaciones de los Estados aplicables a escala nacional. En este sentido, nos gustaría mencionar la directiva de la Comunidad Económica de los Estados de África Occidental (CEDEAO) sobre la lucha contra la ciberdelincuencia, que impone obligaciones a los Estados miembros en este ámbito, incluida la penalización de determinados actos, y que crea un marco para facilitar la cooperación regional en materia de ciberseguridad.

Mi última recomendación sería que el Consejo de Seguridad trabaje en una interpretación más inclusiva y menos discriminatoria de la Carta de las Naciones Unidas, pero también de su propio mandato, para que nuestras deliberaciones puedan reflejar la realidad del mundo actual y poder así abordar temáticas como la ciberseguridad, el cambio climático y las pandemias, porque estas amenazas son reales y, al igual que la COVID-19, no conocen fronteras.

Anexo IV

Declaración del Ministro de Relaciones Exteriores y Defensa de Irlanda, Simon Coveney

Mis felicitaciones a Estonia por su exitosa Presidencia del Consejo.

Mi agradecimiento también a la Alta Representante por sus valiosas reflexiones.

Celebro este oportuno debate, el primero de este tipo en el Consejo de Seguridad.

Hablando del año pasado, el Secretario General pidió a los Estados que pusieran orden en lo que denominó el “lejano Oeste del ciberespacio”.

Si bien en los últimos meses se han logrado progresos satisfactorios en las Naciones Unidas, los problemas de ciberseguridad a los que se enfrentan los Estados siguen aumentando, poniendo en peligro la paz y la seguridad internacionales.

Quisiera centrar mi intervención de hoy tres áreas:

- Desafíos y oportunidades
- La necesidad de que los Estados implementen las medidas acordadas en las Naciones Unidas
- La importancia de un enfoque basado en los valores en esta cuestión

En primer lugar, los desafíos y las oportunidades.

Las tecnologías digitales y de la comunicación siguen impulsando el crecimiento económico y transformando nuestra forma de vivir, comunicarnos y trabajar.

La innovación es la clave para afrontar algunos de los desafíos mundiales más importantes de la actualidad, como el cambio climático. También facilita importantes avances en la investigación médica, mejora el acceso a la educación y aumenta las capacidades de nuestro personal de mantenimiento de la paz, ayudándolas a mantenerse seguras.

En el último año, la pandemia ha puesto de manifiesto nuestra creciente dependencia de las tecnologías de la información y la comunicación, uniendo a las personas en momentos en los que debían permanecer separadas, y exponiendo al mismo tiempo nuestras vulnerabilidades.

Hablo por experiencia reciente sobre este último punto. Los sistemas de salud pública de Irlanda sufrieron el mes pasado un ataque de programas maliciosos secuestradores muy dañino que afectó a servicios médicos críticos.

Un ataque de este tipo durante una pandemia mundial es terrible. Por desgracia, la experiencia de Irlanda no es un caso aislado a nivel internacional.

La ciberactividad maliciosa, incluidos los ataques de programas maliciosos secuestradores, la ciberdelincuencia, el robo de propiedad intelectual y la difusión de desinformación y odio, ha aumentado en los últimos años.

Se apunta cada vez más a la infraestructura crítica.

A Irlanda le preocupa mucho que esta actividad suponga una amenaza a la paz y seguridad internacionales.

Los desafíos de seguridad existentes se ven agravados por las ciberamenazas, como la vulnerabilidad de los sistemas de mando y control de las armas nucleares a los ciberataques. Esto añade una nueva urgencia a la necesidad de hacer progresos en el desarme nuclear.

No podemos permitir que el ciberespacio no esté limitado por normas o leyes, donde los actores maliciosos actúan a su antojo.

Los conflictos internacionales en el ciberespacio deben resolverse por medios pacíficos.

El Consejo debe enviar un mensaje claro de apoyo a un ciberespacio mundial pacífico y seguro, basado en el consenso y la confianza mutua.

Pasando a mi segundo punto, Irlanda se congratula de los recientes progresos realizados en las Naciones Unidas para acordar el marco para el comportamiento responsable de los Estados en el ciberespacio.

Los Estados han reafirmado ahora que el derecho internacional existente, en particular la Carta de las Naciones Unidas, proporciona una base sólida, basada en normas, para todos los enfoques de la ciberseguridad.

Irlanda apoya los esfuerzos destinados a promover un mayor entendimiento entre los Estados sobre la aplicación del derecho internacional al ciberespacio.

Pronto publicaremos nuestra posición nacional y animaremos a otros a hacer lo mismo.

El comportamiento responsable del Estado es, por supuesto, también crítico.

Todos los Estados Miembros han acordado guiarse por las 11 normas voluntarias de comportamiento del Estado en el ciberespacio.

Ahora tenemos que trabajar para promover la comprensión y la aplicación de estas normas, sobre la base del derecho internacional, para reforzar la ciberseguridad mundial. Esto reducirá el potencial de conflicto y mejorará las relaciones internacionales.

Las medidas de fomento de la confianza, incluido el diálogo, generan confianza y reducen las tensiones entre los Estados. Sé que es una obviedad, pero hay que decirlo.

Acogemos con satisfacción el papel de liderazgo que desempeñan las organizaciones regionales a este respecto, incluida la Organización para la Seguridad y la Cooperación en Europa. Irlanda y nuestros socios de la Unión Europea se han comprometido a apoyar las iniciativas de creación de capacidad.

En un ciberespacio muy interconectado, ningún país está seguro hasta que todos los países lo estén. Sin dudas, la pandemia de enfermedad por coronavirus (COVID-19) nos ha enseñado eso.

También seguimos comprometidos con la lucha contra la brecha digital mundial. El acceso en línea para todos será un elemento clave para la consecución de los Objetivos de Desarrollo Sostenible en la próxima década.

Mi tercer punto es que el mantenimiento de la paz y la seguridad internacionales en el ciberespacio debe estar centrado en el ser humano y basado en valores.

Irlanda apoya un ciberespacio seguro y accesible en el que se apliquen los derechos humanos y las libertades fundamentales, tanto dentro como fuera de la red.

Reafirmamos enérgicamente la aplicabilidad del derecho internacional de los derechos humanos a las acciones de los Estados en el ciberespacio.

La protección de los civiles sigue siendo una prioridad absoluta en todos los aspectos de nuestro trabajo. A este respecto, Irlanda se compromete a garantizar el respeto del derecho internacional humanitario en el ciberespacio.

Es una triste realidad que la violencia de género que experimentan demasiadas mujeres y niñas esté ahora frecuentemente acompañada y magnificada por la violencia en línea y las ciberamenazas.

Ello hace que sea aún más importante que nosotros, como líderes, todos los líderes, promovamos conscientemente la participación de las mujeres en los procesos, decisiones y políticas de las Naciones Unidas sobre el ciberespacio.

Tenemos que trabajar con más ahínco para superar la brecha digital de género.

Irlanda ha defendido constantemente la inclusión de un mayor número de expertos en los debates de las Naciones Unidas sobre ciberseguridad y creación de capacidad.

Los gobiernos, junto con quienes impulsan y lideran la innovación tecnológica, tienen la responsabilidad de mantener un ciberespacio seguro y libre.

Las contribuciones de la sociedad civil, los expertos técnicos, los académicos y el sector privado han enriquecido los anteriores ciberdebates de las Naciones Unidas. Hasta la fecha, su compromiso ha sido demasiado limitado, en nuestra opinión, en el tema de la ciberseguridad.

También apoyamos iniciativas, como el Llamamiento de París para la Confianza y la Estabilidad en el Ciberespacio, que reúnen a los interesados estatales y no estatales con el objetivo común de promover la paz y la seguridad.

Debemos trabajar todos juntos para alcanzar mejores soluciones compartidas.

Para concluir, Irlanda seguirá apoyando los enfoques constructivos, multilaterales y de múltiples interesados, basados en el consenso, para reforzar la ciberresiliencia en todo el mundo.

Exhortamos a todos los Estados a que se comporten de forma responsable, en pleno cumplimiento del derecho internacional, y apliquen el marco normativo.

Valoramos el papel del Consejo de Seguridad en la prevención de conflictos y el fomento de la paz y la seguridad, también en el ciberespacio.

E instamos a todos los Estados a que aprovechen los logros alcanzados en las Naciones Unidas en los últimos meses.

De este modo podemos garantizar un ciberespacio global más seguro y pacífico del que todos nos beneficiemos.

Anexo V

Declaración del Ministro de Relaciones Exteriores de Viet Nam, Bui Thanh Son

Agradezco a la Presidenta y a la presidencia estonia por haber convocado esta reunión sobre una cuestión que es esencial. Agradezco las perspicaces observaciones de la Secretaria General Adjunta Nakamitsu.

El desarrollo explosivo de las tecnologías de la información y las comunicaciones (TIC) ha transformado significativamente la forma en que las personas viven, trabajan y se relacionan entre sí. Ha facilitado la comunicación global, la puesta en común de conocimientos y el intercambio cultural, ha ayudado a los pueblos y países a acercarse, y también ha renovado la producción hacia modelos más eficientes, sostenibles e inclusivos.

Por otro lado, estas tecnologías avanzadas, si caen en manos equivocadas y se utilizan con malicia, pueden suponer graves amenazas para la soberanía, la seguridad y la prosperidad de las naciones. Desplegadas por terroristas o delincuentes transnacionales, son capaces de sabotear los sistemas económicos, dañar la estabilidad social y erosionar los valores culturales y humanos.

Tomemos como ejemplo las pérdidas económicas causadas por los ciberataques. El gasto anual mundial en ciberseguridad alcanzó $1 billón en 2020, un aumento del 50 % en comparación con 2018 y un aumento del triple desde 2013. La mayor parte del gasto se destina a la reparación y recuperación de los daños.

Y lo que es más preocupante, se ha informado de ciberataques transnacionales que han socavado la seguridad mundial y nacional, pudiendo incluso desencadenar una ciberguerra.

Por ello, la ciberseguridad es muy urgente y crítica para la paz, la seguridad, el desarrollo y la prosperidad tanto a nivel nacional como mundial. Con ese telón de fondo, quisiera compartir las siguientes ideas.

En primer lugar, cada Estado tiene su propia soberanía e intereses sobre el ciberespacio que deben ser plenamente respetados. Cada Estado Miembro es el principal responsable de crear el marco jurídico para regular el comportamiento en el ciberespacio dentro de su territorio y aplicable a sus ciudadanos. Asimismo, regular los comportamientos de acuerdo con la ley, prevenir los actos intencionales ilegales y facilitar las actividades positivas son principios rectores para crear un ciberespacio seguro y estable para la paz, el desarrollo y la humanidad.

Viet Nam es un país con una gran cobertura de Internet, con casi el 70 % de nuestra población activa en Internet y las redes sociales. Nuestro éxito radica en el amplio marco jurídico que facilita el desarrollo de las TIC y evita su uso indebido. Viet Nam también da prioridad a la mejora de la autoprotección, la autosuficiencia y la resiliencia, junto con una cooperación internacional eficaz.

En segundo lugar, la naturaleza de los ciberataques es transnacional, ya que las redes mundiales de Internet se convierten en objetivo de explotación constante por parte de los autores. En consecuencia, requiere soluciones globales y transnacionales para la ciberseguridad. Viet Nam apoya un marco internacional que establezca reglas

y normas de comportamiento responsable en el ciberespacio, sobre la base del consenso y con la más amplia participación de los países, incluidos los procesos en curso en las Naciones Unidas. Nos preocupa y nos oponemos al uso malintencionado y perjudicial de las TIC, especialmente a los ciberataques a las instalaciones médicas, eléctricas, de agua y alimentarias tan esenciales para la población. Las actividades en el ciberespacio tienen que cumplir los principios de la Carta de las Naciones Unidas y del derecho internacional, en particular, el respeto a la soberanía, la no injerencia en los asuntos internos de los Estados y el no uso de la fuerza y la solución pacífica de las controversias.

En tercer lugar, el aumento de la cooperación internacional, la creación de confianza y la responsabilidad son indispensables para reforzar la ciberseguridad. Todos los países, independientemente de su tamaño y nivel de desarrollo, se benefician de un ciberespacio global seguro y protegido. Por lo tanto, es necesario que participen activamente y contribuyan de forma más práctica y responsable a garantizar la seguridad en el ciberespacio mundial en aras de la paz, la estabilidad y el desarrollo sostenible de todas las naciones.

El desarrollo de las TIC es una importante plataforma de lanzamiento en nuestra búsqueda común de prosperidad. Viet Nam ha aplicado activamente una estrategia nacional de transformación digital. Nuestro objetivo es que la economía digital represente el 30 % del producto interno bruto en 2030. En Asia Sudoriental, Viet Nam ha participado activamente en los mecanismos regionales de ciberseguridad, incluida la estrategia de cooperación en ciberseguridad de la Asociación de Naciones de Asia Sudoriental. También mantenemos una eficaz cooperación bilateral con muchos países y asociados internacionales en este ámbito. Viet Nam está dispuesto a seguir contribuyendo a la mejora de la cooperación internacional para lograr un ciberespacio pacífico, estable, seguro y protegido para nuestra prosperidad compartida y nuestro desarrollo sostenible.

Anexo VI

Declaración del Secretario del Gabinete de Tecnología de la Información y las Comunicaciones, Innovación y Asuntos de la Juventud de Kenya, Joe Mucheru

Felicito a la Presidenta por haber convocado, por primera vez en el Consejo de Seguridad, un debate independiente sobre ciberseguridad. Agradezco a la Alta Representante para Asuntos de Desarme, Sra. Nakamitsu, su exposición informativa.

El aumento de nuestra dependencia de las tecnologías de la información y las comunicaciones (TIC) conlleva tanto beneficios como vulnerabilidades.

Los esfuerzos de quienes desarrollan y utilizan las TIC y las tecnologías emergentes con fines pacíficos se ven estrechamente equiparados por sus contrarios, que las utilizan para el control, la vigilancia ilícita, el fraude, la radicalización y la desestabilización.

Kenya está comprometida con el mantenimiento y la protección de un dominio de Internet libre y abierto. Consideramos que es un motor clave del desarrollo nacional, y buscamos que nuestros jóvenes estén capacitados y sean competitivos en su uso.

Somos un líder mundial en moneda digital, y fuimos pioneros en M-Pesa, la primera plataforma de dinero móvil ampliamente utilizada. Nuestro Gobierno también ha adoptado la prestación de plataformas de servicios públicos digitalizados a través de nuestras instalaciones de servicios de ventanilla única, conocidas como Centros Huduma, que están repartidas por todo el país.

Los jóvenes kenianos están innovando y creando empresas transformadoras. Esto ha sido reconocido por los inversionistas de todo el mundo, ya que nuestro “Silicon Savanna” es lo que más inversiones atrae en nuestra región. Creemos que muchos de nuestros empleos decentes del futuro surgirán de estas empresas.

Con una exposición tan amplia al ámbito digital, Kenya considera un objetivo crítico de seguridad nacional garantizar las TIC.

Para ello, contamos con un sólido régimen normativo. Y también tenemos una capacidad creciente para responder a las amenazas. Nuestro Equipo de Respuesta a Incidentes y Emergencias Informáticas colabora con otros equipos nacionales de respuesta de incidentes informáticos, y a nivel internacional a través del Foro Mundial de Equipos de Seguridad y Respuesta a Incidentes.

Nuestra tarea hoy es ofrecer propuestas sobre cómo el Consejo de Seguridad puede garantizar mejor la paz y la seguridad internacionales frente a las amenazas lanzadas a través del ciberespacio o que lo explotan.

Destacaré tres áreas que creemos que se beneficiarían de una mejor cooperación y colaboración internacional.

El primer ámbito se refiere a las TIC y las economías emergentes. La ciberdelincuencia se centra cada vez más en las economías emergentes. Es necesaria una mayor cooperación para reforzar los mecanismos de resolución de conflictos económicos regionales e internacionales existentes, incluidos esfuerzos coordinados

para identificar y mitigar los riesgos asociados a las actividades vinculadas a las TIC, como el fraude digitalizado, el impacto de las criptomonedas en los sistemas bancarios centrales nacionales y los ciberataques a la infraestructura crítica.

A medida que se acelera la automatización industrial, los puestos de trabajo perdidos deben ser sustituidos por otros decentes, de lo contrario la paz y la seguridad se verán afectadas. Habrá que invertir más en las competencias digitales que permiten a los países con una industria subdesarrollada atraer la inversión que ofrece millones de nuevos puestos de trabajo.

La segunda área está relacionada con las TIC y el extremismo violento. La naturaleza omnipresente, programable y basada en datos de las tecnologías emergentes, aunque beneficiosa, también ha abierto una puerta al uso indebido por parte de grupos armados y terroristas. Estos grupos aprovechan los mecanismos de control opacos, los algoritmos, la impresión en 3D, la aplicación de criptografía y la interfaz de usuario simplificada para reclutar, planificar y llevar a cabo actos terroristas. Esto ha potenciado la radicalización y la militarización.

Kenya pide que se mejore la cooperación entre el Consejo de Seguridad y la Oficina de Lucha contra el Terrorismo para crear una capacidad de seguridad en el ciberespacio que sea sólida y responda a las necesidades de creación de capacidad de los Estados Miembros.

Los mandatos de las operaciones de paz de las Naciones Unidas también deberán tener en cuenta el uso del ciberespacio por parte de actores militarizados hostiles.

Mi tercera área de interés son las TIC y los medios sociales. No se puede exagerar el creciente impacto de las noticias falsas, los “deep fakes”, la desinformación y la desinformación en la paz y la seguridad. Recientemente, hemos visto el impacto de las noticias falsas que empañan las respuestas a la amenaza de pandemia de enfermedad por coronavirus (COVID-19), promoviendo las dudas sobre las vacunas.

Las empresas de medios sociales van a tener que rendir cuentas y asegurarse de que las noticias falsas, en particular las de actores sofisticados, algunos apoyados por los Estados, no proliferen en sus plataformas. Este esfuerzo normativo deberá basarse en una plataforma multilateral para garantizar la uniformidad de los efectos.

Concluyo afirmando la disposición de Kenya a contribuir a la mejora de los esfuerzos mundiales, los marcos institucionales y las normas que amplíen el potencial de un ciberdominio libre, pacífico y estable, y al mismo tiempo mitiguen las amenazas.

Anexo VII

Declaración de la Representante Permanente de los Estados Unidos de América ante las Naciones Unidas, Linda Thomas-Greenfield

Doy las gracias a la Presidenta y a Estonia por haber organizado este importante debate de hoy. Estamos muy agradecidos a Estonia por atraer la atención del Consejo sobre esta cuestión. Asimismo, doy las gracias a la Alta Representante Nakamitsu por su perspicaz exposición informativa.

Este debate llega en un momento oportuno. Especialmente con la pandemia de enfermedad por coronavirus (COVID-19), nunca hemos dependido tanto de la tecnología, y lo estamos viendo hoy. Pero tanto los actores estatales como los no estatales se aprovechan de esta mayor confianza. En los Estados Unidos, incidentes de programas maliciosos secuestradores de gran repercusión afectaron a JBS, una importante empresa de procesamiento de alimentos, y a Colonial Pipeline, una empresa que suministra combustible a gran parte de nuestra costa este. Estos incidentes demuestran el grave e inaceptable riesgo que la ciberdelincuencia supone para la infraestructura crítica. Los efectos de estas actividades maliciosas tampoco suelen estar contenidos dentro de las fronteras. La ciberactividad maliciosa apuntó a la empresa de *software* SolarWinds, por ejemplo, y al *software* Exchange Server de Microsoft.

El riesgo es claro. Nuestra infraestructura (en línea y fuera de ella) está en juego. Nuestros servicios más básicos y críticos, desde los alimentos que comemos, hasta el agua que bebemos, pasando por los servicios de salud en los que todos confiamos durante la pandemia, son objetivos. Así que, en el mundo actual, cuando hablamos de seguridad mundial, tenemos que hablar de ciberseguridad. Afortunadamente, a pesar de nuestras diferencias ideológicas, los Estados Miembros se han unido en repetidas ocasiones durante la última década para intentar prevenir los conflictos derivados de las cibercapacidades. Juntos, hemos articulado un marco de comportamiento responsable de los Estados en el ciberespacio a través del proceso del Grupo de Expertos Gubernamentales. El marco deja claro que el derecho internacional se aplica al ciberespacio. También se describen a grandes rasgos las normas voluntarias y las medidas prácticas de cooperación que deben adoptar los Estados.

En los últimos meses, el Grupo de Trabajo de Composición Abierta, formado por todos los Estados Miembros, llegó a un consenso sobre un nuevo informe que respalda explícitamente el marco de comportamiento responsable de los Estados en el ciberespacio. Y el mes pasado, la sexta reunión del Grupo de Expertos Gubernamentales de las Naciones Unidas también concluyó con éxito con un sólido conjunto de recomendaciones y nuevas orientaciones sobre el marco. Se trata realmente de progresos. Estos informes proporcionan una orientación real, desde el uso de las cibercapacidades por parte del Estado hasta el planteamiento de la complicada cuestión de la atribución de los ciberincidentes. El marco también considera la forma en que los Estados deben cooperar para mitigar los efectos de la ciberactividad maliciosa significativa que emana del territorio de un Estado en particular, incluidas las actividades realizadas por delincuentes.

Todos nosotros compartimos esta responsabilidad. Como señaló recientemente el Presidente Biden, y cito: “los países deben actuar contra los delincuentes que realizan actividades de programas maliciosos secuestradores en su territorio”. Entonces, permítanme ser clara: cuando se notifica a un Estado de una actividad dañina que surge en su propio territorio, debe tomar medidas razonables para abordarla. Dado el carácter transnacional del ciberespacio, esta cooperación es esencial.

El marco que los Estados Miembros se han esforzado tanto en desarrollar proporciona ahora las reglas de procedimiento. Todos nos hemos comprometido con este marco. Ahora, es el momento de ponerlo en práctica. Tenemos un trabajo importante que hacer para garantizar que todos los Estados que quieran actuar de forma responsable en el ciberespacio tengan tanto los conocimientos políticos como la capacidad técnica para hacerlo. Mientras hacemos este trabajo, también tenemos que seguir protegiendo la libertad de Internet. Los mismos derechos que tienen las personas fuera de línea, incluidos los derechos de libertad de expresión, asociación y reunión pacífica, deben protegerse también en línea.

Los Estados Miembros han demostrado una notable voluntad de salvar las diferencias y llegar a un consenso sobre estas cuestiones. Sigamos mostrando esa buena fe y ofrezcamos al mundo un frente unido en materia de ciberseguridad. Juntos, construiremos un ciberespacio abierto, seguro y estable que beneficie a todos.

Anexo VIII

Declaración del Secretario de Relaciones Exteriores de la India, Harsh Vardhan Shringla

Agradezco a la Presidenta y celebro la iniciativa de Estonia de organizar este debate abierto para poner de relieve uno de los ámbitos emergentes más importantes de la ciberseguridad. También damos las gracias a la Secretaria General Adjunta Nakamitzu por su exposición informativa.

Aunque el significado de la paz ha permanecido constante desde la creación del Consejo de Seguridad, la naturaleza del conflicto y sus instrumentos subyacentes se han transformado enormemente a lo largo de las décadas. Hoy en día, asistimos a un aumento de las amenazas a la seguridad de los Estados Miembros procedentes del ciberespacio, que ya no pueden ser ignoradas. Por lo tanto, el debate abierto es oportuno.

El creciente uso de las cibertecnologías y de las tecnologías de la información y las comunicaciones (TIC) ha acelerado el desarrollo económico, ha mejorado la prestación de servicios a los ciudadanos, ha generado una mayor conciencia social y ha puesto la información y el conocimiento en manos de cada individuo. La mayoría de las actividades de esta era cibernética, políticas, sociales, económicas, humanitarias y de desarrollo (incluida esta reunión de alto nivel del Consejo de Seguridad), se realizan ahora en el ciberespacio o están conectadas a él. La pandemia de enfermedad por coronavirus (COVID-19) no ha hecho sino acelerar y ampliar la digitalización de estas actividades.

La característica dinámica y en continua evolución del ciberespacio también ha llevado a la ciberseguridad al discurso de la paz y la seguridad. La naturaleza sin fronteras del ciberespacio y, lo que es más importante, el anonimato de los actores implicados, han desafiado los conceptos tradicionalmente aceptados de soberanía, jurisdicción y privacidad. Estos atributos únicos del ciberespacio presentan su propio conjunto de numerosos desafíos para los Estados Miembros. En mi intervención me centraré en tres desafíos fundamentales:

En primer lugar, algunos Estados están aprovechando su experiencia en el ciberespacio para lograr sus objetivos políticos y de seguridad y se entregan a formas contemporáneas de terrorismo transfronterizo. El mundo ya está siendo testigo del uso de ciberherramientas para comprometer la seguridad del Estado, entre otras cosas, atacando infraestructuras nacionales críticas, incluidas las instalaciones de salud y energéticas, e incluso perturbando la armonía social mediante la radicalización. Las sociedades abiertas han sido especialmente vulnerables a los ciberataques y a las campañas de desinformación.

En segundo lugar, estamos siendo testigos del sofisticado uso del ciberespacio por parte de los terroristas de todo el mundo para ampliar su atractivo, difundir propaganda virulenta, incitar al odio y a la violencia, reclutar jóvenes y recaudar fondos. Los terroristas también han utilizado los medios sociales para planificar y ejecutar sus ataques terroristas y causar estragos. Como víctima del terrorismo, la India siempre ha subrayado la necesidad de que los Estados Miembros aborden y atajen las implicaciones de la explotación terrorista del ciberdominio de forma más estratégica.

En tercer lugar, la integridad y la seguridad de los productos de las TIC, que forman los bloques de construcción del ciberespacio, están en peligro. Existe la preocupación generalizada de que los agentes estatales y no estatales están introduciendo vulnerabilidades y funciones ocultas perjudiciales, incluso a través de canales de puerta trasera, en las redes y productos de las TIC. Estos actos nefastos socavan la confianza en la cadena de suministro mundial de las TIC, comprometen la seguridad y pueden convertirse en un punto de tensión entre los Estados. Resulta del interés de la comunidad internacional asegurar que todos los actores cumplan con sus obligaciones y compromisos internacionales y que no incurran en prácticas que puedan tener efectos potencialmente perturbadores en las cadenas de suministro mundiales y en el comercio de productos de las TIC.

La interconexión del ciberdominio exige que las soluciones a los complejos problemas y amenazas que emanan del ciberespacio no puedan resolverse de forma aislada. Como Estados Miembros, debemos adoptar un enfoque basado en normas de colaboración en el ciberespacio y trabajar para garantizar su apertura, estabilidad y seguridad. El impulso generado por los resultados positivos del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y con el Grupo de Trabajo de Composición Abierta sobre los avances en las TIC debería aprovecharse para encontrar más terreno común y mejorar las cibernormas y normas ya acordadas. Estas normas deben tratar de garantizar la ciberseguridad colectiva mediante la cooperación internacional. La participación de los múltiples interesados será clave para lograr este objetivo.

Fomentar el acceso equitativo al ciberespacio y sus beneficios también debería ser un componente importante de esta cooperación internacional. El aumento de las “brechas digitales” y de las “brechas de conocimiento digital” entre los países crea un entorno insostenible en el ciberdominio. La creciente dependencia digital en la era posterior a la enfermedad por coronavirus (COVID) ha exacerbado los riesgos y expuesto estas fisuras de las desigualdades digitales. Estos problemas deben solucionarse mediante la creación de capacidad. La naturaleza omnipresente y sin fronteras del ciberespacio implica que solo somos tan fuertes como el eslabón más débil de la red global. “Solo juntos” podemos alcanzar el objetivo de un ciberespacio seguro y resistente a nivel mundial, y debemos asegurarnos de que ningún país se quede atrás en este esfuerzo colectivo.

La India está comprometida con un entorno de ciberespacio abierto, seguro, libre, accesible y estable, que se convierta en un motor de innovación, crecimiento económico y desarrollo sostenible, que garantice la libre circulación de la información y respete la diversidad cultural y lingüística. Con nuestras iniciativas tecnológicas transformadoras de los últimos años, como IndiaStack, Aadhar y UPI, hemos aprovechado con éxito el tremendo potencial de las cibertecnologías para aplicar la Agenda 2030 para el Desarrollo Sostenible y mejorar la gobernanza. Como parte de su campaña de vacunación por COVID, una de las mayores del mundo, la India ha desarrollado Co-WIN, una plataforma tecnológica escalable, inclusiva y abierta. La plataforma Co-WIN puede personalizarse y ampliarse para intervenciones de salud en todo el mundo. Estamos trabajando para compartir esta plataforma con los países asociados.

Nuestro objetivo general es aprovechar el ciberespacio para el crecimiento y el empoderamiento de las personas, no solo de nuestro país, sino de toda la humanidad. La India está dispuesta a ofrecer sus conocimientos y compartir su experiencia en esta empresa.

Anexo IX

Declaración de la Ministra de Estado a cargo de Relaciones Exteriores y Comercio Exterior de San Vicente y las Granadinas, Keisal M. Peters

Quisiéramos expresar nuestro agradecimiento a la presidencia estonia por su iniciativa de celebrar el debate abierto de alto nivel de hoy sobre un tema de importancia crítica, para hacer balance de la actuación del Consejo de Seguridad en su tarea de mantener la paz y la seguridad internacionales. Permítaseme también expresar mi agradecimiento a todos los ponentes hoy por sus perspicaces presentaciones.

En el mundo contemporáneo, el ciberespacio afecta a casi todos los aspectos de nuestra vida cotidiana. El papel de las tecnologías de la información y las comunicaciones (TIC) en la obtención de beneficios económicos y sociales es evidente. Sin embargo, a pesar de estos beneficios, el mundo debe seguir siendo consciente de los graves problemas de las TIC que existen. El entorno mundial de las TIC se enfrenta a un dramático aumento del uso malicioso de las mismas por parte de actores estatales y no estatales. Sin duda, el uso indebido de las TIC supone un riesgo para todos los Estados y tiene el potencial de afectar negativamente a la paz y la seguridad internacionales. Por lo tanto, es imperativo que nos basemos en un compromiso anterior para generar medidas de fomento de la confianza que mejoren la paz y la seguridad internacionales y aumenten la cooperación, la transparencia, la previsibilidad y la estabilidad entre los Estados Miembros en este ámbito.

Un entorno de las TIC que sea abierto, seguro, estable, accesible y pacífico es esencial para todas las personas y requiere una cooperación eficaz entre los Estados a fin de reducir los riesgos para la paz y la seguridad internacionales. Además, otros actores con diferentes capacidades y aptitudes de los distintos sectores en todos los niveles de la cadena global de las TIC, tienen un *papel clave para garantizar la ciberseguridad.* Debemos explorar las posibilidades de aumentar la creación de capacidad y los recursos de asistencia técnica. Las Naciones Unidas tienen que mejorar la asistencia a los Estados Miembros y seguir ayudando a garantizar la coherencia de los esfuerzos entre la gama de entidades de las Naciones Unidas que participan en el ciberespacio. Estos esfuerzos deben estar vinculados a los objetivos más amplios de la Organización.

A pesar de nuestros numerosos desafíos como pequeño Estado insular en desarrollo, San Vicente y las Granadinas ha tomado medidas concretas para mejorar su capacidad de hacer frente a la lacra de la ciberdelincuencia. Dos leyes, la Ley de Pruebas Electrónicas (2004) y la Ley de Transacciones Electrónicas (2007), sustentan un marco legislativo básico para la ciberseguridad en el país. En agosto de 2016, los legisladores convirtieron en ley el Proyecto de Ley de Ciberdelincuencia de 2016, dotando así al país de un derecho sustantivo y procesal para poder hacer frente a la ciberdelincuencia con mayor eficacia. También estamos comprometidos con nuestros acuerdos regionales de ciberseguridad en el seno de la OEA y la CARICOM.

Debido a la pandemia de enfermedad por coronavirus (COVID-19) y a las nuevas disrupciones debidas a nuestra reciente erupción volcánica, las escuelas de nuestro país han pasado a la enseñanza a distancia, como ocurre en todo el mundo. Con miles de niños que reciben tabletas del Gobierno para facilitar esta transición, ha aumentado el volumen de uso de Internet y el tiempo de pantalla. Teniendo en cuenta esto, el Ministerio de Educación y Reconciliación Nacional se ha embarcado en una campaña #GoCyberSmart para promover la ciberseguridad. La campaña es una iniciativa de concienciación para que los estudiantes tomen las decisiones digitales correctas. Las tres áreas de interés son la seguridad de la información, la seguridad del hardware y la navegación segura por Internet.

La importancia del intercambio de información entre los Estados Miembros y las organizaciones regionales e internacionales es esencial para garantizar la estabilidad y evitar la escalada de incidentes de ciberseguridad. Además, exhortamos a los Estados Miembros que sigan comprometidos con el derecho internacional y con el marco de comportamiento responsable de los Estados en el ciberespacio.

En nuestro esfuerzo por avanzar en el comportamiento responsable de los Estados en el ciberespacio en el contexto de la paz y la seguridad internacionales, debemos guiarnos por las evaluaciones y recomendaciones contenidas en los informes consensuados del Grupo de Expertos Gubernamentales en 2010, 2013, 2015 y el más reciente en 2021, así como por las conclusiones y recomendaciones del informe final del Grupo de Trabajo de Composición Abierta de las Naciones Unidas.

En conclusión, si no se llega a un acuerdo sobre las reglas de enfrentamiento, las normas políticas y los mecanismos de cooperación internacional para un entorno pacífico de las TIC, solo se obtendrán nuevas fuentes de inestabilidad y conflicto. En el ciberespacio, alentamos a todos los actores de la comunidad internacional a cumplir con sus obligaciones legales internacionales, incluido el respeto a la soberanía y la independencia política consagradas en la Carta de las Naciones Unidas, así como los principios para la resolución pacífica de conflictos de la misma manera que en el mundo físico. El impulso urgente para mantener la paz y la seguridad internacionales en el ciberespacio no debe detenerse nunca.

Anexo X

Declaración del Viceministro de Relaciones Exteriores de Noruega, Audun Halvorsen

Un ciberespacio globalmente accesible, libre, abierto y seguro es esencial para mantener la paz y la seguridad internacionales. Nos alegramos de que Estonia haya señalado este tema al Consejo de Seguridad, el principal órgano de las Naciones Unidas responsable del mantenimiento de la paz y la seguridad internacionales, de conformidad con la Carta de las Naciones Unidas.

Las tecnologías de la información y las comunicaciones (TIC) son una parte fundamental de la infraestructura mundial. Están en el centro del desarrollo, la estabilidad y la seguridad de todos los Estados. Sin embargo, el ciberespacio se está convirtiendo cada vez más en un escenario de competencia y de posibles conflictos entre Estados.

Hemos sido testigos en la última década de cómo las ciberoperaciones maliciosas por parte de Estados y actores no estatales han aumentado en alcance, escala, gravedad y complejidad. Nos encontramos en medio de una pandemia mundial, en la que incluso las infraestructuras críticas de salud han estado entre los objetivos de esta actividad maliciosa, poniendo en riesgo la seguridad de los ciudadanos y nuestros esfuerzos globales para gestionar la crisis de la COVID.

Sin embargo, también hay motivos para ser optimistas. En este último año se ha demostrado que la comunidad internacional está dispuesta a estar a la altura de las circunstancias y a trabajar de forma conjunta para promover un comportamiento responsable de los Estados en el ciberespacio. Los informes consensuados del Grupo de Trabajo de Composición Abierta y del Grupo de Expertos Gubernamentales demuestran el compromiso de todos los Estados Miembros de defender el orden internacional basado en normas en el ciberespacio. Es una victoria del multilateralismo.

La afirmación de la aplicabilidad del derecho internacional al ciberespacio es la piedra angular de los informes aprobados por consenso del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta. El derecho internacional es la base del compromiso compartido por los Estados de prevenir conflictos y mantener la paz y la seguridad internacionales. Es clave para aumentar la confianza entre los Estados. Ambos informes reafirmaron 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 las TIC.

Consideramos que es un gran avance que el informe del Grupo de Expertos Gubernamentales haya reconocido que el derecho internacional humanitario se aplica en todos los conflictos armados, también en el contexto cibernético.

El derecho internacional humanitario apunta a minimizar el sufrimiento de las personas provocado por el conflicto armado. Regula y limita las ciberoperaciones durante conflictos armados, así como también regula y limita cualquier otro medio y método de guerra. En consecuencia, están prohibidos los ataques contra civiles o bienes de carácter civil, y los servicios médicos deben ser protegidos y respetados.

Por lo tanto, está prohibido atacar la infraestructura crítica, como el suministro de energía, la producción de alimentos, las instalaciones de agua potable u otros objetos indispensables para la supervivencia de la población.

Reconocer la aplicabilidad del derecho internacional humanitario en el ciberespacio no legitima la ciberguerra. Todo uso de la fuerza por parte de los Estados sigue rigiéndose por la Carta de las Naciones Unidas y las normas consuetudinarias de derecho internacional. Las disputas internacionales deben solucionarse de forma pacífica, en el ciberespacio y en el resto de las esferas.

Presidenta:

Todos los Estados Miembros han apoyado un marco de comportamiento responsable de los Estados en el ciberespacio. Un marco basado en: la aplicabilidad del derecho internacional, la adhesión a las normas voluntarias acordadas, las medidas prácticas de fomento de la confianza y los esfuerzos de creación de capacidad para reforzar la resistencia y la seguridad de todos. Este es un gran logro; pero solo puede alcanzarse su valor mediante la implementación y el cumplimiento por parte de todos los Estados.

La reunión de hoy es un reconocimiento de que las actividades maliciosas en el ciberespacio pueden afectar de forma grave la paz y la seguridad internacionales. La reunión de hoy también es una señal clara para todos los Estados de que se espera que estemos a la altura del marco para el comportamiento responsable de los Estados en el ciberespacio que hemos acordado: que debemos cumplir con nuestras obligaciones en virtud del derecho internacional y adherirnos a las normas que hemos acordado.

Anexo XI

Declaración del Ministro de Estado para el Commonwealth, las Naciones Unidas y Asia Meridional del Reino Unido de Gran Bretaña e Irlanda del Norte, Lord Ahmad de Wimbledon

Hoy en día, casi todo tiene una dimensión digital.

La comunidad internacional debe aprovechar las enormes oportunidades que ofrece Internet para el aprendizaje, los negocios, la comunicación y, de hecho, el entretenimiento.

Sin embargo, también debemos tratar las amenazas que conlleva con la seriedad que merecen.

Las amenazas que plantea la actividad maliciosa y peligrosa en el ciberespacio son ahora más claras que nunca.

De hecho, el mes pasado, una banda de delincuentes atacó Colonial Pipeline, pidió un rescate por el mayor oleoducto de combustible de los Estados Unidos, y amenazó con provocar una grave disrupción económica.

Parte de esta actividad apunta al robo o la extorsión. Con frecuencia, se trata simplemente de un sabotaje y una disrupción.

Sin embargo, tenemos la responsabilidad colectiva, como comunidad internacional, de crear un ciberespacio que beneficie a todos los países y, de hecho, a todas las personas. Juntos, deberíamos darles forma a las normas que sirven al bien común.

Por supuesto, no partimos de cero en este sentido.

Hace diez años, el Reino Unido reunió a más de 60 países en Londres para establecer principios básicos como el acceso universal a Internet y la protección de los derechos individuales en línea.

Diez años después, hemos avanzado mucho.

Este mismo año, la Asamblea General reafirmó por unanimidad la aplicación del derecho internacional en el ciberespacio y acordó una serie de principios voluntarios, entre los que se encuentra la importancia de proteger las infraestructuras de salud.

Un Grupo de Expertos Gubernamentales avanzó en nuestra comprensión de las normas, reglas y principios del ciberespacio, y estableció interpretaciones claras acerca de cómo se aplica el derecho internacional.

No obstante, queremos avanzar aún más. No es ningún secreto que los Estados están desarrollando ciberoperaciones para apoyar sus capacidades militares y de seguridad nacional. De hecho, el Reino Unido es uno de ellos.

Seré claro: utilizaremos estas capacidades para defendernos de quienes pretenden hacernos daño. Nos comprometemos a utilizar estas capacidades cuando sea necesario, de forma proporcionada y con arreglo al derecho internacional.

Nuestro reto colectivo es aclarar cómo se aplican las normas del derecho internacional a las actividades de los Estados en el ciberespacio, evitar que los actores malintencionados no respeten las normas y aplicar las consecuencias a los que cometen actividades cibernéticas malintencionadas.

El Reino Unido se compromete a trabajar con todos los países, y con sus numerosos interesados, para garantizar que el ciberespacio se rija por reglas y normas que mejoren nuestra seguridad colectiva.

Reglas y normas que promuevan los valores democráticos, reglas y normas que apoyen el crecimiento económico mundial y que contrarresten la expansión del autoritarismo digital.

Debemos proteger el estado de derecho en el ciberespacio: encarnar el comportamiento responsable de los Estados, incentivar el cumplimiento, disuadir los ataques y, de hecho, hacer que otros rindan cuentas por el comportamiento irresponsable de los Estados.

También debemos dar prioridad absoluta y garantizar la protección de los derechos humanos en línea, al igual que fuera de ella, para garantizar que construyamos un ciberespacio libre, abierto, pacífico y seguro, accesible para todos.

El marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio es nuestro punto de partida. Debemos apoyar a todos los Estados para que lo apliquen ahora.

El Reino Unido tuvo el placer de anunciar el mes pasado que invertirá más de 30 millones de dólares para apoyar la creación de capacidad relacionada con la cibernética en países vulnerables, en particular en África y el Indo-Pacífico.

Nuestro trabajo con Interpol ayudará a países como Etiopía, Ghana, Nigeria, Rwanda y Kenya a apoyar operaciones conjuntas contra los ciberdelincuentes.

En otros lugares, la financiación británica ayudará a crear equipos nacionales de respuesta de emergencia para proteger a los países contra estas amenazas.

Por supuesto, no podríamos hacer nada de esto sin nuestros asociados del sector privado y, por supuesto, de la sociedad académica y civil.

Sin embargo, en todo esto, al reunirnos hoy aquí, el Consejo de Seguridad también tiene un papel fundamental e importante que desempeñar.

Cuando las actividades maliciosas plantean un riesgo para la paz y la seguridad internacionales, exacerbando el conflicto o causando sufrimiento humanitario, el Consejo de Seguridad debe estar preparado para responder.

El Consejo debe responder de la misma manera que lo haría a las amenazas planteadas por medios convencionales.

Tenemos la oportunidad de aprovechar las oportunidades del ciberespacio y garantizar que siga siendo una fuerza de prosperidad y progreso para todos.

Para ello, es vital que trabajemos juntos para contrarrestar a quienes quieren poner en riesgo nuestra seguridad colectiva.

Y permítanme asegurarles esto: el Reino Unido está plenamente comprometido con la protección de un ciberespacio libre, abierto, pacífico y seguro para las generaciones venideras.

Anexo XII

Declaración del Ministro Delegado del Ministro de Europa y Relaciones Exteriores de Francia, Franck Riester

[Original: francés]

Quisiera dar las gracias a la Primera Ministra de Estonia por organizar este acto. El Consejo de Seguridad vela por el mantenimiento de la paz y la seguridad internacionales y debe poder hacerlo en el ciberespacio.

El ciberespacio es un lugar de oportunidades pero también de nuevas amenazas. Se ha convertido en un terreno de competencia estratégica entre potencias. Están proliferando los usos maliciosos de las tecnologías de la información y las comunicaciones (TIC) por parte de actores tanto estatales como no estatales.

Lo hemos constatado durante estos últimos meses, en particular en el contexto de la pandemia de enfermedad por coronavirus (COVID-19), que ha acentuado nuestra dependencia de estas tecnologías. Me refiero, en primer lugar, a los deleznables ciberataques con programas informáticos secuestradores contra hospitales y otras infraestructuras críticas. Quiero expresar la solidaridad de Francia con las víctimas de estos ataques. Me refiero asimismo a las campañas de manipulación de la información a través de la propagación de “infodemias” o a la fragmentación creciente de Internet, unas prácticas que son contrarias a los valores democráticos. Las acciones en el ciberespacio tienen consecuencias reales que pueden resultar brutales en nuestras vidas y nuestras sociedades.

El desafío para el próximo siglo será construir una gobernanza y una regulación colectiva del ciberespacio. No queremos un “lejano Oeste digital” ni una compartimentación del ciberespacio. Lo hemos afirmado en el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, así como en el marco del Grupo de los Siete (G7) mediante la declaración de Declaración de Dinard sobre la iniciativa para las normas en el ciberespacio. Francia está decidida a construir junto con sus asociados un ciberespacio abierto, seguro, estable, no fragmentado, accesible y pacífico.

El derecho internacional, incluida la Carta de las Naciones Unidas, se aplica en su totalidad al ciberespacio, lo que implica también respetar el derecho internacional humanitario en las operaciones cibernéticas llevadas a cabo durante los conflictos armados.

Ante la multiplicación de las amenazas en el ciberespacio y los ciberataques, los Gobiernos deben responder mediante la cooperación y el derecho. Desde hace más de un decenio, Francia ha desempeñado un papel pionero en el marco de distintas tareas multilaterales. Estas tareas han permitido el surgimiento de un marco para el comportamiento responsable de los Estados en su uso de las TIC. Dicho marco se basa en el derecho internacional, en un conjunto coherente de normas de comportamiento no vinculantes y en medidas de transparencia y fomento de la confianza. Permite impulsar la cooperación y el entendimiento mutuo entre Estados en el ciberespacio. Quisiera elogiar los éxitos recientes del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y del sexto Grupo

de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, que han adoptado dos informes equilibrados, útiles y consensuados. Francia está dispuesta a seguir participando de manera constructiva en los debates multilaterales en las Naciones Unidas, en particular en el marco del nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) creado en virtud de la resolución 75/240 de la Asamblea General.

Sobre todo, ahora hay que poner en práctica de manera concreta las normas y principios acordados. Francia, junto con 52 asociados, propone crear un Programa de Acción sobre Ciberseguridad en el marco de las Naciones Unidas. Este nuevo instrumento, complementario al nuevo grupo de trabajo, permitirá crear una estructura permanente. Tendrá por objeto sostener la creación de capacidades y crear espacios de diálogo con la sociedad civil, los investigadores y los actores privados. Francia está abierta al diálogo con el conjunto de los Estados y partes interesadas para precisar y construir esta propuesta orientada a la acción.

Este compromiso colectivo de múltiples actores es esencial. En el ciberespacio, los Estados tienen sin duda responsabilidades que ningún otro actor puede asumir, pero no pueden actuar solos. Debemos embarcarnos plenamente en esta nueva forma de diplomacia.

Anexo XIII

Declaración del Representante Permanente de China, Zhang Jun

[Original: chino]

En el mundo actual, se está desplegando una nueva ronda de revolución tecnológica y transformación industrial, y las tecnologías digitales y de Internet se están desarrollando rápidamente, lo que ha cambiado en gran medida el modo de producción y los estilos de vida de la humanidad, promoviendo el desarrollo económico y social del país. Mientras tanto, la cibervigilancia, los ataques, los delitos y el terrorismo se han convertido en peligros públicos mundiales y el ciberespacio está cada vez más militarizado, politizado y centrado en la ideología, lo que sobre interpreta el concepto de seguridad. En el ciberespacio, los países no solo disfrutan de oportunidades compartidas e intereses comunes, sino que también se enfrentan a retos comunes y asumen responsabilidades compartidas. Cada vez más, se convierten en una comunidad con un futuro compartido en las buenas y en las malas.

El Presidente chino, Xi Jinping, declaró que, si bien los países tienen diferentes condiciones nacionales y etapas de desarrollo de Internet, además de diferentes retos sobre el terreno, comparten el mismo deseo de hacer avanzar la economía digital, los mismos intereses para hacer frente a los retos de la ciberseguridad y las mismas necesidades de reforzar la gobernanza del ciberespacio. China siempre cree que la comunidad internacional debe colaborar en un esfuerzo conjunto para proteger la ciberseguridad y mantener la paz internacional.

- Debemos promover la seguridad mediante el mantenimiento de la paz y evitar que el ciberespacio se convierta en un nuevo campo de batalla. La comunidad internacional debe atenerse a los propósitos y principios de la Carta de las Naciones Unidas, en particular los de igualdad soberana, la prohibición del uso de la fuerza, la no injerencia en los asuntos internos y el arreglo pacífico de las controversias. Es esencial respetar los derechos de todos los países a elegir de forma independiente la vía de desarrollo y el modelo de gestión de Internet, y a participar en la gobernanza del ciberespacio en igualdad de condiciones. Los países deben abstenerse de realizar actividades cibernéticas que pongan en peligro la seguridad de otros países. La aplicación del derecho de los conflictos armados en el ciberespacio debe tratarse con cautela y deben evitarse las carreras armamentísticas en el ciberespacio.

- Debemos promover la seguridad a través de los intercambios y la cooperación y crear un entorno favorable para el ciberespacio. Salvaguardar la seguridad en Internet es un tema global, y ningún país puede mantenerse al margen o gestionarlo en solitario. El hegemonismo, el unilateralismo y el proteccionismo en el ciberespacio solo intensificarán los enfrentamientos y envenenarán el ambiente de cooperación, algo que la comunidad internacional debe rechazar y combatir. Los países deben colaborar para profundizar en los intercambios y la cooperación en materia de investigación y desarrollo tecnológico, elaboración de normas e intercambio de información, y frenar conjuntamente el abuso de las tecnologías de la información. Debemos oponernos conjuntamente a la cibervigilancia y a los ataques, combatir el ciberterrorismo y los delitos, y mejorar las capacidades de ciberseguridad. Es esencial proporcionarles a las

empresas un entorno comercial abierto, justo y no discriminatorio, garantizar la apertura, la estabilidad y la seguridad de la cadena mundial de la industria de las TI y de la cadena de suministro, promover el desarrollo saludable de la economía mundial y evitar la interferencia humana en las operaciones comerciales normales de las empresas bajo cualquier pretexto.

- Debemos promover la seguridad mediante la mejora de la gobernanza y fomentar la equidad y la justicia en el ciberespacio. Todos los países deben defender el multilateralismo efectivo, establecer un proceso de gobernanza de la ciberseguridad abierto, inclusivo y sostenible en el marco de las Naciones Unidas con la participación equitativa de todos, formular normas internacionales para el ciberespacio que sean generalmente aceptadas por todos los países, y oponerse a los círculos pequeños y a la política de grupo. China valora muy positivamente la conclusión satisfactoria del informe del Grupo de Trabajo de Composición Abierta como del Grupo de Expertos Gubernamentales sobre ciberseguridad, y espera que el nuevo Grupo de Trabajo de Composición Abierta haga nuevas contribuciones para mantener la ciberseguridad. Estamos dispuestos a trabajar con todas las partes para promover, en el marco de las Naciones Unidas, el desarrollo de una convención internacional contra la ciberdelincuencia. Con un espíritu de consultas amplias, contribuciones conjuntas y beneficios compartidos, deberíamos aprovechar plenamente el papel de los múltiples interesados, como los Gobiernos, las empresas de Internet, las comunidades tecnológicas, la sociedad civil y los ciudadanos individuales.

- Debemos promover la seguridad a través del desarrollo inclusivo y lograr una prosperidad compartida en el ciberespacio. El actual desarrollo económico mundial es lento. La tecnología digital y de Internet puede convertirse en importantes motores para la recuperación y el restablecimiento del desarrollo económico y social de los países tras la pandemia. Los países deben adoptar políticas más proactivas, inclusivas y coordinadas para promover un desarrollo equilibrado de las TIC a escala mundial, desarrollar con vigor nuevos modelos y formatos como la economía digital, y oponerse a la hegemonía tecnológica. Debemos avanzar en el desarrollo de la infraestructura digital y la conectividad, derribar las barreras de la información, reducir las brechas digitales y ayudar a los países en desarrollo a ser más digitales, conectados e inteligentes, a fin de aplicar la Agenda 2030 para el Desarrollo Sostenible. Debemos intensificar la cooperación y la asistencia en materia de ciberseguridad con los países en desarrollo, y mejorar sus capacidades de alerta temprana, prevención y respuesta de emergencia ante incidentes de ciberseguridad.

China concede gran importancia a la seguridad y la informatización de Internet, y se ha comprometido a construir una economía digital, una sociedad y un gobierno digitales utilizando la transformación digital para impulsar cambios en el modo de producción, los estilos de vida y el modelo de gobernanza. China continuará mejorando sus leyes, reglamentos y normas institucionales nacionales de ciberseguridad sobre la base de la Ley de Ciberseguridad y la Ley de Seguridad de Datos.

El año pasado, China presentó la Iniciativa Mundial de Seguridad de los Datos, centrada en cuestiones importantes como la protección de la infraestructura crítica y la información personal, el almacenamiento y la recuperación de datos corporativos

en el extranjero y la seguridad de la cadena de suministro, lo que proporcionó una solución constructiva para mantener la seguridad mundial de los datos y de Internet. Recientemente, China, junto con la Liga de los Estados Árabes, publicó la iniciativa de cooperación en materia de seguridad de datos entre China y los países árabes, en la que se plasmaba el llamamiento conjunto de ambas partes para el mantenimiento de la seguridad de Internet y de los datos. Acogemos con satisfacción la respuesta activa de todas las partes y su participación en la iniciativa, con el fin de formular conjuntamente normas mundiales para la gobernanza digital. China también está impulsando activamente el desarrollo de la iniciativa de la Ruta de la Seda digital, y trabaja con otros países para construir un nuevo paisaje orientado al futuro, inteligente e interconectado.

El ciberespacio encarna el sueño de la humanidad, y tiene que ver con el bienestar, la paz y la seguridad de las personas, China está dispuesta a trabajar con todos los países para aprovechar la oportunidad de la revolución de la información, fomentar el nuevo impulso de la innovación y el desarrollo, crear un nuevo panorama de cooperación digital y ciberseguridad, construir una comunidad con un futuro compartido en el ciberespacio, y trabajar juntos para crear un futuro mejor para la humanidad.

Anexo XIV

Declaración de la Misión Permanente de México ante las Naciones Unidas

[Original: español]

México agradece la convocatoria a este debate abierto y la presentación de la Secretaria General Adjunta y Alta Representante para Asuntos de Desarme, Izumi Nakamitsu.

Como bien hemos escuchado aquí, al igual que en numerosos foros, la creciente importancia del ciberespacio es innegable. El mundo se ha hecho cada vez más dependiente de las tecnologías de la información y las telecomunicaciones y, sobremanera, en el contexto de la pandemia. Las relaciones internacionales también han incursionado velozmente en el plano virtual, por lo que el Consejo de Seguridad no podrá, ni debe, ser ajeno a sus implicaciones sobre la paz y la seguridad internacionales.

Aun cuando casi la mitad de la población mundial no tiene acceso a internet, esto no la exime de ser víctima de alguno de los miles de ataques cibernéticos que, día con día, se producen contra redes gubernamentales, entidades bancarias o financieras, instituciones de investigación e incluso sanitarias.

Estos riesgos latentes han llevado a distintos órganos del sistema de Naciones Unidas a atender amenazas y buscar acuerdos entre los Estados, para asegurar que el ciberespacio no se utilice con fines criminales, hostiles y hasta terroristas, sin perder de vista el equilibrio con los usos pacíficos y las enormes oportunidades que el ciberespacio ofrece para el desarrollo sostenible.

México considera esencial prevenir cualquier escalada de situaciones de riesgo en materia de ciberseguridad. El uso del ciberespacio, como cualquier otro ámbito físico, debería regularse a través de lineamientos y parámetros muy claros, al tiempo que resulta necesario contribuir a la promoción de un ciberespacio abierto, libre, seguro, estable, accesible y resiliente.

Es por ello que México aplaude la exitosa conclusión de los trabajos del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, que permitieron la adopción de informes sustantivos por consenso, los cuales constituyen precedentes fundamentales para el trabajo multilateral. Para mi país, este hecho reafirma la confianza que predomina en el multilateralismo, y el papel constructivo de las Naciones Unidas para alcanzar respuestas integrales, legítimas y de largo plazo sobre los retos del ciberespacio y las tecnologías de la información y las telecomunicaciones.

Sin embargo, esto no es suficiente. Es necesario seguir avanzando en la plena instrumentación del derecho internacional en el ciberespacio, incluyendo no solo la Carta de las Naciones Unidas, sino también el derecho internacional de los derechos humanos, el derecho internacional humanitario y el desarrollo de jurisprudencia al amparo de éstos.

Nuestra convicción se apega a una mayor transparencia en las actividades del ciberespacio, a la rendición de cuentas, y al llamado a la instrumentación de normas

para el comportamiento responsable de los Estados, adoptadas por la propia Asamblea General, y que se complementan con las medidas de fomento a la cooperación internacional para la creación y el fortalecimiento de las capacidades cibernéticas de los Estados.

México espera que, en las deliberaciones y trabajos futuros del Consejo de Seguridad, se haga eco de las voces crecientes de actores de la sociedad civil, la academia y el sector privado, que señalan —con razón— un objetivo común: asegurar los usos pacíficos del ciberespacio para el desarrollo y el uso de las tecnologías digitales.

Anexo XV

Declaración del Representante Permanente de la Federación de Rusia ante las Naciones Unidas, V. A. Nebenzia

[Original: ruso]

El año transcurrido desde el inicio de la pandemia de enfermedad por coronavirus (COVID-19) ha sido un gran reto para el mundo, recordado sobre todo por sus desafíos y pérdidas. También se han visto afectados muchos esfuerzos diplomáticos, con negociaciones estancadas en varios frentes.

Sin embargo, hay al menos una excepción positiva en este contexto. Se trata del debate multilateral sobre la seguridad de la información internacional en las Naciones Unidas. Ha logrado no sólo mantener su impulso, sino también alcanzar, me atrevería a decir, resultados históricos. Los dos órganos de expertos pertinentes de la Asamblea General de las Naciones Unidas —el Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta— pudieron acordar por consenso los informes finales.

Las negociaciones en estos grupos no fueron fáciles. Esto hace que el resultado conseguido sea todavía más valioso. Dicho resultado demostró claramente que la comunidad internacional puede ponerse de acuerdo en cuestiones clave cuando el diálogo es pragmático, despolitizado y constructivo. Gracias a estos esfuerzos, nos encontramos en el umbral de una nueva e importante fase, que se inicia en junio de 2021 durante la sesión organizativa del nuevo Grupo de Trabajo de Composición Abierta 2021-2025.

Consideramos que este resultado es un logro colectivo de la comunidad internacional. Por nuestra parte, llevamos decenios intentando contribuir al proceso de establecimiento de un sistema global de seguridad de la información internacional. Fue Rusia quien ya en 1998 planteó por primera vez en las Naciones Unidas la necesidad de combatir las amenazas en el ámbito de la seguridad de la información internacional, proponiendo una resolución al respecto a la Asamblea General de las Naciones Unidas. A principios de la década del año 2000, propusimos la creación de un grupo de expertos para debatir el tema de la seguridad de la información internacional: el Grupo de Expertos Gubernamentales. Cuando quedó claro que este tema había “rebasado” el ámbito limitado del grupo de expertos, nosotros, en respuesta a una petición de la comunidad internacional, junto con personas de ideas afines, iniciamos en 2019 un proceso de negociación abierto y democrático sobre la seguridad de la información internacional, con la participación de todos los Estados Miembros en el Grupo de Trabajo de Composición Abierta.

Se ha superado así un hito muy importante. Por primera vez, una “mayoría de las Naciones Unidas” tuvo acceso al debate sobre la seguridad digital. Nuestra lógica es muy sencilla: abogamos por un diálogo igualitario y mutuamente respetuoso. Si todos somos iguales ante las amenazas a la seguridad de la información internacional, no debería haber debates entre un estrecho círculo de estados tecnológicamente avanzados, sino que entre todos los miembros de las Naciones Unidas. No debería haber ninguna imposición por parte de quienes se consideran más “avanzados”.

Nuestras propuestas, tanto en su momento con el Grupo de Expertos Gubernamentales como posteriormente con el Grupo de Trabajo de Composición Abierta, no fueron de agrado de todos de manera inmediata. Varios Estados, incluidos los participantes en la reunión de hoy, han votado en contra de su creación. Sin embargo, poco a poco se fueron sumando al debate y se involucraron en él de forma enérgica y constructiva.

La diplomacia multilateral eficaz sobre la seguridad de la información internacional en las Naciones Unidas, que complementa el compromiso bilateral de los Estados sobre este tema, es un excelente ejemplo de cómo resolver estas cuestiones para reducir la desconfianza mutua y disipar las preocupaciones, a diferencia de la famosa diplomacia basada en un uso selectivo de los medios de comunicación a la que, lamentablemente, a veces recurren algunos de nuestros socios.

Desgraciadamente, en paralelo, observamos una peligrosa tendencia consistente en tratar de imponer al Consejo de Seguridad de las Naciones Unidas interpretaciones unilaterales de los acuerdos adoptados en el marco del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, solicitándole en realidad que refrende o, peor aún, que revise los resultados de los debates mantenidos en órganos especializados correspondientes de las Asambleas Generales de las Naciones Unidas. Consideramos que estos intentos son destructivos. Están empujando a la comunidad internacional hacia escenarios de confrontación imprevisibles e indeseables.

Más concretamente, se trata del deseo de algunos países de justificar las presiones y sanciones unilaterales contra otros Estados Miembros, así como el posible uso de la fuerza contra ellos, mediante la distorsión de los acuerdos alcanzados, incluidos los acuerdos que versan sobre los aspectos jurídicos internacionales del uso de las tecnologías de la información y las comunicaciones (TIC). Es sumamente preocupante que una serie de Estados avanzados desde el punto de vista tecnológico estén buscando activamente la militarización del ciberespacio al promover el concepto de “ciberataques militares preventivos”, entre otras cosas, contra infraestructura crítica. Estas doctrinas de confrontación contradicen su compromiso manifestado, incluso hoy, con la prevención de conflictos en el uso de las TIC. Lo vemos como un intento de imponer sus propias “reglas del juego” en la esfera de la información desde una posición de fuerza.

Quiero insistir en que, aunque la esfera digital no está desregulada, el debate sobre cómo se puede aplicarle exactamente el derecho internacional está lejos de haber terminado. Estas cuestiones se debatirán durante al menos otros cinco años en un foro específico bajo los auspicios de la Asamblea General de las Naciones Unidas, en el marco de un nuevo grupo de trabajo de composición abierta.

Los informes del grupo final de expertos gubernamentales y del grupo de trabajo de composición abierta a este respecto representan un conjunto claro y equilibrado de entendimientos, incluida la necesidad de nuevas normas de comportamiento responsable de los Estados en el ciberespacio que reflejen sus especificidades. La lista inicial de estas normas está reflejada en la resolución de la Asamblea General de las Naciones Unidas de 2018 sobre la seguridad de la información internacional, adoptada por iniciativa de Rusia. Hoy, por desgracia, observamos intentos de escoger a conveniencia de dicho conjunto de normas algunas de las disposiciones más favorables para nuestros colegas occidentales, conforme a una interpretación errónea

de la aplicabilidad “automática” del derecho internacional en materia digital, que también permite el uso de la fuerza, y de presentar sus puntos de vista nacionales como el resultado de un consenso global. En consecuencia, nos opondremos a cualquier intento de revisar, a través del Consejo de Seguridad de las Naciones Unidas, los acuerdos equilibrados alcanzados en el marco de órganos especializados de la Asamblea General.

Los puntos de partida doctrinales adoptados por Rusia en relación con la creación de un régimen global de seguridad de la información internacional, según ha señalado el Presidente de la Federación de Rusia, V. V. Putin, durante una reunión del Consejo de Seguridad de la Federación Rusa el 26 de marzo de 2021, siguen siendo abiertos, transparentes y sin cambios. Están recogidos en el Marco de Política de Seguridad de la Información del Estado, que el Presidente Putin aprobó en abril de 2021. Se trata de un documento público, por lo que insto a todos a que lo lean.

Nuestra doctrina se basa en la tesis de utilizar las TIC sólo con fines pacíficos, ante la necesidad de prevenir los conflictos en el espacio de la información y la importancia de reforzar la cooperación multilateral y bilateral en este sentido. Consideramos que es importante que existan acuerdos jurídicos internacionales universales que permitan llevar a cabo estas tareas con eficacia. En el camino hacia este objetivo, es necesario desarrollar y acordar conjuntamente normas universales, justas, exhaustivas y realistas para el comportamiento de los Estados en el espacio de la información, delimitar claramente las acciones permisibles y las no permisibles en él, y hacer que estas normas sean jurídicamente vinculantes para que sean estrictamente observadas por todos los Estados.

Nuestra postura consiste en apoyar la inviolabilidad de la soberanía de los Estados en la esfera digital. Corresponde a cada país determinar los parámetros para regular su propio espacio de información y la infraestructura correspondiente.

Un desafío igualmente importante es crear un sistema de seguridad de la información internacional equitativo y justo en el que importen los intereses de todos los Estados, con independencia del nivel de desarrollo de sus capacidades digitales. Las iniciativas de desarrollo de la capacidad lideradas por las Naciones Unidas encaminadas a superar la brecha digital son vitales y deberían contar con un firme apoyo. Confiamos en que el nuevo grupo de trabajo de composición abierta, de acuerdo con su mandato, pueda seguir examinando de cerca esta cuestión y presentar las recomendaciones pertinentes.

Además, es esencial que luchemos juntos contra el uso de las TIC con fines delictivos. Hacemos un llamamiento a los Estados Miembros para que contribuyan de forma constructiva a los trabajos del Comité Ad Hoc, cuya tarea es elaborar un proyecto de convención para 2023.

La Asamblea General de las Naciones Unidas sigue siendo un foro clave para debatir cuestiones de seguridad de la información a nivel internacional. Precisamente en el marco de dicho organismo se mantendrán durante cinco años debates entre expertos sobre todos los aspectos de este tema. Centrémonos en apoyar este proceso único. La atmósfera constructiva del compromiso multilateral sobre la seguridad de la información internacional bajo los auspicios de las Naciones Unidas debería preservarse en el formato de grupo de trabajo de composición abierta, que ha demostrado ser eficaz y pertinente en la práctica. Así, el nuevo grupo de trabajo de

composición abierta tendrá una oportunidad real de lograr resultados tangibles y prácticos. Es nuestra responsabilidad común como miembros del Consejo de Seguridad de las Naciones Unidas facilitar esto lo mejor que podamos.

Anexo XVI

Declaración del Representante Permanente de Túnez ante las Naciones Unidas, Tarek Ladeb

Para comenzar, deseo expresar nuestro agradecimiento a la presidencia estonia por haber organizado esta reunión sobre la ciberseguridad y el mantenimiento de la paz y la seguridad internacionales en el ciberespacio.

Agradezco a la Sra. Nakamitsu, Secretaria General Adjunta y Alta Representante para Asuntos de Desarme, por su exposición informativa.

Túnez está profundamente preocupado por el aumento significativo en los últimos años de las actividades maliciosas en el ciberespacio que pueden plantear una grave amenaza para la paz y la seguridad internacionales, en especial cuando el objetivo es la infraestructura crítica.

Muchos Estados también han estado desarrollando abiertamente cibercapacidades con fines militares, una tendencia que puede desencadenar una carrera de ciberarmas y aumentar aún más el número de ciberataques y contraataques, así como los riesgos de errores de cálculo que podrían conducir a un conflicto armado.

Túnez está igualmente preocupado por el hecho de que las cibercapacidades, que antes solamente estaban a disposición de los Estados, han pasado a ser accesibles y están siendo utilizadas maliciosamente por actores no estatales, incluidas las organizaciones terroristas. Al parecer, estas capacidades se han adquirido a menudo a través de filtraciones o robos a entidades gubernamentales, lo que plantea aún más la cuestión de la responsabilidad de los Estados.

La posibilidad de que grupos terroristas lancen ciberataques devastadores contra la infraestructura crítica como las centrales nucleares ya no puede excluirse y debe abordarse seriamente.

Túnez reafirma la aplicabilidad del derecho internacional a la hora de abordar el uso de las tecnologías de la información y las comunicaciones por parte de los Estados, y subraya a este respecto la importancia de respetar el principio consagrado en la Carta de las Naciones Unidas, que incluye la solución de controversias internacionales por medios pacíficos, la abstención de la amenaza o el uso de la fuerza y el respeto de los derechos humanos y las libertades fundamentales.

También quisiéramos subrayar nuevamente la aplicabilidad del derecho internacional humanitario a las ciberoperaciones realizadas durante los conflictos armados.

Mi delegación se congratula de la adopción consensuada, a principios de este año, de los informes del Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, que contribuyeron a profundizar en la comprensión de los Estados Miembros sobre el modo en que se aplica el derecho internacional y ofrecieron más orientaciones sobre el modo en que las normas voluntarias y no vinculantes pueden desempeñar también un papel importante en la prevención de

conflictos y la promoción de un ciberespacio abierto, seguro, estable, accesible y pacífico.

Esperamos con interés que continúe el diálogo abierto e inclusivo sobre la ciberseguridad durante las sesiones del nuevo grupo de trabajo de composición abierta (sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones para el período 2021-2025) para reforzar la capacidad de todos los Estados y prevenir o mitigar los impactos de las ciberactividades maliciosas, las ciberamenazas y los ciberataques.

Por su parte, y bajo la supervisión de su Consejo de Seguridad Nacional y con la participación del sector privado y la sociedad civil, Túnez ha adoptado en octubre de 2019 una estrategia nacional de ciberseguridad que tiene como objetivo mejorar la resiliencia de Túnez frente a las ciberamenazas, mediante el desarrollo de sus capacidades nacionales y su sistema jurídico, respetando plenamente los derechos y libertades fundamentales, y mediante el refuerzo de la cooperación internacional.

Por último, dada la naturaleza interconectada del ciberespacio, creemos que el intercambio de información sobre las vulnerabilidades conocidas y la creación de capacidades para quienes lo soliciten son de crucial importancia para reducir los riesgos que las ciberamenazas plantean para la paz y la seguridad internacionales.

Anexo XVII

Declaración de la Misión Permanente de la Argentina ante las Naciones Unidas

[Original: español]

La Argentina agradece a Estonia por esta iniciativa de realizar un debate abierto para contribuir a una mejor comprensión de los crecientes riesgos derivados de actividades maliciosas en el ciberespacio y su impacto en la paz y seguridad internacionales. El Consejo de Seguridad, por su mandato y naturaleza, permite brindar al tema la relevancia y trascendencia que tiene.

El registro regular y creciente de graves incidentes cibernéticos en distintas partes del mundo, es un permanente llamado de atención para todos sobre la necesidad de continuar construyendo mayores entendimientos sobre la gestión de los incidentes, algunos de los cuales son susceptibles de poner en riesgo la paz y seguridad internacionales, generar marcos de cooperación y fomentar la construcción de capacidades de los países para enfrentar estos desafíos que afectan a toda la comunidad internacional. Para ello se requiere de múltiples acciones en distintos niveles, tanto a nivel nacional, como regional e internacional.

En el ámbito internacional y con el objetivo de atender uno de los aspectos más críticos de la cuestión, la Argentina considera de suma importancia la necesidad de mantener espacios amplios e inclusivos en los que países de todas las regiones y diversidad de visiones puedan involucrarse activamente con el objetivo de construir consensos sobre las reglas, normas y principios del comportamiento responsable de los Estados y la forma en que se aplica el derecho internacional en el ciberespacio, entre otros aspectos. La Argentina entiende que existe un importante acervo de normas, reglas y principios voluntarios que han sido aceptados por consenso por todos los miembros de la Asamblea General de las Naciones Unidas para guiar el uso estatal de las tecnologías de la información y las comunicaciones (TIC) y el comportamiento responsable de los Estados en el ciberespacio, que son imprescindibles para mantener el uso pacífico y la estabilidad en el ciberespacio. Este es un punto de partida y una base que debe preservarse y desarrollarse.

En este marco, otorgamos un valor especial a los consensos obtenidos en el marco del primer 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 tiene como base esas características abiertas. También otorgamos un reconocimiento especial al informe del último Grupo de Expertos Gubernamentales sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. Es de destacar que ambos grupos emitieron informes consensuados este año, con importantes recomendaciones y aportes para continuar construyendo sobre los consensos ya obtenidos en el pasado.

La continuidad de un ámbito de discusión abierta, inclusiva y con horizontes más extensos es de fundamental importancia, para seguir consolidando los acuerdos alcanzados y obtener nuevos avances. Es por ello que nos congratulamos con la creación de un nuevo 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, cuyo mandato se extiende hasta el 2025 y en el cual nuestro país continuará participando activamente y con espíritu constructivo.

En este mismo aspecto y con un enfoque más efectivo, la Argentina, junto con un importante número de países de todas las regiones, apoya la iniciativa internacional denominada programa de acción sobre los avances de las TIC en el contexto de la seguridad internacional. Este programa de acción, que se encuentra en pleno desarrollo conceptual, propone un esquema abierto, inclusivo, flexible y permanente de discusión bajo el auspicio de las Naciones Unidas, conducido por los Estados y con una adecuada participación de los múltiples actores que participan del ciberespacio. Invitamos a todos los países a interesarse por esta iniciativa.

La Argentina considera que como base y principio de nuestros entendimientos debe estar la protección y resguardo de los derechos humanos y libertades fundamentales consagrados en la Carta de las Naciones Unidas y en tratados internacionales. La cuestión de género y el resguardo especial de los grupos vulnerables también debe ser transversal a todas las acciones que desarrollemos.

En un contexto de continuas innovaciones en el ámbito de las TIC es necesario trabajar activamente para que los beneficios de estas tecnologías puedan ser disfrutadas por todas las naciones con equidad y equilibrio. Por ello consideramos que la reducción de la brecha digital entre los Estados, y dentro de los mismos, debe ser una preocupación permanente en el marco de este debate.

Dicha preocupación va de la mano del desarrollo de capacidades nacionales. Hay un campo enorme para trabajar sobre este aspecto y uno de los principales para desarrollar las sinergias con los otros actores que participan del ciberespacio, como el sector privado, la sociedad civil, la academia y el sector técnico.

Los organismos regionales y subregionales han probado ser un actor importante y decisivo como catalizadores del desarrollo de las capacidades nacionales, el fomento de entendimientos comunes y la facilitación de la cooperación internacional.

Sin duda los Estados deben hacer esfuerzos nacionales importantes, desarrollar capacidades, estructuras, y normas eficaces otorgando la importancia y prioridad que el tema amerita.

Confiamos que este evento nos permita identificar nuevas vías de entendimiento que contribuya a contar un ciberespacio, libre, abierto, seguro, interoperable y estable.

Anexo XVIII

Declaración del Representante Permanente de Australia ante las Naciones Unidas, Mitchell Fifield

Australia agradece a Estonia la oportunidad de hacer una declaración ante el Consejo de Seguridad sobre la paz y la seguridad internacionales en el ciberespacio. A medida que aumente la importancia estratégica del ciberespacio, más grupos tratarán de ejercer su poder a través de él. Los problemas cibernéticos se han convertido en cuestiones estratégicas de política exterior que preocupan de forma urgente a todos los países, y es vital que la comunidad internacional los trate como tales.

Aunque la frecuencia, la escala, la sofisticación y la gravedad de los ciberincidentes maliciosos van en aumento, las Naciones Unidas tienen un sólido historial de fomento de la cooperación internacional para comprender estas amenazas y promover un ciberespacio abierto, libre, seguro, interoperable y pacífico.

Todos los miembros de las Naciones Unidas hemos acordado, por consenso, que el derecho internacional vigente, en particular la Carta de las Naciones Unidas en su totalidad, es aplicable en el ciberespacio 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[3].

Australia ha articulado sus puntos de vista sobre cómo se aplican determinados principios del derecho internacional al comportamiento de los Estados en el ciberespacio (2017; 2019; 2021) y estudios de caso legales hipotéticos publicados (2020)[4].

El derecho internacional humanitario (incluidos los principios de humanidad, necesidad, proporcionalidad y distinción) se aplica a ciberactividades en un conflicto armado. El derecho internacional humanitario ofrece reglas que se aplican a ciberactividades en un conflicto armado que no constituyen o elevan el nivel de un “ataque”, incluidas las protecciones generales que se ofrecen a la población civil y a sus miembros de los peligros derivados de las operaciones militares.

El derecho internacional de los derechos humanos también se aplica al comportamiento de los Estados en el ciberespacio. Según el derecho internacional de los derechos humanos, los Estados tienen la obligación de proteger los derechos humanos relevantes de las personas que se encuentran bajo su jurisdicción, incluidos el derecho a la privacidad, cuando esos derechos se ejerzan o se materialicen en el ciberespacio.

Reconociendo los atributos únicos del ciberespacio, en 2015 todos los Estados Miembros acordaron guiarse en su uso de las TIC por 11 normas voluntarias y no vinculantes de comportamiento responsable de los Estados en el ciberespacio[5]. Estas normas complementan, pero no sustituyen, las obligaciones legales de los Estados. Combinados, el derecho y las normas internacionales establecen expectativas claras

[3] Véanse las resoluciones 68/243 y 70/237 de la Asamblea General y la decisión A/DEC/75/564.
[4] Véase www.internationalcybertech.gov.au/international-security-at-the-un.
[5] Véase la resolución 70/237 de la Asamblea General.

de comportamiento responsable por parte de los Estados y, por tanto, promueven la previsibilidad, la estabilidad y la seguridad.

Todos los Estados han reconocido también la necesidad de adoptar medidas de fomento de la confianza y de coordinar la creación de capacidad[6]. Las OGC, diseñadas para evitar malentendidos que conduzcan a conflictos, hoy son más importantes que nunca, y es necesario crear capacidades específicas para garantizar que todos los países puedan responder a los desafíos y aprovechar las oportunidades de una mayor conectividad.

Combinadas, estas medidas (derecho internacional, normas, medidas de fomento de la confianza y creación de capacidad) constituyen la base de un ciberespacio seguro, estable y próspero, y a menudo se hace referencia a ellas como un Marco de las Naciones Unidas para un Comportamiento Responsable de los Estados en el Ciberespacio. Cada elemento del Marco se refuerza mutuamente y ninguno de ellos debe considerarse de forma aislada.

La aprobación universal del Marco[7] por parte de todos los Estados Miembros representa un avance significativo en la promoción de la paz y la estabilidad internacionales en el ciberespacio. Si se cumple, el Marco proporciona una base sólida para hacer frente a las amenazas que plantea la ciberactividad maliciosa generada y patrocinada por el Estado.

Australia reafirma su compromiso de actuar de conformidad con el Marco para el Comportamiento Responsable de los Estados en el Ciberespacio, tal y como se elaboró en los informes acumulados de los Grupos de Expertos Gubernamentales en 2010, 2013, 2015 y 2021[8] y en el informe de 2021 del Grupo de Trabajo de Composición Abierta[9], y pide a todos los países que hagan lo mismo.

Sin embargo, un pequeño número de actores estatales y patrocinados por el Estado desprecian cada vez más el derecho y las normas internacionales, a pesar de las claras expectativas establecidas por la comunidad internacional. Al hacerlo, amenazan la paz y la estabilidad internacionales.

Lo que necesitamos no son más (o nuevas) normas, sino el cumplimiento de las que ya hemos acordado, y una mayor responsabilidad cuando se incumplen. Para disuadir la actividad maliciosa, debe haber consecuencias efectivas y proporcionadas para quienes actúen en contra del derecho internacional vigente y de las normas acordadas de comportamiento responsable de los Estados.

Australia se ha comprometido a contrarrestar, disuadir y desalentar la ciberactividad maliciosa, en especial por parte de los Estados y sus representantes. Australia trabajará con sus asociados para reforzar las respuestas coordinadas a los comportamientos inaceptables en el ciberespacio. La disuasión de las actividades maliciosas protege la estabilidad internacional. El objetivo de la política de ciberdisuasión de Australia es evitar incidentes cibernéticos significativos que perjudiquen los intereses de Australia y de nuestros asociados internacionales.

[6] *Ibid.*
[7] Decisión 75/564 de la Asamblea General; A/75/816.
[8] A/65/201; A/68/98; A/70/174.
[9] A/75/816.

La cooperación efectiva entre los Estados y la comunidad de múltiples interesados (incluidos la sociedad civil, el sector privado, el mundo académico y la comunidad técnica) tiene un impacto práctico en la seguridad, eleva la capacidad y crea un ciclo de desarrollo, apertura y estabilidad en el ciberespacio que se refuerza. Los primeros afectados por los ciberincidentes suelen ser protectores de la infraestructura crítica, benefactores y beneficiarios de los conocimientos técnicos, y la evolución de las partes interesadas no gubernamentales en el ciberespacio ofrece intereses complementarios para mantener un entorno en línea pacífico.

La desigualdad de género socava la paz, la estabilidad y la seguridad mundiales en el ciberespacio. Contribuye, y suele agravar, una serie de problemas, como la pobreza, la mala gobernanza, los conflictos y el extremismo violento. El valor de la igualdad de género y de la participación de las mujeres en la toma de decisiones, el liderazgo y la consolidación de la paz asociados a la paz y la seguridad internacionales en el ciberespacio es indiscutible. Australia seguirá adoptando medidas tangibles para apoyar la participación efectiva de las mujeres en todos los foros que analizan la paz y la seguridad internacionales en el ciberespacio.

El daño potencial o la disrupción causada por las actividades cibernéticas maliciosas es significativo y creciente. La creciente atención y concienciación de la comunidad internacional sobre estas cuestiones no debe desaprovecharse. Debe aprovecharse esta oportunidad para profundizar en la comprensión de cómo se aplica el derecho internacional en el ciberespacio, promover la aplicación de las normas de comportamiento responsable de los Estados y las medidas de fomento de la confianza, coordinar la creación de capacidades para que todos los países comprendan y puedan aplicar el Marco, y garantizar que se escuchen diversas voces.

Anexo XIX

Declaración de la Misión Permanente de Austria ante las Naciones Unidas

Austria desea agradecer a Estonia, en su calidad de Presidencia del Consejo de Seguridad durante el mes de junio de 2021, la convocatoria de este debate abierto sobre la paz y la seguridad internacionales en el ciberespacio. Austria se adhiere a la Declaración de la Unión Europea. A título nacional, deseamos añadir las siguientes observaciones:

Hoy es la primera vez que el Consejo de Seguridad aborda la ciberseguridad como un tema independiente, lo cual es un avance positivo. Para seguir siendo relevante y cumplir su mandato, es esencial que el Consejo de Seguridad siga respondiendo a las amenazas contemporáneas a la paz y la seguridad internacionales.

Un número creciente de ciberactividades maliciosas ha aumentado las amenazas en el ciberespacio en los últimos años. En el mundo conectado de hoy, en el que las infraestructuras dependen cada vez más de los sistemas de control digital, los efectos de los ciberataques pueden tener efectos similares o a veces peores que los ataques convencionales. Estos hechos, unidos a los problemas de atribución de los ciberataques, aumentan la inseguridad, el riesgo de errores de cálculo y la posibilidad de que se produzca un error humano a la hora de decidir cómo responder a un ataque entrante.

Aunque el ciberespacio difiere del mundo físico en su funcionamiento, no puede haber ningún error sobre un simple hecho: el derecho internacional en su totalidad se aplica también en el ciberespacio. Esto ha sido reafirmado, más recientemente, por los resultados del Grupo de Trabajo de Composición Abierta sobre Tecnología de la Información y las Comunicaciones (TIC), así como por el Grupo de Expertos Gubernamentales en Ciberseguridad, que acordaron por consenso documentos de resultados sustanciales que amplían nuestra comprensión de los desafíos a los que nos enfrentamos en el ciberespacio. A medida que más y más Estados desarrollan cibercapacidades no solo defensivas, sino también ofensivas, es clave que todos los Estados, en su uso de las TIC, se adhieran al derecho internacional vigente, así como a las normas de comportamiento responsable en el ciberespacio. Esperamos que estos documentos recuerden a los Estados sus obligaciones y contribuyan, por tanto, a una mayor estabilidad en el ciberespacio.

Sobra decir que las disposiciones fundamentales de la Carta de las Naciones Unidas deben guiar a todos los Estados en su comportamiento en el ciberespacio. En particular, los Estados están obligados a respetar la prohibición del uso de la fuerza como pilar fundamental del régimen de seguridad internacional. Además, los anteriores Grupos de Expertos Gubernamentales han acordado normas para el comportamiento responsable de los Estados en el ciberespacio que han sido respaldadas por todos los Estados Miembros. Por tanto, está claro que no es la falta de reglas y normas, sino la falta de su aplicación, lo que contribuye a la inestabilidad y la inseguridad. Por lo tanto, pedimos a todos los Estados que cumplan plenamente el derecho internacional y que sigan las normas de comportamiento responsable de los Estados en su totalidad.

En caso de que un conflicto armado o alguno de sus elementos se libren en el ciberespacio, es imperativo que se respete y cumpla el derecho internacional humanitario: los principios de humanidad, necesidad, proporción y distinción se aplican plenamente en el ciberespacio.

En el contexto de la pandemia de COVID, observamos con preocupación el reciente aumento de los ciberataques a instalaciones médicas y sanitarias que violan flagrantemente las normas de que la infraestructura crítica, incluidas las médicas, debe estar siempre fuera de los límites de las ciberactividades maliciosas.

Para evitar escenarios de conflicto, la creación de confianza es clave: los Estados deben comprometerse de forma constructiva a compartir su comprensión del ciberespacio y las formas en que se comprometen militarmente para evitar errores de cálculo. A este respecto, no se puede subestimar el papel de las organizaciones regionales, muchas de las cuales han llevado a cabo actividades de fomento de la confianza. Acogemos con especial satisfacción el "compromiso de la Organización para la Seguridad y la Cooperación en Europa en este asunto, y confiamos en que, aprovechando su experiencia en una red de puntos de contacto para asuntos de ciberseguridad, podamos también poner en marcha una red mundial a nivel de las Naciones Unidas".

Aunque los Estados y las organizaciones internacionales y regionales han estado en la vanguardia del desarrollo del derecho internacional y de las normas de comportamiento responsable de los Estados, no pueden hacer frente por sí solos a los desafíos que tenemos ante nosotros. Los actores comerciales tienen un papel y una responsabilidad importantes en el ciberespacio, y la sociedad civil y el mundo académico nos ayudan a aportar diferentes perspectivas a nuestros debates. Por ello, los futuros debates sobre el ciberespacio deben guiarse por un enfoque holístico y de múltiples partes interesadas para garantizar que quienes tienen un papel en el mantenimiento de un ciberespacio libre, seguro, abierto y estable sean escuchados y contribuyan a los objetivos comunes que buscamos.

A pesar de todos los progresos realizados en el ámbito de la ciberseguridad, aún quedan muchos interrogantes abiertos: dependerá de la comunidad internacional encontrar respuestas comunes a estas cuestiones. La cooperación seguirá siendo clave y Austria estará dispuesta a contribuir de forma constructiva en los procesos pertinentes. En este sentido, esperamos que los futuros debates abiertos en el Consejo vuelvan a la práctica anterior de permitirles a los no miembros realizar declaraciones verbales para dar visibilidad a todos los Estados interesados.

Anexo XX

Declaración del Representante Permanente de Bahrein ante las Naciones Unidas, Jamal Fares Alrowaiei

[Original: árabe]

La transformación tecnológico-digital y la aparición de tecnologías modernas contribuyen a lograr el progreso, la prosperidad y el desarrollo de toda la humanidad. Esta importancia se manifiesta en el hecho de haberse adoptado, en diferentes sectores, el trabajo, el estudio y la prestación de servicios en línea, debido al brote de la pandemia de enfermedad por coronavirus (COVID-19). A pesar de sus muchos beneficios, el desarrollo tecnológico también está ligado a muchos peligros, sobre todo en caso de que no exista un sistema claro para proteger la seguridad de la información y del ciberespacio, como vemos en los diferentes ciberataques que pueden tener como objetivo las infraestructuras básicas de los países, lo cual amenaza sus sectores vitales, instituciones o individuos.

Las Naciones Unidas han concedido una gran importancia a esta cuestión, habiéndola abordado el Consejo de Seguridad de manera indirecta en varias sesiones relacionadas con el mantenimiento de la paz y la seguridad internacionales, así como en reuniones celebradas con arreglo a la fórmula Arria. La Asamblea General ha establecido una serie de mecanismos, entre ellos el Grupo de Trabajo de composición abierta sobre la seguridad de las TIC (2021-2025) en 2020, cuyo objetivo es estudiar las amenazas que representa el uso de las TIC en el contexto de la seguridad internacional y cómo abordar dichas amenazas, así como formular criterios de comportamiento en el ciberespacio para los estados, aplicar el derecho internacional en el uso de las TIC y medidas de fomento de la confianza y de las capacidades

Partiendo de su convicción en la importancia de proteger el ciberespacio de los ataques y las agresiones en interés de los países y los pueblos, Bahrein ha apoyado el establecimiento de dichos mecanismos y ha participado en la labor del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional que concluyó su labor en 2021 y espera con interés participar activamente en la labor del grupo de trabajo recién constituido.

En el marco de su gran interés por la ciberseguridad en el trasfondo de la transformación digital y el salto cualitativo que vive el sector de las TIC, Bahrein ha trabajado para construir un sistema de gobernanza claro e integral para proteger el ciberespacio mediante el Centro Nacional de Ciberseguridad del Ministerio del Interior y que se ocupa de la ciberseguridad en diferentes sectores del país, así como la Autoridad de Información y Gobernanza Electrónica encargada de la protección de la seguridad de la información en la red nacional de datos del Reino de Bahrein. Además, la Agencia Reguladora de las Comunicaciones se esfuerza en reforzar la cooperación entre el sector público y el privado para garantizar que estén preparados para hacer frente a amenazas de ciberseguridad.

Por otro lado, Bahrein ha velado por establecer la legislación y los marcos legales relacionados con la seguridad de la información y la protección de las personas y las instituciones, siendo las más destacadas la Ley núm. 30 del año 2018

de promulgación de la ley de protección de datos personales y la Ley núm. 16 del año 2016 de delitos informáticos.

A nivel regional, Bahrein participa activamente en la labor del Comité Permanente para la Ciberseguridad de los países del Consejo de Cooperación de los Estados Árabes del Golfo, donde propuso la creación de una plataforma electrónica para el intercambio de información y de datos en el campo de la ciberseguridad entre los estados miembros. Cada uno de los estados miembros designó un oficial de enlace para el intercambio de la información relacionada con la ciberseguridad, como las amenazas y las mejores prácticas.

También, el Reino de Bahrein ratificó la Convención Árabe para la Lucha contra los Delitos de la Tecnología de la Información en 2017.

Por último, el Reino de Bahrein reafirma su apoyo a la cooperación internacional en el campo de la ciberseguridad, lo cual satisfará las aspiraciones de los pueblos del mundo y logrará el progreso, la prosperidad y el crecimiento, con el fin de aplicar los Objetivos de Desarrollo Sostenible 2030.

Anexo XXI

Declaración del Representante Permanente de Bélgica ante las Naciones Unidas, Philippe Kridelka

Permítanme, en primer lugar, expresar mi agradecimiento a la presidencia estonia por acoger este primer debate abierto del Consejo de Seguridad sobre la paz y la seguridad en el ciberespacio. Este oportuno debate demuestra la urgencia de abordar este tema y la relevancia del Consejo de Seguridad para hacerlo. Los riesgos derivados de las actividades maliciosas en el ciberespacio son realmente crecientes y su impacto en la paz y la seguridad internacionales es más perjudicial que nunca. Por lo tanto, es fundamental reafirmar el compromiso de los Estados Miembros 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.

La consecución de este objetivo requiere tanto un entendimiento internacional compartido sobre la gobernanza del ciberespacio como acciones reales para llevar esta visión a la realidad.

El debate internacional sobre la gobernanza del ciberespacio se encuentra en una fase crucial. Bélgica apoya firmemente los debates en curso en el marco de las Naciones Unidas, entre los que se encuentran la Primera Comisión, los distintos GTCA y los GEE. Los siguientes elementos son clave:

En primer lugar, Bélgica defiende una visión compartida de un ciberespacio global, libre, abierto, estable, pacífico y seguro, en el que se respeten los derechos humanos y las libertades fundamentales y el estado de derecho. Este entendimiento compartido se basa en un enfoque inclusivo en el que se escucha a todas las partes interesadas, incluidos la sociedad civil, el sector privado y el mundo académico.

En segundo lugar, la comunidad internacional debe seguir esforzándose por conseguir un marco de ciberseguridad verdaderamente universal para un comportamiento responsable de los Estados. Esto debe basarse en la plena aplicación del derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos. El año pasado, Bélgica, como miembro no permanente del Consejo de Seguridad, participó en una reunión del Consejo de Seguridad celebrada con arreglo a la fórmula Arria, sobre ciberataques a la infraestructura crítica. Los ciberataques dirigidos a infraestructuras críticas ponen en peligro vidas humanas y deben ser condenados por la comunidad internacional. Los ciberataques contra las instalaciones médicas como hospitales son inaceptables.

En cuanto al marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, hay que subrayar que los Estados Miembros de las Naciones Unidas han autorizado (mediante la adopción de la resolución 70/237 de las Naciones Unidas) las conclusiones de los informes del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015, que constituyen una base sólida y consensuada para seguir trabajando. Las Naciones Unidas y sus Estados Miembros han realizado esfuerzos considerables tanto para construir un entendimiento internacional compartido sobre la gobernanza del ciberespacio como para desarrollar acciones reales para aplicar esta visión común sobre el terreno. En un sistema

multilateral eficiente y eficaz, es imperativo que cualquier debate posterior parta de esta base consensuada, para evitar volver a los laboriosos compromisos del pasado y paralizar los esfuerzos futuros.

En tercer lugar, creemos que debemos adaptar mejor la justicia penal internacional a los desafíos del siglo XXI. Por ello, Bélgica se ha unido a Liechtenstein en su iniciativa de crear un Consejo de Asesores sobre la Aplicación del Estatuto de Roma a la Ciberguerra, con el fin de explorar el papel que podría desempeñar la Corte Penal Internacional en este nuevo marco normativo. Aguardamos con interés recibir el informe final del Consejo de Asesores, cuya presentación está prevista para este año.

Los principios rectores deben ir seguidos de acciones para marcar la diferencia. A este respecto, Bélgica está convencida de que la propuesta de Egipto y Francia de establecer un programa de acción constituye la estructura adecuada para poner en práctica nuestra visión. Bélgica se enorgullece de apoyar esta iniciativa junto con más de 50 países, y esperamos que muchos otros Estados se unan a ella.

A nivel nacional, Bélgica ha adoptado recientemente, en mayo de 2021, una nueva Estrategia Nacional de Ciberseguridad 2.0 para el período 2021-2025 que establece el enfoque transversal de nuestro país en términos de aumentar nuestra ciberresiliencia y combatir las ciberamenazas. El objetivo principal de esta estrategia nacional es “impulsar a Bélgica al rango de los países menos vulnerables de Europa”.

La política belga de ciberseguridad también prevé un nuevo mecanismo de atribución concebido como herramienta de disuasión. Si queremos prevenir y disuadir eficazmente las ciberactividades maliciosas en un entorno en el que los ciberataques son cada vez más numerosos y complejos, la atribución formal de una ciberactividad maliciosa dirigida a una organización vital en Bélgica es un instrumento importante. El procedimiento de atribución nacional también puede activarse con el fin de apoyar a un país aliado víctima de ataques similares.

Además, la estrategia nacional prescribe un claro compromiso internacional. Y esto sucede porque Bélgica está hablando por los codos, convencida de que es necesaria una mayor cooperación internacional para promover la seguridad y la estabilidad en el ciberespacio.

El aumento de la cooperación internacional también significa más creación de capacidades y más apoyo a las medidas de fomento de la confianza, incluso a través de los esfuerzos de organizaciones regionales como la Organización para la Seguridad y la Cooperación en Europa (OSCE). Bélgica participa activamente en los trabajos de la OSCE para concretar y hacer operativas estas medidas de creación de confianza. En cuanto a la creación de capacidades, las necesidades son importantes y urgentes a nivel mundial. Es necesario reforzar y ampliar los programas de cooperación o de creación de capacidades existentes, como los ofrecidos por la Unión Europea o por el Foro Mundial de Competencia Cibernética. A todos nos interesa mejorar la resiliencia global a las ciberamenazas.

Anexo XXII

Declaración de la Misión Permanente del Brasil ante las Naciones Unidas

Para empezar, quisiera felicitar a Estonia por la gran iniciativa de promover, por primera vez, un debate abierto oficial del Consejo de Seguridad sobre la ciberseguridad en el contexto más amplio del mantenimiento de la paz y la seguridad internacionales. La rápida evolución de las tecnologías de la información y las comunicaciones (TIC), que han llegado a impregnar todos los ámbitos de la existencia humana, nos obliga a actualizar el concepto de amenazas, a adaptar el marco normativo existente a esta nueva realidad y a desarrollar nuevas pautas de comportamiento responsable de los Estados para superar los desafíos modernos y frenar la aparición de conflictos.

Aunque el tema de la ciberseguridad se acaba de plantear en el organismo que tiene la responsabilidad primordial del mantenimiento de la paz y la seguridad internacionales, los Estados Miembros llevan debatiendo sobre esto más de dos décadas, al menos desde 1998, cuando el tema se introdujo por primera vez en el programa de la Asamblea General. Durante este período, hemos sido testigos de la adopción de cuatro informes consensuados de Grupos de Expertos Gubernamentales (dos de ellos presididos por expertos brasileños) y un informe igualmente consensuado de un Grupo de Trabajo de Composición Abierta. En conjunto, estos documentos forman un acervo, un corpus común de entendimientos y normas, reglas y principios voluntarios y no vinculantes que ayudan a guiar el uso de las TIC por parte de los Estados.

Una de las mayores contribuciones de este acervo al mantenimiento de la paz y la seguridad internacionales es la afirmación de que el derecho internacional, incluido el derecho internacional humanitario (DIH), es aplicable al ciberespacio. En nuestra contribución nacional voluntaria al compendio oficial del último Grupo de Expertos Gubernamentales, reafirmamos la firme convicción del Brasil de que, en su uso de las tecnologías de la información y las comunicaciones, los Estados deben respetar el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional de los derechos humanos y el derecho internacional humanitario. Las Naciones Unidas y otras organizaciones regionales han reconocido que la ley internacional, y en particular la Carta de las Naciones Unidas, es aplicable en el ciberespacio y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de la tecnología de la información y las comunicaciones. Por lo tanto, en los debates actuales, el asunto ya no es si se aplica, sino cómo se aplica el derecho internacional al uso de las TIC por parte de los Estados.

Si bien las analogías en relación con el mundo físico podrían funcionar la mayor parte del tiempo para determinar dicha aplicación, las características únicas del ciberespacio crean nuevas situaciones que, conforme a su diseño original, el derecho internacional no regula. La interconectividad de los sistemas de la información, el carácter intangible de la esfera de las TIC y las complejidades del problema de atribución de responsabilidad ante actos maliciosos y ofensivos en el ciberespacio, entre otros factores, plantean nuevos desafíos al derecho internacional, cuyo desarrollo se ha basado en un orden internacional físico y territorial.

Las diferencias en interpretaciones de los Estados de la forma en que el derecho internacional se aplica al uso de las TIC aumentan el riesgo de que aparezcan comportamientos, malentendidos y el recrudecimiento de tensiones impredecibles. Por lo tanto, es importante identificar de forma progresiva áreas de convergencia entre los Estados en este respecto y, cuando se identifiquen divergencias, trabajar en forma conjunta hacia el aumento de la coherencia en la interpretación de las reglas vigentes. Si es necesario, también debe considerarse el desarrollo de normas adicionales como un medio para llenar las potenciales brechas legales y resolver las incertidumbres restantes.

El mantenimiento de la paz y la seguridad internacionales depende en gran medida del nivel de confianza que exista entre los Estados. Por lo tanto, además del reconocimiento de la aplicabilidad del derecho internacional y del establecimiento y la aplicación de normas, reglas y principios de comportamiento responsable de los Estados, es de suma importancia que los gobiernos apliquen medidas de fomento de la confianza. El establecimiento de una red de puntos de contacto a nivel técnico y político, así como el intercambio de puntos de vista nacionales sobre las amenazas y sobre la gestión de incidentes relacionados con las TIC, son importantes medidas de cooperación y transparencia. Estas iniciativas no solo ayudan a prevenir malentendidos y percepciones erróneas, sino que también son útiles para abordar incidentes graves relacionados con las TIC y para rebajar las tensiones en un escenario de crisis.

La creación de capacidades es también una herramienta esencial para la promoción de un entorno pacífico de las TIC. Al igual que en otros ámbitos, la desigualdad entre las naciones puede generar inseguridad también en el ciberespacio, con impacto directo en el mundo cinético. La cooperación internacional para el desarrollo de instituciones nacionales, recursos humanos y políticas públicas contribuye a reducir las vulnerabilidades de los Estados y son fundamentales para la universalización de la aplicación del derecho internacional y de las normas, reglas y principios de comportamiento responsable de los Estados en el ciberespacio. Si hay algo que la pandemia nos ha enseñado es que nadie está a salvo hasta que todo el mundo esté a salvo; el mismo razonamiento puede aplicarse al ciberespacio, altamente interconectado e interdependiente.

Dada la naturaleza multipartita del ciberespacio, el Brasil considera que ningún debate eficaz sobre ciberseguridad puede tener éxito sin la contribución de la sociedad civil, el mundo académico y el sector privado. Un enfoque de múltiples partes interesadas es esencial para identificar y combatir las amenazas, prevenir conflictos, promover entendimientos comunes, aumentar la ciberresiliencia y fomentar la cooperación. Una mayor interacción entre los agentes públicos y privados de diferentes países, intercambiando experiencias y compartiendo las mejores prácticas, es esencial para lograr un entorno de TIC más abierto, seguro, pacífico y accesible.

El Brasil ha participado activamente en los debates sobre ciberseguridad en el seno de las Naciones Unidas. Siempre hemos buscado ser proactivos tanto en los Grupos de Expertos Gubernamentales como en el último Grupo de Trabajo de Composición Abierta. El Brasil mantendrá su enfoque constructivo en los debates del nuevo Grupo de Trabajo de Composición Abierta, que celebrará su primer período de sesiones sustantivo en diciembre, así como en otros mecanismos de diálogo institucional regular que puedan establecerse, como el programa de acción sobre

ciberseguridad. Al mismo tiempo, como miembro no permanente del Consejo de Seguridad recientemente elegido, tenemos la intención de contribuir al desarrollo de los debates sobre el impacto del uso de las TIC en el contexto de la seguridad internacional también en este órgano. En opinión del Brasil, el Consejo debe guiarse ante todo por el objetivo de promover la adhesión a las recomendaciones pasadas y futuras adoptadas por la Asamblea General sobre la cuestión de la ciberseguridad.

¡Muchas gracias!

Anexo XXIII

Declaración de la Misión Permanente del Canadá ante las Naciones Unidas

[Original: francés]

Queremos expresar nuestro agradecimiento a Estonia por haber organizado esta sesión del Consejo de Seguridad sobre un tema tan oportuno y pertinente. Al Canadá le complace tener la oportunidad de contribuir a este debate.

El mundo depende cada vez más de las tecnologías digitales e Internet. El ciberespacio plantea numerosas amenazas para la paz y la seguridad internacionales. La injerencia en la vida democrática es un ámbito especialmente preocupante. Otro es el aumento reciente de los ataques con programas secuestradores. Por lo tanto, debemos seguir adoptando medidas para que el ciberespacio siga siendo libre, abierto y seguro.

El marco acordado para fomentar el comportamiento responsable de los Estados en el ciberespacio es la base sobre la que se asientan la paz y la estabilidad en este espacio. Este marco tiene por objeto reconocer la aplicabilidad del derecho internacional al ciberespacio, adherirse a las normas acordadas a nivel internacional, crear capacidades y aplicar medidas de fortalecimiento de la confianza. En conjunto, estos elementos reducen los riesgos de escalada y conflicto.

Este marco ha sido reafirmado en los informes consensuados adoptados recientemente por el Grupo de Trabajo de Composición Abierta y el Grupo de Expertos Gubernamentales de las Naciones Unidas. Todos los Estados Miembros de las Naciones Unidas ya se han comprometido a guiarse por este marco.

El derecho internacional es esencial para aplicar al ciberespacio el orden internacional basado en normas. Los informes publicados recientemente por el Grupo de Trabajo y el Grupo de Expertos Gubernamentales reafirman la aplicabilidad del derecho internacional al ciberespacio y suponen importantes avances en este sentido. El informe del Grupo de Trabajo recomienda intensificar la cooperación en materia de creación de capacidades en derecho internacional, con el fin de que un mayor número de Estados puedan formular su propio concepto y construir un punto de vista común. En el informe del Grupo de Expertos Gubernamentales se ha reafirmado la aplicabilidad del derecho internacional y se ha mencionado expresamente el derecho internacional humanitario.

El informe elaborado por el Grupo de Expertos Gubernamentales en mayo de 2021 orienta la aplicación de las 11 normas no vinculantes sobre el comportamiento responsable de los Estados. Estas normas fueron adoptadas por el Grupo de Expertos Gubernamentales de las Naciones Unidas en 2015 y aprobadas por todos los Estados Miembros en la resolución 70/237 de la Asamblea General. El Canadá considera que estas normas y el derecho internacional son suficientes para guiar el comportamiento de los Estados en el ciberespacio. Sin embargo, queda trabajo por hacer en su difusión y aplicación.

Tomemos como ejemplo los recientes ataques con programas secuestradores, muy mediatizados, perpetrados por grupos delictivos. Perturbaron a gran escala

sectores esenciales como la energía y la disponibilidad de alimentos. También afectaron a los mercados financieros.

Aunque los responsables de estos actos sean grupos delictivos, estos ejemplos ponen de relieve la importancia del derecho internacional y de las 11 normas del Grupo de Expertos Gubernamentales. Varias de estas normas abordan de manera directa o indirecta amenazas que entrañan las TIC para las infraestructuras críticas. Una de las normas establece que los Estados deben responder a las solicitudes de asistencia de todo Estado cuya infraestructura crítica sea objeto de actos malintencionados relacionados con las TIC. Otra norma establece que los Estados no deben permitir deliberadamente que su territorio sea utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC.

Los grupos que se dedican a cometer actos delictivos, incluidos ataques con programas secuestradores, viven y trabajan en Estados. Utilizan la infraestructura digital de estos Estados para cometer estos actos, mientras que están sujetos a sus leyes. Los Estados que tengan conocimiento de que un acto malintencionado emana de su territorio tienen la responsabilidad de actuar, hacer cumplir sus leyes y cooperar con los demás Estados. Al aceptar guiarnos por las normas del Grupo de Expertos Gubernamentales, todos nos hemos comprometido a actuar así. Esta es también la razón por la que un creciente número de Estados han adoptado leyes estrictas en la lucha contra la ciberdelincuencia. En muchos casos, estos Estados han basado estas leyes en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, que ya cuenta con partes de todas las regiones del mundo.

Por desgracia, como hemos constatado recientemente, no todos los Estados respetan siempre el marco sobre el comportamiento responsable de los Estados. Determinados países permiten a los ciberdelincuentes operar desde su territorio con total impunidad. Otros recurren a intermediarios o llevan a cabo deliberadamente ciberactividades maliciosas que son contrarias al marco. En varias ocasiones, el Canadá se ha sumado a sus asociados internacionales para denunciar estos comportamientos y reaccionar a la amenaza que representan para la paz y la seguridad internacionales.

El Canadá es uno de los 27 signatarios de la declaración conjunta sobre la promoción del comportamiento responsable de los Estados en el ciberespacio de septiembre de 2019. Además de reafirmar el marco acordado para favorecer un comportamiento responsable de los Estados en el ciberespacio, nos hemos comprometido a trabajar juntos y de manera voluntaria para exigir responsabilidades a los Estados cuando actúan de forma contraria a este marco, en particular adoptando medidas transparentes y conformes al derecho internacional.

Es lo que hemos hecho hasta la fecha y es lo que seguiremos haciendo. Es importante sacar a la luz los comportamientos contrarios a las normas, con el fin de hacer cumplir el marco acordado para favorecer un comportamiento responsable de los Estados en el ciberespacio. Alentamos a todo el mundo a que haga lo propio.

Por lo que respecta al futuro en la Organización de las Naciones Unidas, el Canadá espera con interés participar de manera constructiva en el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Contribuiremos asimismo a la elaboración

de un programa de acción de las Naciones Unidas sobre la ciberseguridad. El Canadá es copatrocinador de este programa de acción, puesto que consideramos que puede servir de foro útil basado en la acción que impulsará la aplicación del marco para el comportamiento responsable de los Estados.

El éxito de estos dos procesos dependerá de su capacidad para integrar diversas voces y perspectivas en sus métodos de trabajo y resultados. En el grupo de trabajo de composición abierta, el Canadá aboga por una participación significativa de las partes interesadas no gubernamentales. En efecto, la sociedad civil, el mundo académico, el mundo técnico y el sector privado tienen mucho que aportar a estos debates, puesto que desempeñan un papel importante en la aplicación de las recomendaciones del Grupo de Expertos Gubernamentales y el grupo de trabajo. Asimismo, abogaremos por un compromiso firme de las partes interesadas en el programa de acción a medida que se elabora.

También será importante velar por que se escuchen realmente las voces de las mujeres, ya sea en el seno del Grupo de Trabajo de Composición Abierta o en la elaboración del programa de acción. El género debe integrarse en los dos procesos desde el inicio, a fin de que el trabajo de los dos grupos aborde los aspectos de la ciberseguridad relacionados con el género. Está bien documentado que la mediación o la participación femenina es importante para alcanzar una paz mucho más sólida, caracterizada por un menor riesgo de reanudación de las hostilidades. Los ciberprocesos de las Naciones Unidas pueden reforzarse de la misma forma, haciendo partícipes a las mujeres de manera importante. La inclusión es importante para el éxito de los dos procesos.

En resumen, el Canadá sigue siendo un firme partidario del marco acordado para favorecer un comportamiento responsable de los Estados en el ciberespacio. Seguiremos promoviendo la aplicación de las recomendaciones de los Grupos de Expertos Gubernamentales precedentes y del reciente Grupo de Trabajo de Composición Abierta. Asimismo, seguiremos denunciando las ciberactividades maliciosas que son contrarias a este marco y respondiendo a ellas. Esperamos con interés seguir trabajando con la comunidad internacional en la promoción de la paz y la seguridad internacionales mediante el refuerzo de la estabilidad y la seguridad en el ciberespacio.

Anexo XXIV

Declaración de la Misión Permanente de Chile ante las Naciones Unidas

Chile reafirma su posición 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 (TIC). Esto, junto con principios específicos de la Carta de las Naciones Unidas, en particular el arreglo pacífico de controversias, la prohibición de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, la no intervención en los asuntos internos de otros Estados y el respeto de los derechos humanos y las libertades fundamentales, son indivisibles tanto en el ámbito físico como en el digital, por lo que Chile seguirá promoviendo su aplicación.

Las actividades malintencionadas relacionadas con las TIC por parte de actores que generan amenazas persistentes, incluidos los Estados y otros agentes, pueden suponer un riesgo significativo para la seguridad y la estabilidad internacionales y el desarrollo económico y social, así como para la seguridad y el bienestar de las personas. La actividad maliciosa contra la infraestructura crítica que proporciona servicios de forma nacional, regional o mundial, se vuelve cada vez más grave, incluso las actividades malintencionadas relativas a las TIC que afectan a las infraestructuras de información críticas, las infraestructuras que prestan servicios esenciales al público, las infraestructuras técnicas esenciales que garantizan la disponibilidad general o la integridad de Internet y las entidades del sector de la salud. En futuros conflictos, estas actividades maliciosas pueden ser más destructivas y afectar gravemente al bienestar y la vida de las personas. En este sentido, los países podrían verse gravemente afectados por los ciberataques generados en el contexto de los conflictos armados.

Durante los conflictos armados, los Estados deben planificar, dirigir y ejecutar sus operaciones en el ciberespacio respetando estrictamente las normas del derecho internacional, con especial consideración al derecho internacional de los derechos humanos y al derecho internacional humanitario.

Chile apoya firmemente el trabajo del Grupo de Expertos Gubernamentales, así como sus informes y recomendaciones adoptadas en 2010, 2013, 2015 y 2021, ya que representaron un enorme avance respecto al derecho internacional, las normas y las medidas de fomento de la confianza en la esfera de las TIC. Chile también apoya la labor del Grupo de Trabajo de Composición Abierta y sus recomendaciones. Para reducir el uso malicioso de las cibercapacidades y construir un ciberespacio más estable, es importante seguir y aplicar estas recomendaciones, en todos los niveles.

El programa de acción para avanzar en el comportamiento responsable de los Estados en el ciberespacio es una iniciativa positiva, constructiva y realista que podría ayudarnos a avanzar y lograr resultados concretos en el marco del entorno de las TIC. El programa de acción podría ser un instrumento internacional permanente, inclusivo, basado en el consenso y orientado a la acción para promover un comportamiento responsable en el uso de las TIC en el contexto de la seguridad internacional. Como copatrocinador de esta iniciativa, Chile cree que el programa de acción debería

ofrecer una plataforma para adoptar recomendaciones operativas, promover la cooperación internacional y fomentar programas de asistencia adaptados a las necesidades de los Estados beneficiarios, especialmente en materia de creación de capacidades.

En lo que respecta al cumplimiento del derecho internacional vigente y a la aplicación de las normas de comportamiento responsable de los Estados en el ciberespacio, es importante que los Estados puedan desarrollar y compartir sus puntos de vista con otros Estados sobre cómo se aplica el derecho internacional en el ciberespacio. La creación de capacidades en este ámbito también es crucial. La existencia de directrices para la aplicación de las normas es un paso importante que debería ayudar a los Estados a avanzar en este asunto. Las organizaciones regionales pueden desempeñar un papel fundamental a la hora de ayudar a los Estados en la aplicación de las normas y el cumplimiento del derecho internacional, desarrollando estrategias regionales al respecto, así como la formación y la creación de capacidades.

Chile cree que es fundamental reforzar las medidas de confianza en el ciberespacio y la creación de capacidades para lo cual las organizaciones regionales deben tener un papel primordial. En este sentido, destacamos la labor que está llevando a cabo la Organización de los Estados Americanos a través de su Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, así como los trabajos y avances realizados por la Organización para la Seguridad y la Cooperación en Europa y la Asociación de Naciones de Asia Sudoriental.

Es importante promover el diálogo entre las regiones en este asunto, pero también en la creación de capacidades y en la aplicación de las normas. Este diálogo debe considerar el intercambio de experiencias, información, directrices, mejores prácticas, lecciones aprendidas, e invitar a los miembros de las organizaciones a participar en estos procesos regionales. Los Estados deben reforzar sus puntos de contacto nacionales, así como el papel de sus Ministerios de Relaciones Exteriores en relación con las políticas de ciberespacio y las TIC. La ciberdiplomacia es una herramienta importante que puede ayudar a los Estados a mejorar la cooperación entre ellos, creando confianza. Los Estados también deberían considerar la posibilidad de establecer mecanismos bilaterales de diálogo y cooperación en materia de ciberseguridad y ciberespacio.

Chile cree que los procesos multilaterales deben ser lo más inclusivos y transparentes posibles. El debate sobre las TIC debe incluir al sector privado, el mundo académico, la sociedad civil, la industria y la comunidad técnica, entre otros. No es posible crear un entorno estable y seguro en el ciberespacio si no garantizamos la participación y el trabajo de todas las partes interesadas. Cuantos más actores formen parte del debate, más probabilidades habrá de lograr resultados beneficiosos para todos. En este sentido, creemos que es necesario que podamos escuchar a todas las partes interesadas y que estas también puedan presentar sus opiniones y aportaciones en las sesiones oficiales. En ese sentido, los Estados deben incluir a todas las partes interesadas a la hora de generar políticas, estrategias y otras iniciativas que tengan como objetivo prevenir conflictos, construir entendimientos comunes y aumentar la ciberresiliencia.

Anexo XXV

Declaración de la Misión Permanente de la República Checa ante las Naciones Unidas

La República Checa desea expresar su agradecimiento a la República de Estonia por haber organizado el histórico primer debate abierto del Consejo de Seguridad sobre el tema de la ciberseguridad en el contexto de la paz y la seguridad internacionales. La adhesión de los Estados al derecho internacional y el comportamiento responsable de los Estados en el ciberespacio son elementos clave para la prevención de conflictos y el mantenimiento de la paz y la seguridad internacionales.

La República Checa se adhiere a la declaración presentada por la Unión Europea y desea destacar a continuación dos puntos adicionales.

Las ciberamenazas a la paz y la seguridad internacionales actuales y de nueva aparición

El ciberespacio ofrece enormes beneficios para el desarrollo humano y económico, pero también se está convirtiendo en un ámbito de crecientes dependencias y problemas de seguridad. Nuestra mayor dependencia de las TIC durante la pandemia de enfermedad por coronavirus (COVID-19), que está siendo continuamente explotada por actores maliciosos en su propio beneficio, es un claro recordatorio de los crecientes desafíos del ciberespacio. En particular, hemos visto un aumento alarmante de las actividades maliciosas relacionadas con las tecnologías de la información y las comunicaciones (TIC) dirigidas contra la infraestructura crítica que presta servicios esenciales al público, incluidas las dirigidas a instalaciones médicas, agua, energía, saneamiento, infraestructuras electorales y la disponibilidad general de Internet. En particular, el creciente número de ciberataques que interrumpen la prestación de asistencia sanitaria provoca más pérdidas de vidas, socava nuestra capacidad colectiva de responder a la COVID-19 y, en última instancia, amenaza la paz y la estabilidad internacionales.

Dichas actividades imprudentes de las TIC destinadas a dañar intencionadamente la infraestructura crítica también corren el riesgo de tener consecuencias humanitarias potencialmente devastadoras y, si son atribuibles a un Estado, violarían las obligaciones de dicho Estado en virtud del derecho internacional. Por ello, la República Checa se congratula de que todos los Estados Miembros hayan afirmado recientemente, a través de los informes finales del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, que las actividades de las TIC dirigidas contra la infraestructura crítica son inaceptables. Si bien el compromiso político es el primer paso necesario, la protección de la infraestructura crítica frente a las amenazas de las TIC requerirá también un esfuerzo práctico sostenido por parte de la comunidad internacional, incluso mediante la intensificación de la cooperación técnica y programas concretos de creación de capacidades relacionadas con la cibernética. El Consejo de Seguridad también puede desempeñar un papel decisivo asegurando que las actividades de las TIC patrocinadas por el Estado y dirigidas contra la infraestructura crítica tengan consecuencias.

Las nuevas y emergentes ciberamenazas no solo afectan a la seguridad nacional de los Estados, sino que también amenazan cada vez más el bienestar y la seguridad de las personas. La República Checa está especialmente preocupada por la creciente división política entre los Estados que abogan por la protección de las libertades personales en el ciberespacio y los que piden una mayor vigilancia tecnológica. En nuestra opinión, la expansión de las técnicas de vigilancia masiva patrocinadas por el Estado a través de las TIC, los cierres parciales o totales de Internet y la amplia censura de contenidos plantean graves problemas de derechos humanos. Es esencial adoptar una acción decidida para proteger a los ciudadanos del ejercicio arbitrario e ilegal del poder del Estado en el ciberespacio. Estas tendencias, unidas a los riesgos potenciales asociados a la introducción de la inteligencia artificial en diversas facetas de nuestras vidas, plantean nuevos desafíos de seguridad, amenazan con socavar la confianza en el ciberespacio y, en última instancia, pueden degradar nuestra capacidad para mantener la paz y la seguridad internacionales.

Reforzar el cumplimiento del derecho internacional y de las normas de comportamiento responsable de los Estados

La República Checa desea reiterar que el cumplimiento por parte de los Estados de sus obligaciones en virtud del derecho internacional es un ingrediente esencial para mantener un ciberespacio libre, pacífico, estable, seguro, interoperable y accesible. La aplicabilidad del derecho internacional vigente al uso de las TIC por parte de los Estados fue afirmada por todos los Estados, concretamente a través del respaldo universal de los informes del Grupo de Expertos Gubernamentales de 2013 y 2015 en las resoluciones 68/243 y 70/237 de la Asamblea General.

A este respecto, la República Checa recuerda también que los derechos de los Estados a ejercer una jurisdicción exclusiva sobre las TIC situadas en su territorio dan lugar no solo a derechos sino también a obligaciones específicas en virtud del derecho internacional. En particular, la República Checa desea reiterar que los corpus jurídicos existentes, incluido el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplican al comportamiento de los Estados en el ciberespacio sin excepción.

Lamentablemente, una pequeña minoría de Estados sigue cuestionando la aplicabilidad del derecho internacional vigente al ciberespacio, incluida la aplicabilidad del derecho internacional humanitario al uso de las TIC en el contexto de los conflictos armados. La República Checa desea subrayar que, en su opinión, la aplicabilidad del derecho internacional humanitario a las operaciones de las TIC no promueve la militarización del ciberespacio, ni tampoco la de ningún otro ámbito. Por el contrario, el derecho internacional humanitario pone límites al uso de la fuerza al exigir que todos los medios y métodos de guerra utilizados en el contexto de un conflicto armado se empleen de acuerdo con sus normas; incluidos los principios de humanidad, distinción y la regla de proporcionalidad.

Además, la República Checa recuerda que, de acuerdo con la ley de responsabilidad por hechos ilícitos internacionales, todos los Estados tienen la obligación de ejercer la debida diligencia y tomar medidas concretas dentro de su capacidad para garantizar que su territorio no se utilice para llevar a cabo actividades cibernéticas maliciosas contra otros Estados.

La República Checa reconoce igualmente que la capacidad del Estado para aplicar el marco existente de comportamiento responsable de los Estados en el ciberespacio, incluida su capacidad para ejercer adecuadamente la diligencia debida, está intrínsecamente ligada a las capacidades de dicho Estado. A este respecto, la República Checa subraya la necesidad de intensificar los esfuerzos internacionales para crear cibercapacidad y aumentar la ciberresiliencia a nivel mundial, incluso mediante el pronto establecimiento del programa de acción de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, que permitiría a los Estados Miembros avanzar en la aplicación de los compromisos existentes mediante una acción práctica y orientada a los resultados.

En conclusión, la República Checa está plenamente comprometida con un enfoque de la ciberseguridad centrado en el ser humano, que hace hincapié en la necesidad de proteger la seguridad de las personas en el entorno de las TIC, ya sea protegiendo la infraestructura crítica de las amenazas de las TIC o garantizando que las medidas de ciberseguridad no se utilicen como pretexto para restringir el pleno disfrute de los derechos humanos y las libertades fundamentales en el ciberespacio.

Anexo XXVI

Declaración conjunta de las Misiones Permanentes de Dinamarca, Finlandia, Islandia, Noruega y Suecia ante las Naciones Unidas

Tengo el placer de hacer uso de la palabra en nombre de los países nórdicos: Finlandia, Islandia, Noruega, Suecia y mi propio país, Dinamarca. Agradecemos a la presidencia estonia por incluir este tema tan pertinente en el programa del Consejo. Es una gran oportunidad para que todos los Estados Miembros se basen en nuestro compromiso con la aplicación del derecho internacional en el ciberespacio y el marco del comportamiento responsable de los Estados en el ciberespacio con el objetivo de promover la paz y la estabilidad.

El mundo se beneficia en innumerables maneras del desarrollo de la tecnología de la información y las telecomunicaciones. Ha aportado un enorme progreso económico y desarrollo social. En la actual pandemia, el ciberespacio nos ha permitido a muchos de nosotros mantener el contacto con la familia, los amigos y los colegas, así como mantener importantes funciones de la sociedad, incluido el funcionamiento de la infraestructura crítica vital para gestionar la crisis sanitaria. Sin embargo, el ciberespacio también se ha utilizado para difundir desinformación sobre el virus de enfermedad por coronavirus (COVID-19), exponiendo nuestra vulnerabilidad colectiva a la disrupción y el abuso del espacio informativo. Además, la pandemia ha dejado al descubierto profundas brechas digitales, entre ellas la de género. Como nórdicos, creemos firmemente que un ciberespacio mundialmente accesible, libre, abierto y seguro es fundamental no solo para el funcionamiento del mundo actual, sino para nuestras ambiciones comunes de construir un futuro mejor, más verde y seguro.

Lamentablemente, las ciberactividades maliciosas siguen desafiando la seguridad y la estabilidad del ciberespacio. El último año y medio ha revelado que los actores estatales y no estatales aprovecharán cualquier oportunidad, incluso una pandemia mundial, para llevar a cabo actividades maliciosas en el ciberespacio. Estas actividades son inaceptables. Amenazan la integridad, la seguridad y la prosperidad de nuestras sociedades y socavan la paz y la estabilidad internacionales.

Permítanme destacar tres tendencias interrelacionadas que plantean un reto para la paz y la seguridad internacionales.

En primer lugar, el reciente aumento de los ciberataques contra las cadenas de suministro de empresas, organizaciones y gobiernos ha dejado expuestos decenas, si no a cientos de miles de sistemas informáticos. Este tipo de ataques muestra una flagrante indiferencia hacia los afectados. El objetivo suele ser robar información sensible y propiedad intelectual para obtener una ventaja en la competencia geopolítica. Estos ataques podrían tener efectos adicionales no deseados, ya que las puertas traseras quedan abiertas para que todo el mundo las explote.

En segundo lugar, los ciberataques disruptivos patrocinados por el Estado, como WannaCry y NotPetya, se han lanzado al mundo con una total indiferencia a sus efectos sistémicos negativos en todo el mundo. Estos ataques no solo han provocado grandes pérdidas económicas, sino que también han paralizado los sistemas de tecnología de la información y las comunicaciones, incluidos los de los hospitales y

los sistemas de control industrial, afectando al crucial suministro de electricidad. Estas actividades ponen en peligro la salud y la seguridad de nuestros ciudadanos.

En tercer lugar, los Estados deben tomar medidas contra los efectos cada vez más graves y desestabilizadores de la ciberdelincuencia originada en su territorio. Los recientes ataques de programas maliciosos secuestradores contra el suministro de combustible en los Estados Unidos de América, los hospitales en Irlanda y la producción de alimentos en el Brasil, los Estados Unidos de América y Australia ilustran que las consecuencias de la ciberdelincuencia se han convertido en una preocupación de seguridad nacional con posibles efectos sobre la paz y la seguridad internacionales. La creciente combinación de grupos estatales y no estatales complica aún más la amenaza.

Día tras día, el umbral de comportamiento tolerado en el ciberespacio se mueve en la dirección equivocada. Debemos revertir esta tendencia cumpliendo con el compromiso compartido que nosotros, los Estados Miembros, asumimos cuando aprobamos los informes del Grupo de Expertos Gubernamentales y el informe de consenso del Grupo de Trabajo de Composición Abierta. Con este espíritu, reafirmamos una vez más que el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica al comportamiento de los Estados en el ciberespacio. También pedimos una mayor adhesión a las 11 normas voluntarias no vinculantes para el comportamiento responsable de los Estados en el ciberespacio formuladas en el informe del Grupo de Expertos Gubernamentales de 2015, teniendo en cuenta las orientaciones y la capa adicional de comprensión de estas normas, proporcionadas por el informe del Grupo de Expertos Gubernamentales de 2021. Esto contribuiría en gran medida a resolver los problemas mencionados anteriormente.

Debemos elevar el costo de la ciberactividad maliciosa exigiendo colectivamente responsabilidades a los responsables. Todos los Estados deben ejercer la debida diligencia y adoptar medidas adecuadas para abordar la ciberactividad malintencionada que tiene origen en sus territorios. No se debe permitir que los grupos hacker actúen con impunidad.

Respaldamos el intercambio continuo de información y mejores prácticas en el seno de las Naciones Unidas, en especial en la implementación de normas relativas al comportamiento responsable de los Estados, las medidas de fomento de la confianza y la aplicación del derecho internacional vigente en el ciberespacio. Deberíamos seguir un camino orientado a la acción que se base en el marco de consenso que ya hemos acordado con el respaldo de la Asamblea General al informe del Grupo de Trabajo de Composición Abierta y a los informes del Grupo de Expertos Gubernamentales. Esto constituye la base para futuros debates. La propuesta de establecer un programa de acción es una buena manera de avanzar hacia la plena aplicación de las normas ya acordadas.

Debemos reconocer que, aunque la ciberamenaza es un reto mundial, tiene diferentes manifestaciones en los distintos países y regiones. Mantener una fuerte ciberresiliencia en todas nuestras sociedades es crucial no solo para nuestra seguridad compartida, sino para el disfrute de los derechos humanos. Tenemos que cooperar para crear capacidad a nivel mundial.

Los Estados no pueden hacerlo solos. La lucha contra las amenazas en el ciberespacio requiere un enfoque de múltiples partes interesadas para ayudar a prevenir conflictos, crear un entendimiento común y aumentar la creación de confianza y capacidad. Necesitamos a las Naciones Unidas como convocante y plataforma para establecer una cooperación eficaz entre los gobiernos, la sociedad civil, el mundo académico y el sector privado. Apoyamos la Hoja de Ruta del Secretario General para la Cooperación Digital, en particular en lo que se refiere a la participación del sector privado, que es vital para la gestión de la infraestructura crítica, la recopilación de información y la protección de sistemas y datos personales.

Todos los Estados deben estar a la altura de su responsabilidad y cumplir con el derecho internacional y respetar las normas en el ciberespacio. De lo contrario, la amenaza de la ciberactividad maliciosa para la paz y la seguridad internacionales seguirá creciendo. Los ciberataques seguirán aumentando el riesgo de conflicto, poniendo en peligro vidas humanas, violando los derechos humanos, ahogando la actividad económica, profundizando las líneas divisorias y provocando disputas. Todos los Estados tienen un papel que desempeñar en la promoción y el mantenimiento de un ciberespacio basado en normas, predecible, abierto, igualitario, libre, accesible, estable y seguro en beneficio de todos.

Anexo XXVII

Declaración del Representante Permanente del Ecuador ante las Naciones Unidas, Cristian Espinosa

[Original: español]

Permítanme en primer lugar felicitar a Estonia por incluir este tema en la agenda formal del Consejo de Seguridad tras un año de la reunión con arreglo a la fórmula Arria sobre el tema. Destaco además el liderazgo de la Primera Ministra Kaja Kallas en esta materia.

Destaco además la presentación de la Secretaria General Adjunta y Alta Representante para Asuntos de Desarme, Izumi Nakamitsu.

Este bienio 2020-2021 marcó un hito en materia de ciberdiplomacia no solo por el mandato y los resultados sustantivos alcanzados el 12 de marzo de 2021 por el primer 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 y por el consenso logrado el 28 de mayo del mismo año por el Grupo de Expertos Gubernamentales sobre el comportamiento responsable de los Estados en el ciberespacio, sino también porque la crisis de la pandemia causada por la enfermedad por coronavirus (COVID-19) que aceleró la transformación digital.

La pandemia impactó de diferentes maneras en todas las dimensiones de la paz y la seguridad. La ciberseguridad no fue la excepción. La seguridad de los servicios esenciales se convirtió en una de las preocupaciones más importante, así como la necesidad de preservar las infraestructuras críticas frente a los posibles ataques cibernéticos capaces de generar daños en el mundo físico.

Las amenazas que enfrentamos hoy son, en mayor medida, de naturaleza transnacional y la única forma de contrarrestarlas, tanto en el espacio físico como virtual, es a través de la cooperación y el diálogo internacional. En ese sentido si un Estado Miembro no está seguro, ninguno lo está.

Por eso el Ecuador reafirma su compromiso con las normas vigentes, según se reflejan en los informes del Grupo de Expertos Gubernamentales y el resultado del Grupo de Trabajo de Composición Abierta, en complemento al derecho internacional. Mi delegación desea insistir en que ninguna esfera puede quedar fuera del espectro del derecho internacional, incluido el derecho internacional de los derechos humanos y el derecho internacional humanitario, lo que no significa que la militarización del ciberespacio sea aceptable.

Por el contrario, el Ecuador defiende el uso exclusivamente pacífico del ciberespacio. La Carta de las Naciones Unidas prohíbe el uso de la fuerza, por lo que toda disputa internacional debe resolverse por medios pacíficos en el ciberespacio.

Promovemos en consecuencia el fomento de la confianza y la construcción de capacidades, para lo cual consideramos que se requiere de una plataforma operativa que facilite la implementación del marco existente por parte de los Estados. Esa plataforma podría corresponder a un programa de acción.

Defendemos y apoyamos cualquier mecanismo que favorezca una mayor cooperación internacional para reducir las asimetrías en la capacidad de implementar las reglas para un comportamiento responsable de los Estados.

Reconocemos además la contribución que las organizaciones regionales pueden brindar para el desarrollo de capacidades y para la implementación de las referidas normas. Destaco por ejemplo la valiosa labor de la Organización de los Estados Americanos en este ámbito, en particular en los esfuerzos contra el ciberdelito y el terrorismo.

Concluyo recordando la necesidad de preservar y promover un uso responsable de las tecnologías de la información y la comunicación como clave para garantizar la estabilidad y seguridad en el ciberespacio. Asimismo, consideramos que las normas existentes deben ser robustecidas tomando en cuenta el rápido desarrollo tecnológico. El Consejo de Seguridad, por su parte, debe considerar mecanismos de fortalecimiento del uso de las tecnologías como medios de consolidación de la paz en complemento a los esfuerzos regulares.

Anexo XXVIII

Declaración de la Misión Permanente de Egipto ante las Naciones Unidas

Egipto concede gran importancia a los aspectos de seguridad internacional de las tecnologías de la información y las comunicaciones (TIC) y pide encarecidamente que las Naciones Unidas desempeñen un papel central y de liderazgo en la promoción y el desarrollo de normas y principios para el uso de las TIC por parte de los Estados mediante un proceso inclusivo y equitativo con la participación de todos los Estados

Varios Estados están desarrollando capacidades de TIC para posibles usos maliciosos y fines militares ofensivos. El uso de las TIC en futuros conflictos entre Estados se está convirtiendo en una realidad y el riesgo de ataques dañinos de las TIC contra la infraestructura crítica es real y grave. Esta nueva carrera armamentística tiene ramificaciones de gran alcance para la paz, la seguridad y la estabilidad internacionales, especialmente porque las líneas entre las armas convencionales y las no convencionales siguen erosionándose.

Además, las tecnologías pertinentes desarrolladas por los Estados están siendo transferidas, copiadas o reproducidas por terroristas y delincuentes. El uso malintencionado de las TIC por parte de organizaciones terroristas y criminales constituye una grave amenaza para la paz y la seguridad internacionales, especialmente a la luz de los problemas relacionados con la atribución.

De acuerdo con el derecho internacional y la Carta de las Naciones Unidas, todos los Estados Miembros deben abstenerse de realizar cualquier acto que, a sabiendas o intencionadamente, dañe o perjudique el uso y funcionamiento de la infraestructura crítica de otros Estados, así como de interferir en sus asuntos internos.

No cabe duda de que los aspectos de la seguridad internacional de las TIC se han vuelto demasiado importantes y estratégicos como para dejarlos sin normas vinculantes claras a nivel internacional. Un proceso inclusivo dentro del sistema de las Naciones Unidas es la mejor y más eficiente manera de establecer acuerdos que sean equitativos, amplios y eficaces en este ámbito.

Las Naciones Unidas ya han dado algunos pasos para establecer un marco normativo que complemente los principios del derecho internacional. Con la reciente adopción por consenso del Informe Final del Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 73/27 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, las Naciones Unidas han establecido ya los elementos iniciales de un marco para la prevención de conflictos y la estabilidad en el ciberespacio.

La Asamblea General pidió a los Estados Miembros que se guíen en su uso de las TIC por las normas de comportamiento responsable del Estado contenidas en los informes consecutivos de los Grupos de Expertos Gubernamentales de la Primera Comisión. Sin embargo, la aplicación de estas modestas normas sigue siendo mínima en el mejor de los casos, debido a su carácter voluntario y a la falta de un mecanismo de seguimiento.

El éxito del Grupo de Trabajo de Composición Abierta, que es el primer proceso inclusivo sobre este importante tema, y la creación de un nuevo Grupo de Trabajo de Composición Abierta mediante la resolución 75/240 de la Asamblea General representan un progreso prometedor hacia un posible acuerdo sobre importantes entendimientos mutuos entre los Estados Miembros en una serie de aspectos clave.

Los procesos inclusivos dentro de las Naciones Unidas, principalmente bajo los auspicios de la Asamblea General, son la forma más eficiente de establecer acuerdos equitativos, amplios y eficaces en este ámbito. Por su parte, se anima al Consejo de Seguridad a que tenga en cuenta las oportunidades que ofrecen las tecnologías emergentes al examinar temas como el mantenimiento de la paz y la lucha contra el terrorismo. Sin embargo, el Consejo no debe ser utilizado como un órgano legislativo que intente establecer normas y reglas en nombre de los Estados Miembros en asuntos que necesariamente requieren procesos inclusivos y transparentes.

Las recomendaciones que han sido aprobadas por la Asamblea General por consenso pueden constituir la base de normas política o jurídicamente vinculantes, especialmente si se derivan de los principios del derecho internacional y de la Carta de las Naciones Unidas.

Egipto también ha alentado la consideración del establecimiento de una plataforma institucional inclusiva dedicada a la cooperación internacional para salvaguardar los usos pacíficos de las TIC y mitigar sus riesgos asociados.

Aunque creemos que el derecho internacional y los principios de la Carta se aplican a todos los ámbitos, incluido el ciberespacio, también creemos que existe una necesidad urgente de identificar obligaciones específicas que hagan que el comportamiento de los Estados en el ciberespacio sea coherente con el derecho internacional y los objetivos de la Carta de las Naciones Unidas.

En un mundo cada vez más conectado, cualquier régimen internacional de ciberseguridad será tan fuerte como su eslabón más débil. Afortunadamente, existe un consenso sobre la necesidad de intensificar y fortalecer las actividades de creación de capacidad a fin de prevenir posibles ataques contra la infraestructura crítica y desarrollar las capacidades y las habilidades técnicas necesarias en los países en desarrollo. Las Naciones Unidas deberían liderar un esfuerzo coordinado para proporcionar la ayuda necesaria a los países en desarrollo.

En conclusión, las TIC ofrecen grandes oportunidades y desafíos. Y subrayamos que existe una necesidad apremiante de identificar y desarrollar normas de comportamiento responsable de los Estados para aumentar la estabilidad y la seguridad en el entorno mundial de las TIC y evitar que el ciberespacio se convierta en otro escenario de conflictos y carreras armamentísticas.

Anexo XXIX

Declaración de la Misión Permanente de El Salvador ante las Naciones Unidas

[Original: español]

El Salvador agradece a la delegación de Estonia en su calidad de Presidencia del Consejo de Seguridad para el mes de junio de 2021, por la organización de este debate abierto, el cual significa la primera vez que el Consejo de Seguridad aborda de manera sustantiva y bajo un formato formal el asunto de la ciberseguridad. Esta iniciativa es una medida muy importante para que este órgano dé cumplimiento al compromiso internacional de considerar a nivel multilateral las amenazas existentes y potenciales en el ámbito de la seguridad en el campo de la información y las telecomunicaciones.

El desarrollo de nuevas tecnologías representa una importante oportunidad para promover el desarrollo económico y social de los Estados. Sin embargo, estos sistemas de información son vulnerables a los ataques de personas que intentan manipular estas redes de comunicación con fines ideológicos o para beneficio propio. Dado que los delincuentes y los terroristas se aprovechan de las nuevas tecnologías de la información y telecomunicaciones para el cumplimiento de sus objetivos, es necesario invertir esfuerzos y recursos para trabajar en directrices especializadas para el desarrollo y la aplicación de normas comunes que nos ayuden a prevenir este tipo de delitos, al mismo tiempo, que facilite la aplicación de la justicia a quienes actúan al margen de ellos.

En ese sentido, destacamos la importancia de los instrumentos internacionales y regionales relacionados con la lucha contra la ciberdelincuencia, así como los avances en la materia, tales como el establecimiento del Grupo de Trabajo de Composición Abierta que tiene a su cargo elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

Acoge con satisfacción los esfuerzos realizados por los Estados Miembros de las Naciones Unidas en materia de terrorismo dentro de la agenda internacional de paz y seguridad. No obstante, constatamos que, de los instrumentos internacionales vinculantes en esta materia, aún no es posible encontrar una mención directa al ciberespacio. Se trata entonces de una brecha que todos debemos de estrechar lo antes posible. Celebra los esfuerzos del Consejo de Seguridad por debatir esta importante amenaza de manera sustantiva y con vistas a ofrecer soluciones eficaces. Insta a este órgano de las Naciones Unidas a que continúe estos esfuerzos, dejando de lado cualquier interés político y/o particular, manteniendo el objetivo en la prevención de nuevos conflictos y la creación de escenarios para su desarrollo.

El Salvador recuerda la resolución 58/199, que la Asamblea General aprobó en 2004, que incluye una lista de aquellos componentes de la infraestructura crítica de un Estado, que debido a la creciente interdependencia tecnológica está expuesta a un número cada vez mayor y a una mayor variedad de amenazas. Esta resolución también reconoce que las vulnerabilidades de las infraestructuras críticas siguen planteando importantes problemas de seguridad.

Además, a fin de crear las condiciones para avanzar hacia el objetivo común de la paz y la seguridad internacionales, el pleno ejercicio de los derechos humanos y el desarrollo económico y social, creemos que el marco previsto en la resolución 58/199 de la Asamblea General, debe de ampliarse para abordar la necesidad de preservar las actividades de las infraestructuras críticas de los ciberataques, además de los esfuerzos actuales para evitar que el ciberespacio se convierta en una plataforma de propaganda para la radicalización, el reclutamiento y la recaudación de fondos para actividades delictivas.

El mundo continúa enfrentándose a uno de los mayores retos desde la creación de esta Organización, el brote de la pandemia por la enfermedad por coronavirus (COVID-19) ha puesto de manifiesto las vulnerabilidades de los sistemas esenciales de los Estados. Hemos visto como durante la pandemia por COVID-19 se han incrementado los ciberataques a sus sistemas nacionales de salud, poniendo en riesgo la vida de millones de personas e impactando directamente en las comunidades y sectores más vulnerables. Aprovecha este espacio para condenar los ciberataques en contra de la Organización Mundial de la Salud, y los intentos de suplantación de identidad sufridos durante los últimos meses. No cabe duda de que el incremento de la interconectividad supone que estos ataques podrían verse incrementados en los próximos años.

El uso malintencionado de las tecnologías de la información y telecomunicaciones se ha extendido en los últimos meses a los ataques cibernéticos en contra de los sectores energéticos, financieros y de suministros de alimentación; entre otros sectores, estos son altamente vulnerables a los ciberataques; asimismo, con propósitos influir en la percepción de los gobernantes e instituciones, hemos visto como se han incrementado las actividades de desinformación, acciones que tienen una alta capacidad de deslegitimar su labor, desencadenando inestabilidad y conflictos sociales.

Lo anterior hace imperativo continuar trabajando en su prevención y en una codificación del derecho internacional orientada a prevenir su mala utilización, que reconozca la interrelación con el derecho internacional humanitario aplicable, incluso en el ámbito de las operaciones cibernéticas durante los conflictos armados.

Insta en la importancia de trabajar sobre la base del consenso, sin la intención de imponer soluciones que no sean compatibles con la realidad de los Estados, así como asegurar que los avances logrados por la Asamblea General, a través de los diferentes acuerdos de consenso de los Grupos de Expertos Gubernamentales y 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; sean tomados en cuenta. Particularmente, celebramos la adopción por consenso del acuerdo del Grupo de Trabajo de Composición Abierta en 2021, donde participaron los 193 Estados Miembros de las Naciones Unidas, incluidos los 15 miembros del Consejo de Seguridad, y otras partes relevantes en este proceso.

El Salvador espera trabajar de forma constructiva 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 desarrollará sus labores sustantivas en el período 2021-2025, encomiamos la labor del Representante Permanente de Singapur ante las Naciones Unidas, Burhan Gafoor, en su calidad de presidencia designada de este proceso.

Destaca el papel fundamental de las organizaciones regionales, el sector privado, la sociedad civil, la academia y otros sectores relevantes para prevenir y combatir estas amenazas. Expresa la urgencia de seguir trabajando en el fortalecimiento de los mecanismos de cooperación regional e internacional para prevenir y combatir estos desafíos, a través de un dinámico intercambio de información y buenas prácticas, el fortalecimiento de capacidades, la estandarización de los marcos legales y el uso de las nuevas tecnologías como el camino para el desarrollo y el combate del crimen organizado.

Anexo XXX

Declaración del Jefe de la Delegación de la Unión Europea ante las Naciones Unidas, Olof Skoog

Es un honor para mí contribuir al debate abierto sobre la ciberseguridad en nombre de la Unión Europea y sus Estados miembros.

Se adhieren a esta declaración Turquía, la República de Macedonia del Norte*, Montenegro* y Albania*, países candidatos; Bosnia y Herzegovina, país del Proceso de Estabilización y Asociación y posible candidato, así como Ucrania y la República de Moldova.

En primer lugar, quisiéramos elogiar a Estonia por celebrar este debate abierto sobre este tema crucial, en un momento en el que las actividades cibernéticas maliciosas siguen en aumento, y en el que los crecientes desafíos que se plantean ponen en riesgo la seguridad y la estabilidad internacionales en el ciberespacio, en particular en estas circunstancias especiales de una pandemia.

La digitalización tiene un impacto cada vez mayor en nuestra seguridad, en las economías y en las sociedades en general, creando tanto oportunidades como desafíos. Los transportes, la energía y la salud, las telecomunicaciones, las finanzas, la seguridad, el proceso democrático, el espacio y la defensa dependen en gran medida de los sistemas de redes e información, que están cada vez más interconectados.

En este sentido, estamos especialmente alarmados por el reciente aumento de las actividades cibernéticas maliciosas dirigidas a operadores esenciales en todo el mundo, incluido el sector de la salud, y que afectan a la disponibilidad, la seguridad y la integridad de los productos y servicios de las tecnologías de la información y las comunicaciones (TIC) y, en consecuencia, a la continuidad de las operaciones, lo que podría tener efectos indirectos y sistémicos y aumentar los riesgos de conflicto.

Por lo tanto, acogemos con satisfacción la oportunidad de debatir esta importante cuestión en el Consejo de Seguridad, que tiene la responsabilidad principal de mantener la paz y la seguridad internacionales. Es una oportunidad para subrayar una serie de desafíos a los que se enfrenta, para reiterar los logros alcanzados hasta la fecha por la comunidad de las Naciones Unidas y para ofrecer una perspectiva sobre cómo abordar estas cuestiones en el seno de las Naciones Unidas.

A este respecto, la Unión Europea y sus Estados miembros se congratulan de los significativos informes acordados por consenso por el reciente Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional (Grupo de Trabajo de Composición Abierta) y el Grupo de Expertos Gubernamentales de las Naciones Unidas para promover un comportamiento responsable de los Estados en el ciberespacio.

Los informes contribuyen significativamente a aumentar la conciencia y permiten mejorar la capacidad de prevención, respuesta y recuperación ante ciberamenazas y ciberactividades maliciosas. Esto es muy necesario, ya que la falta

* La República de Macedonia del Norte, Montenegro, Serbia y Albania siguen formando parte del Proceso de Estabilización y Asociación.

de conciencia y de capacidades constituye una amenaza en sí misma, ya que todos los países dependen cada vez más de las TIC.

Por lo tanto, es esencial aumentar la ciberresiliencia mundial, ya que reduce la capacidad de los posibles autores de hacer un mal uso de las TIC con fines maliciosos. También permite a los Estados ejercer la debida diligencia y tomar las medidas apropiadas contra los actores que realicen dichas actividades desde su territorio, en consonancia con el derecho internacional y los informes aprobados por consenso de 2010, 2013, 2015 y 2021 de los Grupos de Expertos Gubernamentales de las Naciones Unidas (GEG) en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional.

Los informes del GEG sucesivos y del Grupo de Trabajo de Composición Abierta ofrecen una base para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, es decir, reafirman la aplicación del derecho internacional, abordan las normas de comportamiento responsable de los Estados, las medidas de fomento de la confianza en el ciberespacio y la creación de cibercapacidades.

La Unión Europea y sus Estados miembros reafirman que un marco para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio solo puede basarse en el derecho internacional vigente, que incluye la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, tal y como ha refrendado la Asamblea General desde 2013.

Profundizar en la comprensión de cómo se aplica el derecho internacional en el ciberespacio es reducir aún más los malentendidos y aumentar la rendición de cuentas en el ciberespacio, y los miembros de las Naciones Unidas deberían seguir avanzando y aplicando este marco con vistas a la seguridad y la estabilidad internacionales en el ciberespacio.

Por ejemplo, la Unión Europea y sus Estados miembros consideran que el derecho internacional humanitario es plenamente aplicable en el ciberespacio en el contexto de los conflictos armados. Reiteramos que su aplicación en el ciberespacio no debe entenderse erróneamente como una legitimación de cualquier uso de la fuerza incompatible con la Carta de las Naciones Unidas. El derecho internacional humanitario establece protecciones esenciales para quienes no participan, o ya no participan, en las hostilidades, entre otras cosas para proteger a los civiles contra los efectos de las hostilidades y a los combatientes contra sufrimientos innecesarios. También impone límites a los medios y métodos de guerra permitidos, incluidos los nuevos.

En segundo lugar, la adhesión a las normas de comportamiento responsable del Estado es de suma importancia. El conjunto de las normas acordadas refleja las expectativas compartidas de la comunidad internacional, que establecen estándares de comportamiento responsable de los Estados. Permite a la comunidad internacional evaluar las actividades e intenciones de los Estados para prevenir conflictos y aumentar la estabilidad y seguridad en el ciberespacio.

En tercer lugar, las medidas de fomento de la confianza relacionadas con el ciberespacio constituyen un medio práctico para prevenir conflictos. Mediante la cooperación y el intercambio de información, las medidas regionales de fomento de

la confianza han demostrado que reducen el riesgo de interpretaciones erróneas, escaladas y conflictos que pueden derivarse de los incidentes relacionados con las TIC.

Por último, el marco incluye la importante cuestión de la creación de capacidades. Apoyamos activamente el llamamiento a una mejor coordinación para mejorar la coherencia de los esfuerzos de creación de capacidades en el uso de las TIC para cerrar la brecha digital, incluso mediante nuestros numerosos esfuerzos con asociados de todo el mundo.

La Unión Europea apoya la labor de creación de cibercapacidades a través de sus Instrumentos de Financiación Exterior, que abarcan una serie de programas de alcance mundial que incluyen acciones ejecutadas en África, Asia y América Latina, así como en los países vecinos de la Unión Europea y los Balcanes Occidentales. Concretamente, la Unión Europea está invirtiendo actualmente en actividades en todo el mundo, para apoyar la aplicación en cooperación con sus asociados en la ejecución, a través de proyectos como la Ciberresiliencia para el Desarrollo de la Unión Europea, Glacy+, EU Cyber Direct y la Iniciativa de Seguridad Reforzada en y con Asia.

Para subrayar el marco de la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, la Unión Europea seguirá promoviendo un comportamiento responsable en el ciberespacio. En este sentido, la Unión Europea y sus Estados miembros se comprometen a resolver las controversias internacionales por medios pacíficos también cuando dichas controversias surjan en el ciberespacio.

El marco para una respuesta diplomática conjunta de la Unión Europea, por lo tanto, forma parte del planteamiento de la Unión Europea en materia de ciberdiplomacia, que contribuye a la prevención de conflictos, a contrarrestar las amenazas para la ciberseguridad y a una mayor estabilidad en las relaciones internacionales. Con el fin de promover y proteger un ciberespacio abierto, libre, estable y seguro, la Unión Europea seguirá utilizando su caja de herramientas de ciberdiplomacia y cooperando con los asociados internacionales a tal fin.

Desde el principio, y dada la compleja naturaleza del ciberespacio, es de suma importancia que los Estados, así como la comunidad multipartita, aborden los desafíos que el ciberespacio conlleva, mejoren la cooperación y refuercen sus capacidades. También tenemos la responsabilidad primordial de permitir que todas las partes interesadas asuman su responsabilidad de promover un ciberespacio abierto, libre, seguro y estable, basado en los derechos humanos, las libertades fundamentales, la democracia y el estado de derecho, y de apoyar sus esfuerzos. El enfoque de la Unión Europea sobre la ciberdiplomacia también tiene en cuenta la importancia de la perspectiva de género para reducir la “brecha digital de género” y promover una participación efectiva y significativa de las mujeres en los procesos de toma de decisiones relacionados con el uso de las TIC en el contexto de la seguridad internacional.

Para reforzar la cooperación, consideramos que las Naciones Unidas deben desempeñar un papel central para avanzar en la aplicación de los logros alcanzados hasta la fecha. Para promover un debate multilateral eficaz entre las múltiples partes interesadas con el fin de avanzar en la paz y la seguridad en el ciberespacio, existe una clara necesidad de llevar adelante el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. Junto con 53 Estados

Miembros, la Unión Europea propone establecer un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio.

Basándose en el acervo vigente aprobado por la Asamblea General, el programa de acción ofrece una plataforma permanente para la cooperación y el intercambio de mejores prácticas en las Naciones Unidas. El programa de acción ofrece la oportunidad de fomentar programas de creación de capacidades adaptados a las necesidades identificadas por los Estados beneficiarios. También proporciona un mecanismo institucional dentro de las Naciones Unidas para mejorar la cooperación con otras partes interesadas, como el sector privado, el mundo académico y la sociedad civil, sobre sus respectivas responsabilidades para mantener un entorno de TIC abierto, libre, seguro, estable, accesible y pacífico.

Debido al carácter permanente y orientado a la acción de esta plataforma, creemos que la propuesta de programa de acción es oportuna y merece ser estudiada por la comunidad internacional. Constituye una base sólida y orientada a la acción para seguir trabajando en el marco de la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio y para garantizar que los Estados puedan aprovechar los beneficios de un ciberespacio mundial, abierto, estable y seguro.

Anexo XXXI

Declaración de la Misión Permanente de Georgia ante las Naciones Unidas

Queremos expresar nuestra gratitud a la Presidencia estonia por haber convocado el debate de alto nivel de hoy sobre esta importante cuestión y dar las gracias a los distinguidos oradores.

Georgia lleva mucho tiempo comprometida con el desarrollo de un ciberespacio responsable y ético, que incluya la ciberseguridad y la resiliencia, a fin de habilitar marcos integrales para un entorno digital seguro, confiable y de confianza en beneficio de toda la nación. En la última década, establecimos la base legal necesaria de la información y la ciberseguridad e identificamos los temas críticos del sistema de información; adoptó y aplicó dos estrategias de ciberseguridad con los correspondientes planes de acción; y está en marcha el proceso de adopción para la tercera estrategia nacional de ciberseguridad.

Sin embargo, como todos sabemos, junto con las grandes oportunidades económicas y sociales, la innovación y el desarrollo, el ciberespacio trae consigo nuevos tipos de amenazas a la seguridad. En los últimos años hemos sido testigos de cómo el ciberespacio se ha utilizado no solo con fines de terrorismo, fraude y delincuencia, sino también como una poderosa herramienta para la guerra híbrida y la injerencia en los asuntos internos de los Estados.

Desgraciadamente, la guerra híbrida también se ha convertido en un poderoso instrumento en manos de algunos Estados para promover sus intereses nacionales, y como este órgano está bien informado, Georgia tiene una larga y dolorosa experiencia en el tratamiento de amenazas híbridas procedentes de uno de sus miembros permanentes. La Federación de Rusia lleva librando una guerra híbrida contra Georgia desde principios de los años 90 y nunca ha dejado de intentar socavar la soberanía, la integridad territorial y las aspiraciones europeas y euroatlánticas de nuestro país.

La lista de incidentes es extensa. En agosto de 2008, durante la agresión militar a gran escala de Rusia contra Georgia, asistimos al primer precedente de un ciberataque masivo realizado en paralelo a la agresión en curso. En 2019, se lanzó un ciberataque en gran escala contra los sitios web, los servidores y otros sistemas operativos de la Administración del Presidente de Georgia, los Tribunales, asambleas municipales, órganos estatales, organizaciones del sector privado y medios de comunicación. Gracias a la investigación realizada por las autoridades de Georgia, en cooperación con nuestros asociados, se llegó a la conclusión de que este ciberataque había sido planeado y ejecutado por la División Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia.

Lamentablemente, incluso cuando la comunidad internacional está luchando contra la pandemia de enfermedad por coronavirus (COVID-19), la Federación de Rusia sigue intentando obtener dividendos políticos intensificando la guerra propagandística contra una de las instituciones más exitosas de Georgia en la lucha contra la propagación del coronavirus: el Centro Richard Lugar para la Investigación de la Salud Pública. Las acusaciones de Rusia representan una típica campaña de información errónea y propaganda contra este laboratorio único que se creó para identificar y hacer frente a brotes como el de la pandemia.

Hoy en día, todos somos testigos de la aplicación agresiva del conjunto de herramientas híbridas por parte de Rusia, no solo en nuestra región, sino también a escala mundial. Los instrumentos más destacados de la caja de herramientas híbrida rusa son la presencia militar, las operaciones de información, los ciberataques, el apoyo a grupos políticos interpuestos, la injerencia en los asuntos internos y la influencia económica.

En conclusión, debemos subrayar que los ciberataques y la guerra híbrida contra Estados soberanos representan graves violaciones del derecho internacional, sus normas y principios, y socavan la paz y la seguridad internacionales. Y a la vez que reafirmamos nuestro compromiso de seguir reforzando la ciberseguridad a nivel nacional e internacional, también hacemos un llamamiento a la comunidad internacional para que preste más atención a las actividades maliciosas de la Federación de Rusia en materia de tecnologías de la información y las comunicaciones en Georgia y en otros lugares.

Anexo XXXII

Declaración de la Misión Permanente de Alemania ante las Naciones Unidas

Hace un año y medio, la pandemia de enfermedad por coronavirus (COVID-19) asoló el mundo y nos hizo tomar conciencia, con dramática brusquedad, de hasta qué punto las tecnologías digitales configuran tanto nuestra vida cotidiana como nuestra capacidad de recuperación económica. Al mismo tiempo, ha expuesto sin piedad nuestras vulnerabilidades. Los ciberataques, incluidos los realizados contra las infraestructuras críticas, pueden constituir una amenaza para la paz y la seguridad internacionales, y Alemania sigue convencida de que este es un tema importante para el Consejo de Seguridad.

La paz y la seguridad internacionales se ven sometidas a presiones desde distintos frentes: en primer lugar, las actividades de los ciberdelincuentes socavan la fiabilidad y la confianza en las tecnologías que, a día de hoy, son cruciales para el funcionamiento de nuestras economías, gobiernos y sociedades modernas en su conjunto. Por citar solo algunos ejemplos, desde el estallido de la pandemia de COVID-19 se ha producido un fuerte aumento de los ataques de denegación de servicio, el phishing y la propagación de programas maliciosos. También aumentan los ataques a la infraestructura crítica en Europa y América del Norte y los ciberataques utilizados como vehículo de extorsión.

En segundo lugar, las actividades cibernéticas maliciosas patrocinadas por los Estados con fines de espionaje, sabotaje, desinformación y desestabilización o beneficio financiero están dañando tanto la confianza internacional como los mecanismos de cooperación para la mitigación de conflictos, y por lo tanto amenazan la seguridad en todo el mundo.

En tercer lugar, la sociedad civil en su conjunto y los defensores de los derechos humanos en particular están sometidos a una presión creciente en el ciberespacio. El espacio para la libertad de expresión, la transparencia y la comunicación genuina, para la que se ha diseñado Internet, sigue reduciéndose.

Para hacer frente a estas crecientes amenazas, es necesario adoptar un enfoque basado en varios pilares: uno de ellos es reforzar nuestra resiliencia a nivel nacional e internacional. Esto incluye la mejora de la infraestructura técnica y las capacidades políticas y jurídicas, así como una mayor cooperación internacional.

Un segundo pilar consiste en seguir avanzando y definiendo nuestra comprensión común del comportamiento responsable de los Estados en el ciberespacio y en fijar las líneas rojas que no deben cruzarse. Por lo tanto, debemos defender el acervo vigente logrado por el Grupo de Trabajo de Composición Abierta y el Grupo de Expertos Gubernamentales y seguir avanzando en el desarrollo de normas de comportamiento responsable de los Estados.

La posición de Alemania es que el derecho internacional, incluida la Carta de las Naciones Unidas y el derecho internacional humanitario, se aplica tanto en línea como fuera de ella. Los Estados deben abstenerse estrictamente de apoyar actividades relacionadas con las tecnologías de la información y las comunicaciones (TIC) que sean contrarias a las obligaciones que les impone el derecho internacional, sobre todo

por su potencial para crear y agravar las tensiones interestatales. La actividad de las TIC no debe dañar intencionalmente la infraestructura crítica ni perjudicar de otro modo su uso y funcionamiento. En particular, ningún actor debe poner en peligro la disponibilidad general o la integridad del núcleo público de Internet, que es vital para la estabilidad del ciberespacio. Exhortamos a todos los Estados para que cumplan estrictamente sus obligaciones de diligencia debida y tomen medidas rápidas contra los actores que lleven a cabo actividades cibernéticas maliciosas desde su territorio, de acuerdo con el derecho internacional.

Para estimular los debates en curso sobre el derecho internacional en el ciberespacio, Alemania ha publicado un documento político sobre la aplicabilidad del derecho internacional en el ciberespacio, y animamos a otros a hacer lo mismo.

Sin embargo, no basta con acordar un acervo común. Es igualmente importante que haya una respuesta firme al comportamiento inaceptable. Se pueden considerar varios instrumentos, que van desde el diálogo y el intercambio hasta las declaraciones políticas de los Estados o grupos de Estados en las que se exponen y denuncian los comportamientos irresponsables, o se imponen sanciones a las personas y entidades pertinentes. Junto con nuestros asociados de la Unión Europea, hemos puesto en marcha un régimen de sanciones relacionadas con la cibernética que nos permite responder a los ciberataques de manera firme, eficaz y específica, y en plena consonancia con el derecho internacional. Hemos utilizado este instrumento en el pasado y no dudaremos en volver a utilizarlo si nuestra seguridad se ve comprometida. Además, una cultura de atribución puede reforzar el marco normativo y fomentar la responsabilidad en el ciberespacio.

Un intercambio continuo con la sociedad civil, el sector privado y el mundo académico es esencial para aumentar nuestra capacidad de resiliencia en el ciberespacio y hacer avanzar la causa de la gobernanza de Internet. La abundante experiencia que reside fuera de las autoridades debe ser aprovechada e incluida en estos esfuerzos, con el objetivo de mantener la paz y la seguridad internacionales en el ciberespacio.

Anexo XXXIII

Declaración de la Misión Permanente de Grecia ante las Naciones Unidas

Las tecnologías digitales contribuyen profundamente a la transformación actual de las economías y las sociedades, ofreciendo importantes oportunidades de crecimiento económico, así como de desarrollo sostenible e integrador. El ciberespacio, en particular, se ha convertido en una de las columnas vertebrales de nuestras sociedades. Al mismo tiempo, el aumento de los comportamientos malintencionados en el ciberespacio, incluido el abuso de las tecnologías de la información y las comunicaciones (TIC) por parte de actores estatales y no estatales con fines maliciosos, se ha convertido en la fuente de nuevos riesgos y desafíos. Estos comportamientos amenazan el crecimiento económico y pueden provocar efectos desestabilizadores y en cascada con mayores riesgos de conflicto.

Por lo tanto, apoyamos firmemente el marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, aprobado por la Asamblea General, y destacamos la necesidad de centrar nuestros esfuerzos colectivos en el desarrollo de las habilidades y la capacidad para hacer frente adecuadamente a las ciberamenazas. La necesidad de una ciberresiliencia mundial se pone de manifiesto en la actual crisis sanitaria mundial, en la que hemos observado ciberamenazas y ciberactividades maliciosas dirigidas al sector de salud.

La ciberresiliencia mundial reduce la capacidad de los posibles autores de hacer un uso indebido de las TIC y refuerza la capacidad de los Estados para responder eficazmente a los ciberincidentes y recuperarse de ellos. Como parte de nuestros últimos esfuerzos por reforzar la resiliencia mundial y desarrollar medidas prácticas de cooperación, actualmente estamos organizando un seminario regional sobre ciberseguridad, con participantes de los Balcanes Occidentales.

A través de nuestra participación en organizaciones internacionales como las Naciones Unidas, la OTAN y la Organización para la Seguridad y la Cooperación en Europa, tratamos de cooperar, intercambiar experiencias y mejores prácticas, y contribuir en la mayor medida posible a desarrollar medios adecuados para hacer frente a las ciberamenazas. Además, como miembro de la Unión Europea, aplicamos un marco estratégico inclusivo y multifacético para la prevención de conflictos y la estabilidad en el ciberespacio. Dentro de la Unión Europea, la ciberseguridad es un esfuerzo coordinado y colectivo entre los Estados miembros que sienta un precedente único y valioso de cooperación multilateral.

Estamos muy comprometidos con un ciberespacio mundial, pacífico, seguro, abierto e independiente, regido por el derecho internacional, en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho. Hemos compartido activamente nuestras experiencias en la aplicación de las normas, las medidas de fomento de la confianza y la creación de capacidades, tanto a nivel bilateral como multilateral, en todos los foros regionales e internacionales en los que participamos. Estamos muy comprometidos a participar activamente en debates posteriores en las Naciones Unidas sobre los problemas de ciberseguridad, y reafirmamos nuestra voluntad de participar de forma activa en un esfuerzo para realizar progresos constructivos.

Anexo XXXIV

Declaración de la Misión Permanente de Guatemala ante las Naciones Unidas

Guatemala desea expresar su agradecimiento a la delegación de Estonia en su calidad de Presidente del Consejo de Seguridad por haber convocado este debate abierto sobre un tema que, sin duda, es de suma importancia para los Estados. El ciberespacio se ha convertido en un ámbito central e indispensable de la actividad mundial, y su protección mediante un comportamiento responsable de los Estados es fundamental para garantizar el mantenimiento de la paz y la seguridad internacionales. Confiamos en que este tipo de reuniones sean una excelente oportunidad para que nuestros países intercambien opiniones y buenas prácticas sobre los diferentes niveles de aplicación de un tema cada vez más relevante.

El mundo se enfrenta actualmente a varios desafíos de seguridad que se ven agravados por la aparición de nuevas amenazas, como los problemas de ciberseguridad. Si recordamos los ciberataques del pasado, así como su incremento en tiempos de la pandemia de enfermedad por coronavirus (COVID-19), la necesidad de abordar este tema es evidente, sobre todo si tenemos en cuenta que puede afectar a los sectores más vulnerables de nuestra sociedad.

Las amenazas y ataques cibernéticos surgen y evolucionan derivados de las diversas actividades que se desarrollan por la interconexión de los medios digitales, lo que representa una complejidad de condiciones que requieren la participación y cooperación de todos los sectores de nuestros países, con el fin de desarrollar los marcos técnicos y legales que fortalezcan la ciberseguridad tanto a nivel nacional como mundial.

Como ocurre en todos los países, el aumento del uso de las tecnologías de la información y las comunicaciones (TIC) se ha generalizado en todos los sectores de nuestra sociedad. Este nuevo escenario facilita un desarrollo sin precedentes del intercambio de información y de las comunicaciones, pero al mismo tiempo implica nuevos riesgos y amenazas que pueden afectar a la seguridad de nuestras poblaciones.

Por ello, mi delegación quiere expresar su preocupación por estas nuevas tecnologías, especialmente por el carácter civil y de doble uso del ciberespacio y las redes digitales, que pueden ser utilizadas por grupos criminales y terroristas. Es extremadamente preocupante que varios Estados estén desarrollando capacidades en materia de tecnologías de la información y las comunicaciones con fines militares y que la utilización de estas tecnologías en futuros conflictos entre Estados se está volviendo cada vez más probable.

Guatemala reconoce que la naturaleza interconectada y compleja del ciberespacio requiere de los esfuerzos conjuntos de los gobiernos, el sector privado, la sociedad civil y la academia para abordar los desafíos de la ciberseguridad de manera integral y equilibrada. Es responsabilidad de todos estos sectores mantener un ciberespacio abierto, libre, seguro y estable.

Por esta razón, mi país promueve medidas de fomento de la confianza y de transparencia y apoya las actividades de creación de capacidades, el intercambio de

información y la difusión de las mejores prácticas, tanto a nivel subregional como regional e internacional.

Mi delegación subraya que la aplicabilidad del derecho internacional al comportamiento de los Estados en el ciberespacio, las normas voluntarias no vinculantes de comportamiento de los Estados aplicables en tiempo de paz y la aplicación de medidas de fomento de la confianza, siguen siendo cruciales. Además, tras comprobar las diferencias existentes entre los países en materia de ciberseguridad y defensa, mi país presta especial interés a los esfuerzos de creación de capacidades para encontrar un terreno de juego más equitativo que ayude a mantener la paz y la seguridad internacionales.

Guatemala considera que las organizaciones regionales desempeñan un papel indispensable en el establecimiento de la paz sobre el terreno. Existe un potencial considerable para aumentar su presencia en el ciberespacio, tanto a nivel regional como mundial, para avanzar de forma innovadora en el programa de sostenimiento de la paz. Las organizaciones regionales y subregionales se han centrado en mejorar la seguridad de los Estados, lo que ha supuesto un gran avance en la aplicación de medidas prácticas de fomento de la confianza en las distintas regiones para mejorar la ciberestabilidad. No cabe duda de que, sin la contribución de estas organizaciones, los esfuerzos de prevención de conflictos y estabilidad serían menores.

Guatemala cuenta actualmente con una Estrategia Nacional de Ciberseguridad cuyo objetivo principal es fortalecer las capacidades del país, creando el entorno y las condiciones necesarias para garantizar la participación, el desarrollo y el ejercicio de los derechos de las personas en el ciberespacio. Además, cuenta con un Centro de Respuesta a Emergencias Informáticas (EREI), que ofrece servicios de auditoría de ciberseguridad, exploración de vulnerabilidades y clasificación de alertas. Ambos se lograron con el acompañamiento de la Organización de los Estados Americanos.

Además, Guatemala se encuentra en proceso de elaboración de una ley sobre ciberdelincuencia, definiendo claramente las líneas de actuación y los tipos de delitos con y en las TIC para promover la capacitación a través de la cooperación internacional, favoreciendo el debido proceso al contar con protocolos bien definidos para la cadena de custodia y el manejo de la evidencia digital. También es necesario mencionar que mi país tiene el honor de ser un país observador del Convenio sobre la Ciberdelincuencia, que pretende hacer frente a los delitos informáticos y a los delitos en Internet mediante la armonización de las leyes entre las naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

Mi delegación considera la necesidad de continuar realizando transformaciones y adecuaciones en las leyes que rigen en cada país de manera armonizada y diseñar sistemas que permitan la detección, investigación y enjuiciamiento de probables delitos en un marco que salvaguarde los derechos de las personas y al mismo tiempo reduzca el riesgo de que las redes de computadoras sean utilizadas en contra de la confidencialidad, integridad y disponibilidad de la información. Esperamos que nuestro debate de hoy contribuya positivamente y complemente el proceso de elaboración de cibernormas que se está llevando a cabo en la Asamblea General, en particular a través de los significativos trabajos del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta para el período 2021-2025.

Por último, les recordamos a los Estados que las TIC deben ser utilizadas de forma pacífica y por el bien común de la humanidad, promoviendo el desarrollo sostenible de todos los países, independientemente de su nivel de desarrollo científico y tecnológico.

Anexo XXXV

Declaración del Encargado de Negocios de Indonesia ante las Naciones Unidas, Mohammad Kurniadi Koba

Permítaseme dar las gracias a Estonia por haber convocado esta reunión. También me gustaría agradecer a la ponente su valiosa información.

A medida que aumenta la dependencia de las personas de la conectividad digital, las tecnologías de la información y las comunicaciones (TIC) se han convertido en parte integrante de nuestra vida cotidiana.

Además, durante la pandemia de enfermedad por coronavirus (COVID-19), las TIC han sido un salvavidas para los sectores público y privado en la prestación de servicios esenciales para la población.

A este respecto, es fundamental subrayar que las actividades cibernéticas maliciosas por parte de actores estatales y no estatales, en particular las dirigidas a la infraestructura crítica, podrían poner en peligro la estabilidad nacional, así como la paz y la seguridad internacionales.

En ese contexto, Indonesia desea destacar lo siguiente:

En primer lugar, la primacía del estado de derecho para guiar nuestro comportamiento en el uso de las TIC, así como su implicación en la paz y la seguridad internacionales.

Los principios del derecho internacional y la Carta de las Naciones Unidas proporcionan las normas jurídicas fundamentales que guían a los Estados en el uso de las TIC, incluso para responder a cualquier ataque malicioso.

Todos los Estados deben guiarse por el mismo conjunto de normas y leyes. Nadie debería estar exento.

Además, Indonesia apoya las normas de comportamiento responsable de los Estados que se incluyen en la resolución 70/237 de la Asamblea General.

Si bien seguimos abordando la creciente necesidad de identificar y desarrollar un marco jurídico internacional en esta materia, nuestro esfuerzo debe dirigirse también a subsanar las deficiencias entre países y regiones.

Aparte de las brechas técnicas, es imperativo reforzar los marcos políticos nacionales, así como la aplicación del derecho internacional vigente y de las normas voluntarias y no vinculantes en el ciberespacio.

En segundo lugar, el papel de los enfoques bilaterales, regionales y multilaterales en el fortalecimiento de la confianza en el ciberespacio.

Las medidas de cooperación a nivel bilateral, regional y multilateral se refuerzan mutuamente a la hora de avanzar en la comprensión y reforzar la estabilidad en el ciberespacio, en particular en el ámbito de la creación de capacidad y confianza.

Las medidas de fomento de la confianza de la ASEAN, mediante el establecimiento de puntos de contacto, los intercambios periódicos de información, el diálogo y la puesta en común de las mejores prácticas, han contribuido a la

ciberestabilidad en la región de Asia Sudoriental y fuera de ella, en particular a través del Foro Regional de la ASEAN.

Además, Indonesia subraya el mérito de una asociación significativa con otras entidades multipartitas para ayudar a los Estados a aplicar el marco de comportamiento responsable en su uso de las TIC.

En este sentido, destacamos la necesidad de que los países desarrollados compartan las tecnologías de las TIC con los países en desarrollo. Al igual que todos los demás problemas mundiales, garantizar que los demás dispongan de las herramientas y capacidades adecuadas para hacer frente a esta amenaza contribuirá a la estabilidad general en el ámbito de las TIC.

En tercer lugar, el papel de las Naciones Unidas a la hora de liderar un esfuerzo coordinado para abordar los conflictos que puedan derivarse de los incidentes de las TIC.

El de hoy es el primer debate oficial del Consejo dedicado al impacto de las tecnologías de la información y las comunicaciones en el mantenimiento de la paz y la seguridad internacionales.

Supone un importante paso adelante en esta cuestión en las Naciones Unidas.

En el futuro, el Consejo debe anticiparse al aumento de las amenazas en la ciberesfera, así como a posibles incidentes significativos en el entorno de las TIC que podrían dar lugar a una guerra importante.

Subrayamos la importancia de garantizar que las acciones de las Naciones Unidas se mantengan coordinadas y en sinergia. El Consejo debe seguir respondiendo a la paz y la seguridad internacionales, así como a las implicaciones humanitarias de los avances en el ámbito de las TIC.

Al mismo tiempo, el Consejo debe guiarse por las normas y reglas que delibera y desarrolla la Asamblea General.

Permítanme concluir reiterando el compromiso de Indonesia de avanzar en nuestros esfuerzos comunes para responder adecuadamente a los desafíos cada vez mayores para el mantenimiento de la paz y la seguridad relacionados con el uso de las TIC.

Anexo XXXVI

Declaración del Comité Internacional de la Cruz Roja

El Comité Internacional de la Cruz Roja (CICR) agradece la oportunidad de contribuir a este debate abierto del Consejo de Seguridad sobre “El mantenimiento de la paz y la seguridad internacionales en el ciberespacio”.

En las dos últimas décadas, las ciberoperaciones hostiles se han convertido en una preocupación cada vez más importante para el mantenimiento de la paz y la seguridad internacionales. A medida que las sociedades se digitalizan, también lo hacen las capacidades militares de los Estados y otros actores. Hoy, la comunidad internacional reconoce que “varios Estados están desarrollando capacidades en materia de TIC con fines militares” y que “la utilización de esas tecnologías en futuros conflictos entre Estados se está volviendo cada vez más probable”[10].

A la luz de esta realidad, el CICR desea recordar los daños potenciales que el uso de la cibertecnología puede causar a los seres humanos y, posteriormente, presentar la forma en que los Estados pueden mitigar estas consecuencias humanitarias adversas a través de acciones a nivel internacional y nacional.

Hoy en día es bien sabido que las ciberoperaciones contra infraestructuras civiles críticas han causado importantes daños económicos, disrupciones en las sociedades y tensiones entre los Estados. En el informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, todos los Estados reconocieron que las ciberoperaciones contra la infraestructura crítica corren el riesgo de tener “consecuencias humanitarias potencialmente devastadoras”[11]. Aunque el CICR no puede confirmar ninguna ciberoperación con bajas humanas, nos preocupan los efectos destructivos de las ciberoperaciones, como la disrupción del suministro eléctrico, de los sistemas de agua o de los servicios médicos[12]. Este tipo de operaciones suponen graves riesgos para los seres humanos en todo momento. Sin embargo, nuestra experiencia demuestra que la disrupción de las infraestructuras civiles críticas tiene consecuencias especialmente graves en las sociedades ya debilitadas por los conflictos armados.

Las consecuencias humanitarias adversas *no* son inevitables. Los Estados deben tomar medidas decisivas para garantizar que su uso de las ciberoperaciones durante los conflictos armados se ajuste a las normas vigentes del derecho internacional. En opinión del CICR, esto requiere una acción a nivel internacional y nacional.

A nivel internacional, los Estados han afirmado que el derecho internacional se aplica en el entorno de las TIC. Esto comprende, en primer lugar, las obligaciones de los Estados en virtud de la Carta de las Naciones Unidas, en particular la prohibición del uso de la fuerza y la obligación de resolver las controversias internacionales por medios pacíficos. Recientemente, el Grupo de Expertos Gubernamentales también observó que “el derecho internacional humanitario solo se aplica en situaciones de

[10] Grupo de Trabajo de Composición Abierta, Informe Final, 2021, párr. 16; Grupo de Expertos Gubernamentales, Informe Final, 2021, párr. 7.

[11] Grupo de Trabajo de Composición Abierta, Informe Final, 2021, párr. 18.

[12] Disponible en www.icrc.org/en/document/potential-human-cost-cyber-operations.

conflicto armado". El grupo recordó "los principios jurídicos internacionales establecidos, incluidos, en su caso, los principios de humanidad, necesidad, proporcionalidad y distinción que se señalaron en el informe de 2015", y reconoció "la necesidad de seguir estudiando cómo y cuándo se aplican estos principios al uso de las TIC por parte de los Estados y subrayó que recordar estos principios no legitima ni fomenta en absoluto los conflictos"[13]. El CICR apoya plenamente este punto de vista: las ciberoperaciones durante los conflictos armados no se producen en un "vacío legal" o en una "zona gris", sino que están sujetas a los principios y normas establecidos del derecho internacional humanitario.

Para garantizar que el derecho internacional humanitario se entienda y se aplique eficazmente, el CICR acoge con satisfacción que se siga estudiando cómo y cuándo se aplica este ámbito del derecho. Para evitar consecuencias humanitarias adversas y la disrupción de las sociedades, pedimos a los Estados que interpreten y apliquen las normas y los principios del derecho internacional humanitario de manera que se tengan en cuenta las características específicas del entorno de las TIC. Las cuestiones esenciales sobre la protección de la vida civil requieren un estudio más profundo y un posicionamiento claro por parte de los Estados. Por ejemplo, en un mundo cada vez más basado en los datos, debería ser una prioridad para los Estados acordar que los datos civiles disfruten de protección contra los ataques, al igual que los archivos civiles en papel. Además, los Estados deberían afirmar que las ciberoperaciones que dañan los bienes de carácter civil interrumpiendo su funcionamiento están sujetas a todas las normas del derecho internacional humanitario sobre las hostilidades[14].

Aunque es importante seguir estudiando y llegar a un acuerdo sobre el modo en que el derecho internacional limita las ciberoperaciones durante los conflictos armados, estas normas solo se harán efectivas mediante su aplicación a nivel nacional. A partir de las discusiones con operadores militares y expertos, el CICR identificó una serie de pasos clave sobre cómo los Estados pueden, y deben, evitar los daños a los civiles de las operaciones militares durante los conflictos armados[15]. Hoy, me gustaría destacar cuatro de ellos:

- En primer lugar, cada Estado es responsable de todos sus órganos implicados en ciberoperaciones y de otros actores que actúan bajo las instrucciones de ese Estado, o bajo su dirección o control. Los Estados deben garantizar que todos estos actores respeten el derecho internacional humanitario.
- En segundo lugar, los Estados deben desarrollar procesos internos claros para garantizar que, si se utilizan medios o métodos de guerra relacionados con la cibernética, estos cumplan con el marco legal aplicable.
- En tercer lugar, los Estados tienen la obligación de tomar todas las precauciones posibles para evitar, o al menos minimizar, los daños incidentales a la población civil cuando lleven a cabo ataques, incluso a través de medios y métodos de guerra relacionados con la informática. En el entorno de las TIC, esto puede

[13] Grupo de Expertos Gubernamentales, Informe Final, 2021, párr. 71 f).

[14] Véase también Comité Internacional de la Cruz Roja (CICR), Derecho internacional humanitario y ciberoperaciones durante conflictos armados: documento de posición del CICR, 2019.

[15] CICR, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

incluir la aplicación de medidas técnicas como el “bloqueo del sistema”, el “bloqueo geográfico” o los “interruptores de seguridad”[16].

- En cuarto lugar, los Estados también tienen la obligación de establecer medidas para proteger a la población civil contra los peligros derivados de las ciberoperaciones militares. Es posible que algunas de estas medidas deban aplicarse ya en tiempos de paz.

Para concluir, el CICR elogia a los Estados Miembros por esforzarse en hacer avanzar el diálogo internacional y el acuerdo sobre el costo humano potencial de las ciberoperaciones y las medidas para prevenir y mitigar los daños humanos. En nuestra opinión, el derecho internacional humanitario debe formar parte de esos debates, y el CICR sigue estando disponible para prestar su experiencia en ellos.

[16] “Bloqueo del sistema” significa impedir que el programa malicioso se ejecute por sí mismo a menos que haya una coincidencia precisa con el sistema de destino, “bloqueo geográfico” significa limitar el programa malicioso para que solo opere en un rango de IP específico, e “interruptores de seguridad” significa una forma de desactivar el programa malicioso después de un tiempo determinado o cuando se activa de forma remota.

Anexo XXXVII

Declaración del Director Ejecutivo para Servicios Policiales de la Organización Internacional de Policía Criminal (INTERPOL)

Introducción

La ciberdelincuencia es un desafío mundial en la era digital. Su impacto va mucho más allá de lo que se informa o detecta, afectando a la vida diaria de más de 4.500 millones de personas en línea. El reciente aumento de la dependencia del entorno digital ha creado más oportunidades delictivas en el ciberespacio. La ciberdelincuencia, que ha desplazado sus objetivos a los gobiernos, las empresas, las infraestructuras clave e incluso los hospitales, plantea hoy un formidable desafío a la seguridad en todo el mundo. Debido a su rápido crecimiento tanto en escala como en gravedad, la Organización Internacional de Policía Criminal (INTERPOL) ha dado prioridad a la lucha contra la ciberdelincuencia.

En su calidad de organización intergubernamental mundial y neutral, INTERPOL es consciente del derecho internacional, las normas, las medidas de fomento de la confianza y los esfuerzos de creación de capacidad para mantener la paz y la seguridad en el ciberespacio. A la luz del objetivo de este debate abierto para comprender mejor los crecientes riesgos derivados de las actividades maliciosas en el ciberespacio, INTERPOL presenta esta declaración escrita al Consejo de Seguridad para apoyar su compromiso de lograr un ciberespacio pacífico y seguro. En la declaración se exponen las últimas tendencias en materia de ciberdelincuencia y sus repercusiones, así como los mecanismos y soluciones mundiales de INTERPOL que están a disposición de sus 194 países miembros para hacer frente a estos apremiantes problemas.

Ciberamenazas actuales y emergentes

En el último año, INTERPOL ha analizado una amplia gama de ciberamenazas. Su reciente evaluación subrayó que la pandemia de enfermedad por coronavirus (COVID-19) ha abierto nuevos caminos para que los ciberdelincuentes lleven a cabo diversas formas de delincuencia en línea, independientemente de la región. Entre las amenazas más destacadas se encuentran la extorsión con programas maliciosos secuestradores, las estafas a empresas por correo electrónico mediante suplantación de identidad, las operaciones ilegales de recogida de datos, la información errónea y el resurgimiento de antiguos tipos de programas maliciosos, que se utilizaron para sacar provecho de la pandemia mundial.

Las tendencias detectadas también implican un cambio de objetivos hacia las grandes empresas, los gobiernos y la infraestructura crítica[17]. Los ciberdelincuentes y los estafadores se aprovechan de las necesidades y ansiedades sociales fundamentales. Desde marzo de 2020, INTERPOL ha recibido varias solicitudes de sus países miembros para hacer frente a los ataques de programas maliciosos secuestradores contra hospitales y otras instituciones que están en primera línea de la

[17] INTERPOL, informe de evaluación sobre los efectos de la COVID-19 en la ciberdelincuencia, recuperado de https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf.

lucha contra el coronavirus[18]. Al atacar estas infraestructuras críticas que desempeñan un papel crucial en la respuesta al brote, los delincuentes pudieron maximizar los daños y los beneficios económicos.

Aunque los ataques de programas maliciosos secuestradores no son nuevos, es la forma de ciberdelincuencia que más rápido crece. El programa malicioso secuestrador ofrece un modelo de negocio muy atractivo y lucrativo para los ciberdelincuentes, con el uso de la doble extorsión y el modelo de programa malicioso secuestrador como servicio. También observamos una pauta en la que dichos ataques no estaban limitados geográficamente, lo que sugiere que los delincuentes estaban ampliando su enfoque para atacar cualquier institución en todo el mundo. Por ejemplo, la misma cepa de programa malicioso secuestrador que cerró un hospital en Europa también se utilizó en Asia.

Además, hemos visto fraudes complejos que han afectado a víctimas de Europa y cuyo producto se ha dirigido hasta África Occidental y Asia Sudoriental en cuestión de horas. También siguen produciéndose violaciones masivas de datos que causan importantes pérdidas financieras a las empresas de todo el mundo. Al mismo tiempo, los ciberdelincuentes se esconden en la Internet oscura, que garantiza un acceso anónimo e imposible de rastrear. Esto acentúa la importancia y la pertinencia de las notificaciones de INTERPOL[19], en particular la notificación morada, que es un instrumento para que los países miembros intercambien información sobre el modus operandi de estas tramas fraudulentas. El objetivo es difundir esta información crítica más rápido que el próximo ataque.

Además, la convergencia entre la ciberdelincuencia y la delincuencia financiera está planteando un complejo desafío. Este tipo de delito contiene múltiples fases, desde el ciberataque hasta la explotación de los datos, pasando por las fases de blanqueo de dinero en capas y el eventual cobro. El uso de criptomonedas en este proceso también dificulta una respuesta eficaz y oportuna. Dada la complejidad, se requiere un modelo operativo conjunto que combine las capacidades de diferentes unidades especializadas en la aplicación de la ley para combatir mejor el fraude cibernético y el blanqueo de capitales. Para ofrecer toda la gama de apoyo operativo y analítico a este respecto, INTERPOL puso en marcha el Grupo Especial Mundial de INTERPOL de Lucha contra los Delitos Financieros a finales de 2020.

Mecanismo mundial para mitigar las ciberamenazas

De hecho, la cooperación policial internacional es vital para mantener la seguridad del mundo altamente interconectado. Como se reconoce en el estudio exhaustivo de la UNODC sobre el delito cibernético, INTERPOL desempeña un papel único a la hora de facilitar la cooperación entre policías[20]. En apoyo de los 194 países miembros, se le confía el mandato de facilitar la cooperación policial transfronteriza y, en su caso, apoyar a las organizaciones, autoridades y servicios gubernamentales e intergubernamentales cuya misión es prevenir o combatir la delincuencia, dentro de

[18] https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Los-ciberdelincuentes-secuestran-datos-de-las-instituciones-esenciales-de-atencion-medica.
[19] https://www.interpol.int/es/Como-trabajamos/Notificaciones/Acerca-de-las-notificaciones.
[20] Estudio exhaustivo de la UNODC sobre el delito cibernético, pág. 195.

los límites de las leyes existentes en los distintos países y en el espíritu de la Declaración Universal de Derechos Humanos.

Dada su neutralidad y su presencia mundial, INTERPOL se encuentra en una posición única para dirigir y coordinar la respuesta mundial de las fuerzas de seguridad a la ciberdelincuencia. También permite a las fuerzas de seguridad de todo el mundo compartir información sobre la ciberdelincuencia y los agentes que la amenazan, y ofrece una amplia gama de conocimientos, orientación técnica y apoyo operativo. Basándose en esta función única, INTERPOL defendió y subrayó la importancia de la cooperación policial internacional en varios procesos políticos de las Naciones Unidas, como el Grupo de Expertos de las Naciones Unidas encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético[21] y el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre Seguridad de las TIC.

Llevando la asociación al siguiente nivel, el 23 de noviembre de 2020 se aprobó por unanimidad la segunda revisión bianual de la resolución de la Asamblea General sobre la cooperación entre las Naciones Unidas e INTERPOL[22]. Fue un logro significativo, ya que introdujo un nuevo lenguaje en áreas clave de cooperación, incluida la ciberdelincuencia, proporcionando así una mayor legitimidad para una mayor colaboración entre las dos organizaciones en este campo.

En esta era de la digitalización, las soluciones nacionales e incluso las regionales ya no son suficientes. Para ayudar a conseguir la paz y la seguridad internacionales en el ciberespacio, INTERPOL puede servir de mecanismo mundial para combatir eficazmente la ciberdelincuencia y proporcionar a sus países miembros una serie de servicios y herramientas, entre las que se incluyen:

- Un sistema mundial de comunicaciones policiales seguras denominado I-24/7 para compartir información policial urgente de forma segura y en tiempo real;
- 19 bases de datos[23] y notificaciones[24] que son fundamentales para alertar a la comunidad internacional y apoyar las investigaciones transnacionales;
- El Programa Mundial de Ciberdelincuencia de INTERPOL proporciona capacidades policiales para prevenir, detectar, investigar y desbaratar la ciberdelincuencia, con el objetivo de reducir el impacto global de la ciberdelincuencia y proteger a las comunidades para lograr un mundo más seguro;
- El Grupo Mundial de Expertos en Ciberdelincuencia de INTERPOL y los Grupos de Trabajo Regionales con los Jefes de las Unidades de Ciberdelincuencia para debatir cuestiones urgentes relacionadas con la ciberdelincuencia y elaborar planes operativos y estratégicos;
- Plataformas de comunicación como Intercambio de Conocimientos sobre la Ciberdelincuencia para compartir información de forma segura dentro de la

[21] https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf y https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf.

[22] Resolución 75/10 de la Asamblea General, relativa a la cooperación entre las Naciones Unidas y la Organización Internacional de Policía Criminal (INTERPOL).

[23] https://www.interpol.int/es/Como-trabajamos/Bases-de-datos/Nuestras-19-bases-de-datos.

[24] https://www.interpol.int/es/Como-trabajamos/Notificaciones/Acerca-de-las-notificaciones.

comunidad policial en general y la Plataforma Colaborativa sobre Ciberdelincuencia-Operaciones para debates operativos cerrados;

- Plataforma de intercambio de información sobre la ciberdelincuencia para agregar datos de ciberdelincuencia y realizar análisis en profundidad;
- El punto de contacto de INTERPOL para la ciberdelincuencia 24/7 permite conectar en tiempo real a las unidades de ciberdelincuencia de distintos países para que cooperen con las fuerzas de seguridad;
- El marco de la Unidad Mundial de Respuesta a Ciberincidentes de INTERPOL (I-CIRT) para coordinar las respuestas mundiales de las fuerzas de seguridad a los principales ciberincidentes;
- Grupo Especial Mundial de INTERPOL de Lucha contra los Delitos Financieros para reducir el volumen y la repercusión de la delincuencia financiera en todo el mundo mediante la mejora de la cooperación y la innovación internacionales, centrándose en el ciberfraude y las tramas de blanqueo de capitales.

Un enfoque multipartito

Las investigaciones de ciberdelincuencia presentan una serie de desafíos que no se experimentan en el ámbito físico. Para las fuerzas de seguridad, es difícil saber de primera mano que se ha producido un ataque, e incluso entonces los índices de notificación son bajos. La investigación de la ciberdelincuencia también requiere conocimientos y tecnología específicos, que no están disponibles en todo el mundo. La ciberdelincuencia, al ser intrínsecamente global, suele ser perjudicial para una respuesta eficaz, ya que las pruebas y los sospechosos se encuentran en múltiples jurisdicciones simultáneamente.

Para superar estos desafíos, INTERPOL ha situado la colaboración en el centro de sus esfuerzos para hacer frente a la ciberdelincuencia. En la 88ª reunión de la Asamblea General de INTERPOL, celebrada en 2019, los países miembros han aprobado un marco jurídico denominado “Gateway” que permite a INTERPOL compartir información con empresas del sector privado[25]. Esta decisión se basó en el hecho de que las fuerzas de seguridad deben colaborar estrechamente con el sector privado, en el que se encuentra la mayor parte de los datos y los conocimientos especializados en relación con la ciberdelincuencia.

El Programa Mundial contra la Ciberdelincuencia de INTERPOL cuenta actualmente con 12 socios privados en este marco que comparten información y conocimientos especializados actualizados sobre la ciberdelincuencia, además de proporcionar asistencia técnica a los organismos encargados de la aplicación de la ley. El acceso a los datos, tanto del sector público como del privado, permite a INTERPOL proporcionar a los países miembros un apoyo operativo y una orientación técnica adaptados.

Además, la colaboración con diversos actores del ecosistema global de la ciberseguridad es crucial, ya que los diversos conjuntos de datos pueden ayudar a configurar políticas eficaces y respuestas operativas a la ciberdelincuencia. Esto

[25] https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/La-Asamblea-General-de-INTERPOL-traza-una-hoja-de-ruta-para-la-labor-policial-mundial.

también ayuda a poner en común nuestra sabiduría para ser resilientes y ágiles, especialmente en tiempos de incertidumbre. A finales del año pasado, INTERPOL apoyó a la policía nigeriana, junto con su socio privado, en la detención de miembros de un grupo de delincuencia organizada responsable de campañas de *phishing* y de estafas por correo electrónico que afectan a gobiernos y empresas del sector privado en más de 150 países[26].

INTERPOL también hace especial hincapié en la prevención. Para prevenir la ciberdelincuencia, INTERPOL colabora estrechamente con sus asociados públicos y privados para promover una buena ciberhigiene mediante una serie de campañas de concienciación a escala mundial. Estos esfuerzos también apoyan a las organizaciones encargadas de la aplicación de la ley para que superen los numerosos desafíos que plantea la lucha contra la ciberdelincuencia, concienciando a la población sobre el propio delito, las formas de protegerse y lo que hay que hacer cuando se produce.

Conclusión

Dado que el nexo de los actores criminales, la infraestructura y las víctimas va más allá de las fronteras y jurisdicciones nacionales, las fuerzas locales de seguridad no siempre tienen las capacidades o los medios para abordar estos elementos transitorios en la lucha contra la ciberdelincuencia. Los países miembros deben tener en cuenta que las brechas en las cibercapacidades de las fuerzas de seguridad en las distintas regiones siguen siendo un factor fundamental para que las redes delictivas distribuyan sus infraestructuras y actividades allí donde el riesgo es menor.

Para mitigar estas amenazas y riesgos en constante evolución relacionados con el ciberespacio, los países miembros deben aprovechar y maximizar el uso de la cooperación policial para dar una respuesta oportuna y eficaz. Gracias a su huella local en cada país, INTERPOL es capaz de atar cabos; identificar y desbaratar a los actores criminales en el ciberespacio, junto con nuestros países miembros y asociados.

Es evidente que la ciberdelincuencia solo puede combatirse eficazmente mediante una respuesta coordinada a nivel mundial y, sobre todo, rápida. Tenemos que proteger los sistemas, preparar a nuestros dirigentes, compartir soluciones y fomentar la respuesta adecuada. En particular, los organismos encargados de la aplicación de la ley deben ser un asociado confiable y eficaz, ya que el intercambio de datos es fundamental, incluso entre las fuerzas policiales nacionales, el sector privado y los expertos mundiales como INTERPOL. Aumentar la confianza dentro de la comunidad mundial de las fuerzas del orden con la actitud de “atreverse a compartir” es crucial en el marco del objetivo común de la lucha contra la ciberdelincuencia.

En un momento en que la comunidad internacional está sometida a una presión excepcional, garantizar nuestra seguridad común requiere que avancemos hacia una mayor colaboración e inclusión. Esto es lo que representa INTERPOL: ayudar a la cooperación internacional en materia de aplicación de la ley para un mundo más seguro. Como compartimos la convicción de que la seguridad y la justicia son

[26] https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Tres-personas-detenidas-a-raiz-de-una-investigacion-en-la-que-INTERPOL-Group-IB-y-las-Fuerzas-Policiales-de-Nigeria-desmantelan-un-prolifico-grupo.

fundamentales para lograr un ciberespacio pacífico y sostenible, INTERPOL trabaja al lado de las Naciones Unidas facilitando la cooperación internacional en materia de aplicación de la ley. Para que este esfuerzo sea un éxito, INTERPOL seguirá apoyando a sus países miembros en la lucha contra la ciberdelincuencia.

Anexo XXXVIII

Declaración del Representante Permanente de la República Islámica de Irán ante las Naciones Unidas, Majid Takht Ravanchi

El ciberespacio ofrece oportunidades excepcionales para que la humanidad desarrolle y promueva constantemente todos los aspectos de su vida. Por lo tanto, no solo hay que promover este excelente instrumento en todo el mundo, especialmente en los países en desarrollo, sino también protegerlo contra todas las amenazas.

El ciberespacio también puede utilizarse para cometer actos de agresión, quebrantamientos de la paz, "la amenaza o el uso de la fuerza", "para intervenir en asuntos que son esencialmente de la jurisdicción interna de cualquier Estado", para violar la soberanía de los Estados o para coaccionar a otros Estados. También deben prevenirse de forma eficaz.

Como principio rector, los principios y normas de derecho internacional "aplicables" existentes, por supuesto sin interpretaciones erróneas ni arbitrarias, deben regir los derechos, deberes y comportamientos de los Estados en relación con el ciberespacio.

Sin embargo, cuando no hay consenso sobre la aplicabilidad del derecho internacional, o incluso cuando no hay normas internacionales relacionadas con el ciberespacio, la comunidad internacional debe trabajar para desarrollar las normas necesarias.

Para ello, y dado que la Asamblea General tiene el mandato de la Carta para el "desarrollo progresivo del derecho internacional y su codificación", la Asamblea debe continuar sus esfuerzos en curso para desarrollar y codificar los principios y normas internacionales necesarios para el ciberespacio, incluso en forma de un instrumento internacional jurídicamente vinculante.

Paralelamente a estos esfuerzos, los Estados deben hacer todo lo posible para promover el uso más amplio posible del ciberespacio para su desarrollo y, al hacerlo, actuar de forma responsable y de acuerdo con el derecho internacional aplicable, en particular los Propósitos y Principios de las Naciones Unidas.

La responsabilidad principal de mantener un ciberespacio seguro y confiable recae en cada uno de los Estados. Por lo tanto, dada la compleja situación actual de la gobernanza del ciberespacio, debe promoverse y garantizarse el papel destacado y la participación seria de los Estados en la gobernanza del entorno del ciberespacio a nivel mundial, en particular en la política y la toma de decisiones.

Al mismo tiempo, la gobernanza del ciberespacio prevista debe desarrollarse de manera que no afecte negativamente a los derechos de los Estados a la hora de tomar sus decisiones de desarrollo, gobernanza y legislación con respecto al entorno del ciberespacio.

El derecho de los Estados a tener "libre acceso a la información y a desarrollar plenamente, sin injerencias, su sistema de información y sus medios masivos de comunicación y a utilizar sus medios de información para promover sus intereses y aspiraciones políticas, sociales, económicas y culturales", así como "el derecho y el

deber de los Estados de combatir, dentro de sus prerrogativas constitucionales, la difusión de noticias falsas o distorsionadas", que también ha sido reafirmado por la Asamblea General en la "Declaración sobre la Inadmisibilidad de la Intervención y la Injerencia en los Asuntos Internos de los Estados" de 1981, deben ser plenamente respetados.

En el cumplimiento de sus responsabilidades para mantener un ciberespacio seguro y confiable, los Estados deben adoptar un enfoque de cooperación y no de confrontación.

Como reafirmó la Asamblea General en la "Declaración sobre la Inadmisibilidad de la Intervención en los Asuntos Internos de los Estados y Protección de su Independencia y Soberanía" de 1965, "ningún Estado tiene derecho de intervenir directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro". Por lo tanto, todos los Estados deben prevenir y abstenerse de cometer tales actos, entre otros, contra los elementos políticos, económicos y culturales o la infraestructura crítica ciberrelacionada de los Estados, incluso a través de formas y medios ciberrelacionados.

Además, la Asamblea, a través de la "Declaración sobre la Inadmisibilidad de la Intervención y la Injerencia en los Asuntos Internos de los Estados" de 1981, ha reafirmado el deber de un Estado de "velar por que su territorio no sea utilizado de ninguna manera que atente contra la soberanía, la independencia política, la integridad territorial y la unidad nacional o perturbe la estabilidad política, económica y social de otro Estado"; "abstenerse de toda acción o tentativa, en cualquier forma o bajo cualquier pretexto, de desestabilizar o socavar la estabilidad de otro Estado o de cualquiera de sus instituciones", así como "abstenerse de toda campaña de difamación, vilipendio o propaganda hostil que tenga por fin intervenir o injerirse en los asuntos internos de otros Estados". Estas normas también deben ser observadas por los Estados con respecto al ciberespacio.

Según uno de los principios reafirmados por la Asamblea General en la "Declaración sobre los Principios de Derecho Internacional referentes a las Relaciones de Amistad y a la Cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas" de 1970, los Estados no deben utilizar ningún "tipo de medidas para coaccionar a otro Estado con el fin de obtener de él la subordinación del ejercicio de sus derechos soberanos y de obtener de él ventajas de cualquier tipo". Asimismo, los Estados no utilizarán los adelantos relacionados con el ciberespacio como instrumentos para adoptar medidas coercitivas económicas, políticas o de cualquier otro tipo, incluidas medidas de restricción o bloqueo contra otros Estados.

Además, los Estados deben abstenerse de utilizar la amenaza o el uso de la fuerza en o a través del entorno del ciberespacio. También deben abstenerse de aprovechar las cadenas de suministro relacionadas con el ciberespacio, desarrolladas bajo su control y jurisdicción para crear o ayudar al desarrollo de vulnerabilidades en los productos, servicios y mantenimiento que puedan comprometer la soberanía y la protección de datos de otros Estados, y deben evitar que eso ocurra.

Los Estados también deben ejercer el debido control sobre las empresas y plataformas relacionadas con el ciberespacio que se encuentran bajo su jurisdicción, y adoptar las medidas adecuadas para que rindan cuentas por su comportamiento en el entorno de las TIC, incluso por violar la soberanía nacional, la seguridad y el orden

público de otros Estados. En cualquier caso, los Estados son responsables de sus actos internacionalmente ilícitos dentro o a través del ciberespacio.

Además, todas las disputas internacionales relacionadas con el ciberespacio deben resolverse exclusivamente por medios pacíficos y sobre la base de “la igualdad soberana de los Estados y de acuerdo con el principio de libre elección de los medios”, tal y como se recoge en la “Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales” de 1970.

Cabe recordar en este contexto que, durante los últimos años, hemos asistido a una tendencia alarmante de acusaciones sistemáticas por parte de ciertos Estados contra otros Estados de lanzar ciberataques o actividades similares en el ciberespacio. Dados los desafíos existentes asociados a la atribución en el entorno del ciberespacio, así como la ausencia de un conjunto de normas desarrolladas y acordadas internacionalmente sobre pruebas genuinas, confiables y adecuadas para fundamentar la atribución, tales acusaciones deben considerarse meramente motivadas políticamente.

En definitiva, el ciberespacio y sus medios, técnicas y tecnologías conexas deben utilizarse exclusivamente con fines pacíficos y, para ello, los Estados deben actuar de forma cooperativa, responsable y en plena conformidad con el derecho internacional aplicable.

Por último, compartimos la opinión de que el examen de las cuestiones relacionadas con el ciberespacio debe continuar en la Asamblea General. Por su parte, la República Islámica del Irán, como una de las víctimas de ciberataques, a través del gusano informático malicioso Stuxnet (que se cree que fue construido conjuntamente por los Estados Unidos y el régimen israelí para causar daños a las instalaciones nucleares pacíficas iraníes) está dispuesta a contribuir a los esfuerzos de la Asamblea en el desarrollo de los principios y normas necesarios para el ciberespacio.

Anexo XXXIX

Declaración de la Misión Permanente de Italia ante las Naciones Unidas

Italia felicita a Estonia por llamar la atención del Consejo de Seguridad sobre la cuestión de la ciberseguridad y se complace en participar en el debate abierto de hoy.

También agradecemos el apoyo y la dedicación de la Alta Representante para Asuntos de Desarme, la Sra. Nakamitsu, y su disposición a informar al Consejo de Seguridad en un momento en que hay preocupación entre los Estados Miembros por el creciente número de incidentes de ciberseguridad.

Italia hace suya la declaración de la Unión Europea, y desea asimismo agregar los siguientes comentarios en nombre del país.

El momento de este debate no podía ser más oportuno. La Asamblea General ha reconocido el trabajo de los dos últimos años realizado por la Primera Comisión sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en materia de seguridad internacional y sobre el avance del comportamiento responsable de los Estados en el ciberespacio. Los dos informes adoptados por el Grupo de Trabajo de Composición Abierta y el Grupo de Expertos Gubernamentales durante este semestre representan importantes logros que deberían contribuir a fomentar la confianza entre los Estados Miembros. También han dado visibilidad a un ámbito que durante varios años se ha considerado eminentemente técnico.

El ritmo de la digitalización se está acelerando a nivel mundial y, junto con los beneficios asociados a este desarrollo, viene el reto de mantener el ciberespacio como un dominio mundial, abierto y estable. El aumento de los incidentes en los últimos meses, a veces dirigidos a la infraestructura crítica e imponiendo altos costos a las economías mundiales, es deplorable. Algunos de los ataques ofrecieron una visión de la pérdida de vidas humanas que pueden causar estas acciones, especialmente durante una pandemia. El potencial destructivo del uso indebido de las nuevas tecnologías es cada vez más evidente y también la necesidad de mantenerlas a raya. Italia cree que las Naciones Unidas son las mejor posicionadas para esta tarea y para promover la ciberpaz y la estabilidad.

Italia desea hacerse eco de la declaración de la Unión Europea en lo que respecta a la aplicabilidad del derecho internacional en el ciberespacio, incluidos el derecho internacional humanitario y el derecho de los derechos humanos, la importancia de adherirse a las normas de comportamiento responsable de los Estados y la utilidad de las medidas de fomento de la confianza como medio práctico para prevenir conflictos. También deseamos destacar el importante papel que las organizaciones regionales pueden ejercer en el ámbito de la ciberseguridad. Como partidarios incondicionales del multilateralismo, alentamos el diálogo entre las Naciones Unidas y las organizaciones regionales y, en este sentido, acogemos con satisfacción los recientes debates entre el Secretario General de las Naciones Unidas y el Consejo Europeo, como una valiosa oportunidad para intercambiar opiniones sobre los desafíos a los que nos enfrentamos. También apreciamos los esfuerzos de la presidencia sueca de la Organización para la Seguridad y la Cooperación en Europa, que está poniendo de relieve las interrelaciones entre los derechos humanos, las cuestiones de género y la ciberseguridad.

En un mundo cada vez más interconectado, el diálogo se hace aún más esencial para promover entendimientos compartidos y aumentar las oportunidades de cooperación. Con este espíritu, apoyamos el diálogo de la Unión Europea con las Naciones Unidas y con las organizaciones regionales, especialmente la Unión Africana, el Foro Regional de la Asociación de Naciones de Asia Sudoriental y la Oficina del Asesor Especial.

A través de las organizaciones regionales, los Estados Miembros pueden maximizar sus propios contactos bilaterales, compartiendo las mejores prácticas y las lecciones aprendidas, garantizando así que los enfoques regionales no sean divergentes. Deberían dedicarse más esfuerzos a los mecanismos de arreglo pacífico de controversias, así como a las iniciativas para desarrollar la ciberdiplomacia y la cibermediación.

Creemos que el ciberdominio debe permanecer abierto, libre, seguro y estable, como medio para que los Estados apliquen políticas que permitan a las sociedades prosperar y garantizar el desarrollo sostenible para todos, contribuyendo a la consecución de los ODS. No se puede subestimar la importancia de la creación de capacidades, ya que garantiza una resistencia homogénea de los Estados, aumenta la conciencia y estimula el desarrollo de capacidades. Queda mucho por hacer en este sector, y creemos que el programa de acción para fomentar el comportamiento responsable de los Estados en el ciberespacio, promovido junto con otros 52 Estados Miembros, puede representar la plataforma prioritaria desde la que coordinar y promover este esfuerzo. Ya hemos manifestado nuestra disponibilidad para seguir intercambiando sobre esta iniciativa en el contexto de los debates de la Primera Comisión y deseamos reiterar hoy nuestra voluntad. El programa de acción también puede ser el foro en el que tome forma el enfoque multipartito y se desarrollen las asociaciones público-privadas.

La pandemia ha supuesto un dramático retroceso en 2020 y 2021. Nuestros esfuerzos conjuntos deben centrarse en relanzar el desarrollo sostenible y el ciberdominio es un ingrediente esencial para ello. Italia está trabajando para alcanzar este objetivo como miembro del G7 y está promoviendo esta visión en el contexto de su actual presidencia del G20. El debate de hoy es un paso fundamental para aumentar la conciencia y garantizar que los avances relacionados con la digitalización se produzcan en un ciberdominio seguro y estable, salvaguardando al mismo tiempo todos los esfuerzos para que no se vean perjudicados.

Este debate tiene lugar mientras los ministros de Asuntos Exteriores del G20 se reúnen en Matera para debatir los temas de la recuperación y el desarrollo sostenible, con el objetivo de no dejar a nadie atrás. Esperamos que estos esfuerzos se refuercen mutuamente y que el Consejo de Seguridad siga centrándose en las cuestiones cibernéticas, supervise los avances y esté preparado para exhortar a los Estados incumplidores a cumplir con sus obligaciones. Esperemos que estos casos sean muy pocos, ya que los Estados Miembros convergen en la necesidad de dedicar tiempo y esfuerzo a una agenda positiva de ciberseguridad, que desarrolle la confianza, la transparencia y la inclusión.

Anexo XL

Declaración del Embajador para Asuntos de las Naciones Unidas y Política Cibernética del Ministerio de Asuntos Exteriores del Japón, Akahori Takeshi

El Japón desea expresar su sincero agradecimiento a Kaja Kallas, Primera Ministra de la República de Estonia, por haber organizado este debate abierto sobre la Ciberseguridad. El Japón agradece a Estonia que reconozca en su nota conceptual el debate abierto sobre los complejos desafíos contemporáneos para la paz y la seguridad internacionales organizado en 2017 bajo la presidencia del Japón.

El Japón se congratula de la adopción del informe del Grupo de Trabajo de Composición Abierta en marzo y de la adopción del informe del sexto Grupo de Expertos Gubernamentales en mayo, ambos por consenso.

El mayor valor del informe del Grupo de Trabajo de Composición Abierta fue que se adoptó por consenso en un proceso en el que todos los Estados Miembros pudieron participar plenamente. Los Estados Miembros afirmaron directamente el acervo, e incluyeron que el derecho internacional, en particular la Carta de las Naciones Unidas en su totalidad, es aplicable en el ciberespacio.

El informe del Grupo de Expertos Gubernamentales tiene un valor adicional. Para cada una de las 11 normas incluidas en el informe del Grupo de Expertos Gubernamentales de 2015, el nuevo informe proporciona orientación y ejemplos de aplicación. El Japón espera que este contenido fomente aún más la cooperación entre los Estados para promover un comportamiento responsable de los Estados. Además, ahora está más claro que los hechos internacionalmente ilícitos atribuibles a un Estado implican la responsabilidad de dicho Estado. La aplicabilidad del derecho internacional humanitario se expresa de forma clara. El Grupo volvió a señalar el derecho inherente de los Estados a tomar medidas, que se reconoce en la Carta.

Esperamos profundizar en los debates concretos sobre la aplicación del derecho internacional en el ciberespacio en diversos foros en el futuro. El Japón espera que el documento de posición que proporcionó al compendio de posiciones nacionales del Grupo de Expertos Gubernamentales contribuya a estos debates. Aquí me gustaría compartir los puntos más esenciales de la posición del Japón.

El Japón considera que un Estado no debe violar la soberanía de otro mediante ciberoperaciones. Asimismo, un Estado no debe intervenir en asuntos dentro de la jurisdicción interna de otro Estado mediante ciberoperaciones. Los hechos internacionalmente ilícitos cometidos por un estado en el ciberespacio conllevan la responsabilidad del Estado.

Los Estados tienen una obligación de diligencia debida respecto de las ciberoperaciones conforme al derecho internacional. Las Normas 13 c) y f) y la segunda oración del párrafo 71 g) del informe del Grupo de Expertos Gubernamentales de 2021 se relacionan con esta obligación. En relación con el reciente incidente de Colonial Pipeline, el Presidente de los Estados Unidos mencionó los esfuerzos llevados a cabo para lograr “una especie de norma internacional para que los gobiernos que sepan que se están produciendo actividades delictivas desde su territorio actúen sobre esas empresas delictivas”. Reconocemos la dificultad de

atribuir las ciberoperaciones a un Estado. La obligación de diligencia debida puede proporcionar las bases para invocar la responsabilidad del Estado del territorio en el que se originó una ciberoperación que no se atribuye a ningún Estado.

Cualquier disputa internacional que involucre ciberoperaciones debe resolverse mediante medios pacíficos conforme al Artículo 2 3) de la Carta de las Naciones Unidas. Para garantizar el arreglo pacífico de controversias, deben utilizarse las facultades del Consejo de Seguridad con base en los Capítulos VI y VII de la Carta de las Naciones Unidas y las funciones de los otros organismos de las Naciones Unidas en controversias que surgen de ciberoperaciones. El Japón tiene reservas ante la idea de establecer un nuevo mecanismo internacional de atribución.

La opinión del Japón es que, cuando una ciberoperación constituye un ataque armado conforme al Artículo 51 de la Carta de las Naciones Unidas, los Estados deben ejercer el derecho inmanente de legítima defensa, individual o colectiva, reconocido en el mismo artículo.

El derecho internacional humanitario también se aplica a las ciberoperaciones. Esta afirmación contribuye a la regulación de los métodos y medios de guerra. El argumento de que la afirmación conducirá a la militarización del ciberespacio carece de fundamento.

El derecho internacional de los derechos humanos también se aplica a las ciberoperaciones. Los individuos disfrutan de los mismos derechos humanos respecto de las ciberoperaciones que de otro modo disfrutan.

En cuanto a la relación entre el derecho internacional y las normas voluntarias, para la estabilización del ciberespacio es esencial que el derecho y las normas internacionales trabajen juntos para prevenir los actos ilícitos internacionales que utilizan las TIC y para promover el comportamiento responsable de los Estados en el ciberespacio. Como se expresa claramente en el informe del Grupo de Trabajo de Composición Abierta, las normas no sustituyen ni alteran las obligaciones de los Estados en virtud del derecho internacional.

El Japón espera que un gran número de Estados Miembros publique voluntariamente sus posiciones nacionales sobre la aplicación del derecho internacional.

El Japón cree que ha llegado el momento de dar prioridad a la aplicación de las normas y obligaciones voluntarias acordadas en virtud del derecho internacional, junto con las medidas de fomento de la confianza y las medidas de creación de capacidad.

En el contexto de la aplicación, el Japón desea invitar a los gobiernos a que anuncien de forma proactiva su evaluación jurídica cuando se produzca una ciberoperación maliciosa, incluso, entre otras cosas, si constituye una violación del derecho internacional. Esta práctica fomentará la comprensión compartida de cómo se aplica el derecho internacional a las ciberoperaciones. La aplicación del derecho internacional por parte de los tribunales internacionales y nacionales a los ciberincidentes tendría un efecto similar. El Japón espera que las actividades maliciosas en el ciberespacio se vean disuadidas por la acumulación de estas prácticas.

El Japón apoya firmemente el programa de acción. Creemos que el programa de acción será un mecanismo eficaz para garantizar y supervisar la aplicación de las normas acordadas, las obligaciones en virtud del derecho internacional, las medidas de fomento de la confianza y la creación de capacidades. Esperamos profundizar en los debates sobre el programa de acción. También seguiremos participando de forma proactiva en el nuevo Grupo de Trabajo de Composición Abierta.

El Japón se compromete a salvaguardar un ciberespacio libre, justo y seguro, y seguirá contribuyendo activamente a los debates y esfuerzos para promover el Estado de Derecho en el ciberespacio, incluso en las Naciones Unidas.

Anexo XLI

Declaración del Representante Permanente de Kazajstán ante las Naciones Unidas, Magzhan Ilyassov

Expresamos nuestra gratitud a la Presidencia estonia por haber organizado y dirigido el debate titulado “Mantenimiento de la paz y la seguridad internacionales: ciberseguridad”.

En condiciones de amenazas globales, garantizar la seguridad requiere la coordinación de la comunidad internacional y la resolución de muchos aspectos de naturaleza política y económica. En este contexto, cabe señalar que ha aparecido un nuevo y a la vez complicado componente en el mundo: la ciberseguridad.

Debe quedar claro que las tecnologías de la información y las comunicaciones tienen un enorme potencial para el desarrollo de los Estados. Al mismo tiempo, crean nuevas oportunidades para los delincuentes y pueden contribuir a un aumento de los niveles y la complejidad de la delincuencia, el riesgo potencial del uso indebido de las tecnologías emergentes, incluida la inteligencia artificial. En este sentido, la prevención y supresión del uso de las tecnologías de la información y las comunicaciones con fines delictivos debería ser una prioridad en la labor de los Estados en la etapa actual.

A este respecto, acogemos un comité intergubernamental de expertos ad hoc de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, teniendo plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional para combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, prevista en la resolución 74/247, aprobada por la Asamblea General el 27 de diciembre de 2019.

Creemos que la labor de las Naciones Unidas en este ámbito se verá aún más influenciada por el informe sustantivo final del Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, adoptado en marzo de 2021 y consensuado por la resolución 75/240, que estableció un Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), así como por el informe consensuado adoptado por el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el contexto de la seguridad internacional en mayo de 2021.

Los Estados deben seguir reforzando las medidas para proteger toda la infraestructura crítica frente a las amenazas de las TIC y aumentar los intercambios de buenas prácticas al respecto.

En este sentido, acogemos con satisfacción el proceso de negociación sobre ciberseguridad en las Naciones Unidas y la comprensión de los participantes y los Estados Miembros de que todas las decisiones sobre esta agenda específica deben tomarse por consenso.

Anexo XLII

Declaración de la Misión Permanente de Letonia ante las Naciones Unidas

Los avances en las tecnologías de la información y las comunicaciones (TIC) han proporcionado a los Estados y a las sociedades innumerables beneficios en el ámbito de la economía, los servicios, la educación y la comunicación. Junto a los efectos enormemente positivos de la aplicación de las TIC, Letonia está cada vez más preocupada por las implicaciones del uso malicioso y disruptivo de las TIC, con las consecuencias que ello conlleva tanto para la paz, la seguridad y la estabilidad internacionales como para los derechos humanos.

Los Estados sufren con mayor frecuencia este tipo de delitos, incluidos los que afectan a las instituciones democráticas y a la infraestructura crítica. Es aún más alarmante que las ciberactividades maliciosas estén aprovechando la pandemia del coronavirus para atacar los sistemas de atención médica esenciales para el mantenimiento de la salud humana, la investigación de vacunas, así como el espacio de información.

La amplia participación y el propio debate desplegado en la reunión con arreglo a la fórmula Arria del Consejo de Seguridad de las Naciones Unidas el año pasado confirmaron la creciente relevancia de la ciberseguridad para la agenda de paz y estabilidad internacional. Por lo tanto, es oportuno y apropiado incluir la cuestión de la ciberseguridad en el programa oficial del Consejo de Seguridad. Letonia apoya plenamente los esfuerzos de Estonia por reflexionar adecuadamente sobre la mitigación del comportamiento irresponsable en el ciberespacio sobre la paz y la seguridad internacionales.

Las Naciones Unidas deben seguir siendo un protagonista mundial significativo para promover la paz, la seguridad y la estabilidad, incluso en el ciberespacio. La labor activa del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Comunicaciones en el Contexto de la Seguridad Internacional en los últimos años ha dado bases sustanciales para el debate de hoy.

Los dos informes finales, basados en el consenso, del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta son un buen trampolín para seguir trabajando con vistas a forjar un entendimiento común sobre una amplia gama de cuestiones.

En este sentido, el programa de acción sobre el uso responsable de las TIC por parte de los Estados en el contexto de la seguridad internacional es un valioso resultado de los informes del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta. El programa de acción relacionado con la cibernética debe servir de base sólida y, sobre todo, orientada a la acción, para seguir trabajando con el fin de lograr avances tangibles en la aplicación de las normas de comportamiento responsable.

En este contexto, Letonia desea subrayar la naturaleza multipartita del ciberespacio, que requiere la participación en los debates de una serie de actores no estatales del sector privado, la sociedad civil y el mundo académico. Teniendo en cuenta su importancia en el ecosistema de las TIC, estas partes interesadas pueden contribuir significativamente de muchas maneras diferentes, compartiendo sus perspectivas, conocimientos y experiencia.

Los Estados deben seguir trabajando activamente y estar dispuestos a debatir en profundidad en el marco de los futuros procesos de las Naciones Unidas para avanzar en el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. Aunque todos tenemos que trabajar sin descanso para reforzar la protección y la seguridad de nuestras propias TIC, los Estados no deben permitir que otro Estado o agente no estatal utilice las TIC en su territorio para cometer hechos internacionalmente ilícitos. Exhortamos a todos los Estados para que se abstengan de llevar a cabo, permitir o tolerar este tipo de actividades que no se ajustan al derecho internacional, incluida la Carta de las Naciones Unidas, para evitar que se obstaculice la seguridad asociada al uso de las TIC. La responsabilidad, la creación de confianza y la previsibilidad deben ser los elementos clave de la cooperación internacional en el ámbito de la ciberseguridad.

Para evitar malentendidos y percepciones erróneas, por un lado, y para establecer una práctica de comunicación sobre incidentes relacionados con las TIC, por otro, debemos establecer canales de comunicación abiertos entre los Estados Miembros. La creación de una red de puntos de contacto a nivel político y técnico en las Naciones Unidas puede contribuir significativamente a una comunicación más eficaz a nivel mundial. La red de puntos de contacto ya ha demostrado su eficacia a nivel regional en la Organización para la Seguridad y la Cooperación en Europa.

Por último, Letonia desea elogiar a todos los Estados Miembros por demostrar su compromiso de cooperar y trabajar juntos para alcanzar un consenso sobre los informes en los procesos del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta. Este es el camino correcto y una excelente oportunidad para reforzar aún más la cooperación internacional hacia un ciberespacio mundial, abierto, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho.

Anexo XLIII

Declaración del Encargado de Negocios Interino y Representante Permanente Adjunto de Liechtenstein ante las Naciones Unidas, Georg Sparber

Las ciberoperaciones han servido de ecualizador en la guerra moderna al proporcionar nuevas vías para las operaciones ofensivas y defensivas a todos los actores, incluidos los que tienen menos recursos. Como resultado, la frecuencia y la gravedad de las ciberoperaciones se han intensificado en los últimos años, amenazando la paz y la seguridad internacionales. Es alarmante que estos ataques puedan causar graves sufrimientos a la población civil, incluso la pérdida de vidas y la disrupción de los servicios esenciales. En este contexto, recordamos que los Estados están cada vez más de acuerdo en que el derecho internacional, concretamente la Carta de las Naciones Unidas en su totalidad y las normas de derecho internacional consuetudinario derivadas de los principios de la Carta, así como el Estatuto de Roma de la Corte Penal Internacional y el derecho internacional humanitario, se aplican al ciberespacio.

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 institucionalizó los debates sobre la paz y la seguridad internacionales en el cibercontexto dentro de las Naciones Unidas. Por otra parte, el informe final publicado por el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (Grupo de Expertos Gubernamentales) reafirma la aplicabilidad y necesidad del derecho internacional en el ciberespacio. Liechtenstein toma nota de las contribuciones combinadas del Grupo de Trabajo de Composición Abierta y del Grupo de Expertos Gubernamentales para hacer avanzar el debate sobre cómo se aplica el derecho internacional, en particular la Carta de las Naciones Unidas, al ciberespacio.

Uno de los hitos que logró la Carta de las Naciones Unidas es la prohibición del uso de la fuerza. El uso de la fuerza está prohibido, excepto cuando lo autorice el Consejo de Seguridad en virtud del Capítulo VII o cuando se lleve a cabo en legítima defensa en virtud del artículo 51 de la Carta. Sin embargo, el artículo 51 se invoca cada vez más como base legal para el uso de la fuerza sin las justificaciones legales necesarias. Existe un riesgo importante de que esta tendencia se extienda al ciberespacio con el desarrollo de nuevas tecnologías y capacidades de los Estados. Debemos asegurarnos de que el ciberespacio no facilite operaciones de autodefensa injustificadas. Y, recordemos que invocar el artículo 51 de forma preventiva requiere la prueba de la inminencia de un ataque armado, y siempre requiere la prueba de la necesidad y la proporcionalidad de las medidas adoptadas en respuesta.

La Carta de las Naciones Unidas prevé que el Consejo de Seguridad desempeñe una función coercitiva en relación con las violaciones más graves de las normas pertinentes del derecho internacional que constituyan actos de agresión. Además de las herramientas contenidas en la Carta, el Consejo tiene ahora la opción de iniciar la responsabilidad penal individual de los autores del crimen de agresión remitiendo las situaciones pertinentes a la CPI. En este contexto, Liechtenstein cree que tener una

comprensión clara de cómo se aplica el Estatuto de Roma a las ciberoperaciones ayudará a informar el trabajo del Consejo.

En un esfuerzo por dilucidar la aplicación del Estatuto de Roma a las ciberoperaciones, Liechtenstein, junto con otros diez Estados parte de la CPI, creó un Consejo de Asesores para explorar el papel de la CPI en la regulación de la ciberguerra. Compuesto por 16 eminentes juristas internacionales, el Consejo de Asesores se reunió tres veces a lo largo de 2019 y 2020 para debatir en qué medida las disposiciones fundamentales del Estatuto de Roma se aplican a las ciberoperaciones. Está previsto presentar un informe final este año. Confiamos en que esto contribuya a la comprensión común de la responsabilidad en el contexto de las ciberoperaciones, así como a la disuasión de estos delitos en primer lugar.

Liechtenstein subraya la necesidad de tener un marco jurídico sólido que regule el ciberespacio para la paz y la seguridad internacionales. Nos complace contribuir a los esfuerzos mundiales para combatir las ciberoperaciones maliciosas a través de nuestro próximo informe centrado en el Estatuto de Roma, y seguiremos bregando por la paz y la seguridad internacionales con nuestro inquebrantable compromiso con el derecho internacional.

Anexo XLIV

Declaración de la Misión Permanente de Malta ante las Naciones Unidas

Malta agradece a Estonia la organización de este oportuno debate sobre una cuestión que, en nuestra opinión, debería figurar en el programa del Consejo de Seguridad. Aunque se ha aludido a las cuestiones de ciberseguridad en varios debates del Consejo de Seguridad, creemos que debería darse más importancia a estas cuestiones, teniendo en cuenta que representan uno de los desafíos más importantes y en constante evolución para la paz y la seguridad internacionales.

Malta se adhiere a la declaración presentada por la Unión Europea y desea destacar algunas observaciones a título nacional. La evolución del ciberespacio ha traído consigo una serie de oportunidades para los Estados Miembros y los ciudadanos de todo el mundo y ha propiciado un aumento de la prosperidad, la conectividad y el crecimiento económico. Sin embargo, el ciberdominio también ha abierto la puerta a actividades maliciosas destinadas a perturbar y explotar las vulnerabilidades de las sociedades y a realizar ataques que pueden tener un impacto considerable en los Estados Miembros y en sus ciudadanos, por ejemplo, en términos de datos sensibles y de la infraestructura crítica. De hecho, cuanto más nos desplazamos hacia el mundo virtual e interconectado, más susceptibles somos a este tipo de actividades malignas.

Malta cree que las Naciones Unidas tienen un papel central en la regulación del comportamiento de los Estados en el ciberespacio, concretamente por el amplio corpus de derecho internacional que ya existe. También nos sentimos muy alentados por los resultados obtenidos por el Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta de las Naciones Unidas (Grupo de Trabajo de Composición Abierta), que han adoptado informes aprobados por consenso sobre, entre otras cosas, el avance del comportamiento de los Estados en el ciberespacio. Necesitamos que estos procesos sigan alimentándose en el sistema de las Naciones Unidas y que se profundice en la aplicación del derecho internacional en el ciberespacio, en la importancia de las medidas de fomento de la confianza y en la oferta de orientaciones y normas adicionales. Valoramos la participación y la contribución de los Estados Miembros en estos procesos e instamos a que estos debates avancen y sigan el ritmo de los rápidos avances en este ámbito.

Hemos sido testigos del devastador impacto que pueden tener los ciberataques en los datos e infraestructuras sensibles. Es vital que las normas y regulaciones para el comportamiento del Estado en el ciberdominio estén bien perfiladas. Esto permitirá aumentar la previsibilidad y evitar cualquier error de cálculo al evaluar las ciberamenazas. El uso malicioso del ciberespacio tiene un impacto tan duradero que también es necesaria la cooperación a nivel internacional para evitar los posibles conflictos que puedan surgir.

Las medidas de fomento de la confianza entre los Estados mediante la aplicación de buenas prácticas y normas establecidas es un componente vital para avanzar. Esto reducirá los posibles malentendidos y permitirá evaluar mejor los comportamientos maliciosos.

La comunidad internacional también debe llegar a la miríada de otras partes interesadas en este asunto, incluida la sociedad civil y el sector privado, para

garantizar la igualdad de condiciones y un conjunto de normas equitativas. Todos los usuarios potenciales del ciberespacio deben reconocer el papel que desempeñan en el aumento de la ciberresiliencia y en la prevención del uso malicioso de las herramientas que tenemos a nuestra disposición.

Malta considera que el Consejo de Seguridad tiene un importante papel que desempeñar en lo que respecta a las nuevas tecnologías que pueden tener un impacto en la paz y la seguridad internacionales. El Consejo de Seguridad debe velar por que todos los actores relevantes del ciberespacio respeten el derecho internacional y las normas y directrices establecidas a fin de evitar posibles conflictos derivados de los ciberataques. Instamos al Consejo a que siga ocupándose de este asunto y a que se asegure de que fomentemos juntos una mayor comprensión y confianza mutua.

Anexo XLV

Declaración de la Misión Permanente de Marruecos ante las Naciones Unidas

[Original: francés]

El Reino de Marruecos expresa, en primer lugar, su agradecimiento a Estonia por haber organizado este primer debate abierto del Consejo de Seguridad dedicado a la cuestión, tan pertinente como oportuna, del mantenimiento de la paz y la seguridad internacionales en el ciberespacio. Marruecos alaba la intervención exhaustiva de la Sra. Kaja Kallas, Primera Ministra de la República de Estonia, así como el excelente liderazgo de Estonia en las cuestiones cibernéticas y de seguridad del ciberespacio. Marruecos agradece asimismo a la Alta Representante para Asuntos de Desarme, la Sra. Izumi Nakamitsu, su exposición informativa sobre los desafíos actuales para el mantenimiento de la paz y la seguridad internacionales en el ciberespacio.

Como país en desarrollo con una alta conexión, el Reino de Marruecos ha concedido desde el principio una importancia particular al desarrollo de las tecnologías de la información y las comunicaciones (TIC) y a sus ventajas como motores de desarrollo sostenible. Sin embargo, aunque existe unanimidad sobre los beneficios y las ventajas que aportan los avances de las TIC al bienestar cotidiano de la Humanidad, ha comenzado a instaurarse una conciencia mundial sobre las amenazas que pueden derivarse de ellas, que van desde la simple circulación de noticias falsas hasta verdaderas amenazas para la paz y la seguridad, tanto a nivel nacional como internacional.

En un momento en el que se habla de términos asumidos de la Internet de las cosas, de revolución digital o de ciberguerra, nuestra capacidad para luchar contra las amenazas cibernéticas se ha quedado corta con respecto a nuestra gran dependencia de estas herramientas indispensables. Además, es importante señalar que el contexto actual marcado por la pandemia de enfermedad por coronavirus (COVID-19) no solo nos ha propulsado más hacia la era cibernética sino que, en paralelo, nos ha expuesto a un nivel exponencial e irreversible de vulnerabilidad a ciberataques y amenazas, incluidas las que tienen como objetivo infraestructuras críticas.

Estas operaciones maliciosas, además de amenazar la soberanía de los Estados, lamentablemente pueden aumentar el riesgo de conflictos en el ciberespacio y causar considerables daños humanos y materiales, lo que puede minar la paz y la seguridad internacionales y erigir los ciberataques como una gran amenaza emergente.

Vivimos en una época peligrosa, como afirmó el Secretario General en la presentación de su Agenda para el Desarme en 2018.

En efecto, los riesgos potenciales y reales asociados a las amenazas en el ciberespacio reclaman la atención, ahora más que nunca, de la comunidad internacional y los Estados Miembros de las Naciones Unidas. Solo podremos garantizar que el ciberespacio siga sirviendo de motor de paz, seguridad, estabilidad y desarrollo esforzándonos, de manera colectiva e individual, por prevenir los usos maliciosos de las TIC.

A este respecto, Marruecos considera que la necesidad de asegurar y proteger el ciberespacio sigue siendo una responsabilidad compartida de los Estados, principales líderes. Por eso, Marruecos ha emprendido desde el primer momento, de conformidad con las Altas Directrices Reales, importantes acciones a nivel legislativo, organizativo y preventivo, entre ellas:

- La presentación detallada de una estrategia de ciberseguridad, basada en los cuatro ejes estratégicos de: evaluación de los riesgos para los sistemas de información en las administraciones, organismos públicos e infraestructuras críticas; protección y defensa de estos sistemas de información; refuerzo de las bases de la seguridad (marco jurídico, sensibilización, formación e investigación y desarrollo); y fomento y desarrollo de la cooperación nacional, regional e internacional;

- La promulgación, el 25 de julio de 2020, de la Ley núm. 05-20 sobre Ciberseguridad, que tiene por objeto establecer un marco jurídico que recomiende a las entidades un conjunto mínimo de normas y medidas de seguridad para garantizar la fiabilidad y resiliencia de sus sistemas de información. También tiene como objetivo el desarrollo de la confianza digital, la digitalización de la economía y, en general, la garantía de la continuidad de las actividades económicas y sociales de Marruecos, con el fin de favorecer el desarrollo de un ecosistema nacional de ciberseguridad;

- La creación, a lo largo de este decenio, de varias organizaciones destinadas a garantizar la gobernanza estatal de la ciberseguridad, como el Comité Estratégico de Seguridad de los Sistemas de Información en 2011, la Dirección General de Seguridad de los Sistemas de Información, la Agencia Nacional de Reglamentación de las Telecomunicaciones, la Comisión Nacional de Control de la Protección de Datos Personales o el Centro Marroquí de Investigaciones Politécnicas e Innovación que desarrolla la Campaña Nacional de Lucha contra la Ciberdelincuencia.

En vísperas de la celebración de este debate abierto, Marruecos también aprobó, el 28 de junio de 2021, un proyecto de decreto relacionado con la ciberseguridad que establece las normas aplicables en materia de seguridad de los sistemas de información, así como la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales.

Sin embargo, en vista de la naturaleza global de las amenazas cibernéticas, deben poder operar importantes medidas acordadas a nivel internacional que complementen las reglamentaciones establecidas a nivel nacional. Por ello, Marruecos ha ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, y en 2018 se sumó al Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio. Participa, en el marco de las Naciones Unidas, 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, en el Grupo de Expertos Gubernamentales para fomentar un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, en el nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) y en la elaboración del próximo programa de acción para la promoción de un comportamiento responsable de los Estados en el ciberespacio.

Marruecos también es miembro del Grupo de Amigos sobre Gobernanza Electrónica y Ciberseguridad que copreside Estonia, magníficamente, junto con Singapur.

Para concluir, el Reino de Marruecos subraya que es responsabilidad compartida de los Estados demostrar una voluntad común y firme de proteger el ciberespacio, principalmente porque los aspectos de prevención y seguridad del ciberespacio son corolarios del uso de las TIC.

En particular, el Consejo de Seguridad está llamado a desempeñar un papel fundamental, especialmente porque la perpetración de ciberataques constituye una amenaza directa para la paz y la seguridad internacionales, pero también pionero en materia de prevención.

Marruecos reitera su sincero agradecimiento a Estonia por haber organizado este debate abierto, necesario y oportuno, puesto que necesitamos una mayor sensibilización y debates sobre la cuestión del mantenimiento de la paz y la seguridad internacionales en el ciberespacio, y por haber introducido esta cuestión en la agenda del Consejo de Seguridad.

Anexo XLVI

Declaración de la Representante Permanente de los Países Bajos ante las Naciones Unidas, Yoka Brandt

El Reino de los Países Bajos desea agradecer a Estonia y a la Primera Ministra Kallas la organización de este debate abierto sobre el mantenimiento de la paz y la seguridad internacionales en el ciberespacio.

Es una reunión oportuna, dado el fuerte aumento de los ciberataques, tanto por parte de actores estatales como no estatales. Estas actividades cibernéticas maliciosas pueden conducir a una disrupción potencialmente enorme en nuestras sociedades, a través de recursos relativamente limitados, lo que trae aparejada la desestabilización de las relaciones internacionales.

Por lo tanto, ha llegado el momento de trabajar juntos para garantizar un ciberespacio abierto, libre y seguro, fomentando el comportamiento responsable de los Estados, denunciando los comportamientos irresponsables e imponiendo consecuencias.

Aunque reconocemos que hay muchos otros ángulos relevantes en esta cuestión, los Países Bajos se limitarán a tres elementos específicos que siguen siendo imprescindibles para aumentar la estabilidad en el ciberespacio:

- Adhesión al acervo
- Atribución
- Creación de capacidad

Adhesión al acervo

A lo largo de los años, las ciberoperaciones contra infraestructuras críticas y civiles han demostrado ser una amenaza real y creíble. Esto ha sido más evidente en el último año, en el que hemos sido testigos de la evolución de los ciberataques en cuanto a su alcance, escala, gravedad y sofisticación. Como sociedades, hemos trasladado cada vez más casi todos los aspectos de nuestra vida a un mundo digital y debemos darnos cuenta de que es Internet quien facilita estas conexiones en todo el mundo. Por lo tanto, no debería sorprender que los efectos nocivos de las ciberoperaciones maliciosas contra la infraestructura crítica, los gobiernos o las sociedades, se sientan de forma inmediata y generalizada. Esto supone un riesgo importante para la seguridad y la estabilidad internacionales, el desarrollo económico y social, así como para la seguridad y el bienestar de las personas.

Con el reciente consenso alcanzado en los informes del Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional y del Grupo de Expertos Gubernamentales de las Naciones Unidas para promover el comportamiento responsable de los Estados en el ciberespacio (Grupo de Expertos Gubernamentales), los Estados disponen ahora de un marco de comportamiento responsable de los Estados en el ciberespacio. Esto permite que los Estados comprendan mejor la aplicabilidad del derecho internacional y las 11 normas voluntarias no vinculantes acordadas. Los Países Bajos recuerdan que el derecho

internacional vigente, en particular la Carta de las Naciones Unidas, es aplicable al ciberespacio y es esencial para mantener la paz y la estabilidad y para promover un ciberespacio libre, abierto y seguro, que incluya el respeto de los derechos humanos y las libertades fundamentales en el ciberespacio.

Los Estados acordaron que las ciberoperaciones maliciosas contra las infraestructuras y las infraestructuras de información que apoyan los servicios esenciales de las infraestructuras públicas están prohibidas, confirma la norma 13(f) del Grupo de Expertos Gubernamentales. Es prerrogativa de cada Estado determinar qué infraestructuras designa como críticas y pueden incluir instalaciones médicas, servicios financieros, la energía, el agua, el transporte y el saneamiento. Los Países Bajos se han centrado sistemáticamente en tres infraestructuras (no exhaustivas):

- La infraestructura técnica esencial para la disponibilidad general o la integridad de Internet;
- La infraestructura técnica esencial para las elecciones;
- El sector de atención de la salud.

En este sentido, alentamos a los Estados a que definan y compartan públicamente lo que consideran infraestructura crítica mediante la emisión de declaraciones nacionales en las que se detallen las posiciones de los Estados Miembros sobre la adhesión al marco de comportamiento responsable del Estado. Solo así podremos aumentar la transparencia, desarrollar un entendimiento común, crear previsibilidad y generar confianza. Es necesario seguir trabajando en la aplicación del marco acordado para reducir el riesgo de escalada, así como la adhesión al acervo por parte de todos los Estados.

Atribución

Parece que todos estamos de acuerdo con las reglas y normas del ciberespacio. Sin embargo, seguimos asistiendo a un aumento de las ciberamenazas. Los Países Bajos están consternados por el abuso de la pandemia de enfermedad por coronavirus (COVID-19) para realizar ciberoperaciones maliciosas contra la infraestructura crítica; el sector de salud, la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet, así como la infraestructura técnica para las elecciones.

Seamos claros: trabajaremos juntos de forma voluntaria para que los Estados rindan cuentas cuando actúen en contra de este marco, incluso adoptando medidas transparentes y coherentes con el derecho internacional. Debe haber consecuencias para el mal comportamiento en el ciberespacio.

Creación de capacidad

La resiliencia digital es clave para gestionar los ciberriesgos y mitigar su impacto. Sin embargo, los diferentes niveles de capacidad de ciberseguridad entre los distintos Estados amplían la vulnerabilidad de nuestro mundo interconectado. Por lo tanto, nuestro interés común es comprometernos en los esfuerzos de creación de capacidades específicas para garantizar que todos los Estados responsables puedan aplicar este marco y proteger mejor sus redes de actividades cibernéticas significativas que perturben, destruyan o desestabilicen. Además, la creación efectiva

de cibercapacidades requiere la cooperación entre actores estatales y no estatales. En este sentido, los Países Bajos crearon el Foro Mundial de Competencia Cibernética, que ha madurado hasta convertirse en una sólida plataforma de creación de capacidades público-privadas que aprovecha y consolida los más de 700 esfuerzos existentes en materia de creación de cibercapacidades, proporcionando asistencia en la creación de resiliencia técnica y ayuda en la redacción de legislación que garantice la seguridad y el respeto de los derechos humanos.

Elogiamos a Estonia por sentar las bases para futuros debates sobre ciberseguridad en el Consejo de Seguridad y acogemos con satisfacción el primer debate oficial de hoy sobre ciberseguridad.

Anexo XLVII

Declaración de la Misión Permanente de Nueva Zelandia ante las Naciones Unidas

Nueva Zelandia desea señalar nuestro agradecimiento a Estonia por haber introducido en el orden del día del Consejo de Seguridad la importante cuestión del mantenimiento de la paz y la seguridad internacionales en el ciberespacio.

Las ciberamenazas son un problema acuciante y generalizado para todos los Estados Miembros. Las amenazas cibernéticas plantean riesgos importantes para la prosperidad y la seguridad de Nueva Zelandia, así como para la paz y la seguridad internacionales.

Debemos trabajar juntos para construir un entorno en línea estable y seguro para que todos podamos disfrutar de los beneficios de la conectividad digital, que es un importante factor de desarrollo económico, social y cultural.

Valoramos la oportunidad de compartir las perspectivas de Nueva Zelandia sobre los esfuerzos internacionales para mantener la paz y la seguridad en el ciberespacio. Para ello, reiteramos la importancia crítica del marco acordado de comportamiento responsable de los Estados en línea:

- Debemos cumplir nuestras obligaciones en virtud del derecho internacional vigente, que todos hemos acordado que se aplica tanto en línea como fuera de ella;
- Debemos aplicar las normas de comportamiento responsable del Estado en línea, que cada uno de nosotros ha refrendado mediante la resolución 70/237 de la Asamblea General;
- Debemos garantizar que las Medidas de Fomento de la Confianza se adopten y utilicen ampliamente; y
- Debemos redoblar nuestros esfuerzos de capacitación para garantizar que todos seamos ciberresilientes.

Este marco proporciona lo que necesitamos para fomentar un comportamiento responsable en línea, pero es necesario vivirlo para que sea eficaz. Tenemos que seguir aplicando el marco de forma práctica, significativa y concreta. Nueva Zelandia se compromete a seguir trabajando con todos ustedes en este sentido.

Derecho internacional

Como Estado pequeño, Nueva Zelandia defiende con firmeza el sistema internacional basado en normas. Esto se cumple en particular con respecto a las amenazas transfronterizas. Nuestro aislamiento geográfico no nos protege de las ciberamenazas.

Garantizar que este sistema promueva un entorno en línea abierto, seguro, estable, accesible y pacífico y que fomente un comportamiento responsable de los Estados en el ciberespacio es una prioridad clave de Nueva Zelandia.

Llegar a un consenso sobre la forma precisa en que se aplica el derecho internacional en línea es una contribución crucial para el mantenimiento de la paz y

la estabilidad. Todos estamos de acuerdo en que el derecho internacional se aplica tanto en línea como fuera de línea. El derecho internacional aplicable incluye: la Carta de las Naciones Unidas; el derecho de la responsabilidad del Estado; derecho internacional humanitario; y el derecho internacional de los derechos humanos.

Sin embargo, reconocemos que siguen existiendo algunas diferencias sobre estos temas. Para apoyar la comprensión de cómo se aplica el derecho internacional en línea, en diciembre de 2020, Nueva Zelandia publicó una declaración de posición nacional. Animamos a los demás Estados Miembros a que compartan sus perspectivas nacionales para desarrollar y mejorar nuestro entendimiento común sobre estas cuestiones.

Normas de comportamiento responsable de los Estados

Nueva Zelandia se compromete a prevenir, detectar, disuadir y responder a la ciberactividad maliciosa, y a defender las normas de comportamiento responsable de los Estados, tal y como se indica en el informe del Grupo de Trabajo de Composición Abierta de las Naciones Unidas de 2021. Las normas con las que todos nos hemos comprometido son un componente central de la estabilidad y la seguridad en el ciberespacio. Tenemos que seguir rindiendo cuentas (y hacer que otros las rindan) acerca de los compromisos que hemos asumido.

Entre otras cosas, debemos promover la cooperación entre los Estados, proteger la infraestructura crítica, salvaguardar las cadenas de suministro mundiales, prestar asistencia cuando sea necesario, respetar los derechos humanos y la privacidad e impedir el uso malicioso de las tecnologías digitales en los territorios nacionales de los Estados.

Seguimos reflexionando sobre la forma en que la pandemia de enfermedad por coronavirus (COVID-19) ha puesto de relieve la importancia de un ciberespacio seguro. Hemos visto informes a nivel internacional de una gama de diferentes actividades maliciosas en línea, tanto de actores estatales como no estatales. Esta actividad ha tenido como objetivo, entre otros, las infraestructuras sanitarias críticas; funcionarios que trabajan en la respuesta; y miembros del público. Esto es inaceptable y pone de manifiesto que las amenazas en el ciberespacio ponen vidas en riesgo. Nueva Zelandia, junto con otros Estados, ha condenado públicamente la ciberactividad maliciosa que socava la respuesta a la pandemia.

Medidas de fomento de la confianza

Seguimos comprometidos con resultados constructivos, prácticos y concretos para mejorar la ciberseguridad internacional y regional. Las medidas de fomento de la confianza constituyen un camino importante para lograrlo, y acogemos con satisfacción las iniciativas prácticas que apoyan el entendimiento mutuo, la transparencia, la previsibilidad y la estabilidad en el ciberespacio.

Para Nueva Zelandia, el Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN) es un foro clave para los debates regionales sobre ciberseguridad. Apreciamos la cooperación que tenemos con los miembros de ese foro y esperamos seguir trabajando con todos ustedes en los próximos años. Nueva Zelandia acoge la oportunidad de compartir las lecciones aprendidas dentro y entre

regiones para mejorar la transparencia, la comprensión y la confianza entre los asociados regionales en el ciberespacio.

Creación de capacidad

Nueva Zelandia quiere contribuir a que todos los Estados puedan reducir los riesgos asociados al aumento de la conectividad, sin dejar de beneficiarse de ella. Esto incluye el apoyo a una comprensión más amplia y profunda del marco de comportamiento responsable del Estado en el ciberespacio y su adhesión a él.

Para lograrlo, tenemos que asegurarnos de que todos nosotros contamos con las herramientas y la capacidad necesarias para participar de forma significativa en las discusiones y áreas de debate en curso, y para poner en marcha iniciativas a nivel nacional y regional que apoyen la estabilidad a nivel internacional.

Nueva Zelandia sigue comprometida con la creación de capacidad regional en materia de ciberseguridad, centrándose especialmente en la colaboración con nuestros vecinos del Pacífico y Asia Sudoriental. Seguimos llevando a cabo iniciativas en el marco del programa neozelandés de apoyo a la ciberseguridad en el Pacífico, dotado con NZ$10 millones, y apoyando el Centro de Excelencia sobre Ciberseguridad de la ASEAN-Singapur.

Conclusión

Tenemos mucho trabajo por delante, pero no partimos de cero. Una vez más, acogemos con satisfacción los resultados tanto del reciente Grupo de Expertos Gubernamentales de las Naciones Unidas como de los procesos del Grupo de Trabajo de Composición Abierta. Estos procesos, y los informes resultantes, son importantes logros complementarios que se refuerzan mutuamente. Debemos seguir construyendo sobre los cimientos creados por este (y otros) acuerdos de consenso refrendados por la Asamblea General.

Es importante que en los debates participen diversos puntos de vista, incluidos los de los Estados pequeños y los de las partes interesadas no gubernamentales. La amplitud del interés de los Estados Miembros por la ciberseguridad nos ha animado (la paz y la seguridad en el ciberespacio nos afectan a todos) y es alentador ver a una gama tan amplia de Estados realmente comprometidos con los esfuerzos para abordar estos desafíos. Nueva Zelandia está dispuesta a participar con todos ustedes en este desafío.

Anexo XLVIII

Declaración del Representante Permanente del Pakistán ante las Naciones Unidas

Quisiera expresar mi profundo reconocimiento y mi sincero agradecimiento a la Misión Permanente de la República de Estonia por haber convocado este importante y oportuno debate abierto del Consejo de Seguridad sobre el tema “Mantenimiento de la paz y la seguridad internacionales en el ciberespacio”.

Las tecnologías de la información y las comunicaciones (TIC) ofrecen grandes oportunidades y siguen creciendo en importancia para la comunidad internacional. Al mismo tiempo, la complejidad de las cuestiones inherentes al uso de las TIC plantea graves riesgos para la paz y la seguridad internacionales.

El uso hostil de las cibertecnologías se está acercando rápidamente a la fase en la que puede constituir una ruptura de la paz o una amenaza para la paz y la seguridad internacionales.

El uso indebido y el uso no regulado de las TIC podría derivar en graves consecuencias para la paz y la seguridad internacionales en caso de que se produjera un ataque cibernético contra una infraestructura clave. Los recientes incidentes de presuntos ciberataques son ilustrativos.

Es necesario abordar con urgencia la creciente perspectiva de la ciberseguridad como parte de los esfuerzos más amplios de las Naciones Unidas para prevenir los conflictos.

A este respecto, la adopción del informe aprobado por consenso por 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, en marzo de este año, tuvo una importancia histórica a la hora de apoyar los esfuerzos mundiales hacia el objetivo común de crear un entorno de TIC seguro, estable y pacífico.

También fue una fuerte reafirmación de la capacidad de la comunidad internacional para unirse y abordar los principales desafíos mundiales en las circunstancias más difíciles, como la pandemia.

Aunque entendemos que el informe no aborda las preocupaciones de todos los Estados Miembros, consideramos que es importante consolidar los avances logrados hasta ahora y mantener el impulso para continuar este proceso inclusivo y transparente.

El Pakistán sigue participando de forma positiva y constructiva en la labor del Grupo de Trabajo de Composición Abierta y acoge con satisfacción la creación del nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), establecido en virtud de la resolución 75/240 de la Asamblea General.

Este (el nuevo Grupo de Trabajo de Composición Abierta) proporciona foros extremadamente útiles para lograr un progreso significativo, basándose en las recomendaciones anteriores, con el fin de reforzar las normas de comportamiento responsable en el ciberespacio y lograr una cooperación internacional significativa

para minimizar las amenazas que suponen para la seguridad internacional los usos maliciosos de las TIC.

El Grupo de Expertos Gubernamentales de 2015 y el reciente informe del Grupo de Trabajo de Composición Abierta acordaron un conjunto de importantes conclusiones que contribuyeron a generar un amplio consenso entre los Estados Miembros de que el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad en el entorno de las TIC.

La Carta de las Naciones Unidas es inequívoca en su defensa categórica de los principios de soberanía, integridad territorial y no injerencia en los asuntos internos de otros Estados. Estos principios deben servir de guía para navegar por las complejidades de la cibergobernanza.

Al mismo tiempo, el grado, el alcance y la naturaleza de la aplicabilidad del derecho internacional y su interpretación en el comportamiento de los Estados y su uso de las TIC requieren una cuidadosa consideración.

Una simple afirmación de la aplicabilidad del derecho internacional vigente al ciberespacio no es suficiente para abordar los polifacéticos desafíos legales que surgen de las TIC. Debe adaptarse a las características únicas de la ciberesfera.

El Pakistán reconoce la importancia de desarrollar un instrumento internacional jurídicamente vinculante, adaptado específicamente a los atributos únicos de las TIC, para proporcionar un curso regulador que busque crear estabilidad y seguridad en el ciberespacio. Dicho marco jurídico debe abordar las preocupaciones e intereses de todos los Estados, basarse en el consenso y llevarse a cabo en el seno de las Naciones Unidas con la participación equitativa de todos los Estados.

Las normas voluntarias y no vinculantes sobre el uso responsable de las TIC por parte de los Estados pueden contribuir a reducir los riesgos para la paz y la seguridad internacionales. Sin embargo, dadas las amenazas sin precedentes en el entorno de las TIC y el rápido ritmo de los avances tecnológicos, es necesario reforzar los esfuerzos internacionales para desarrollar normas vinculantes que puedan ayudar a mantener la paz y la estabilidad y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico.

Debemos asegurarnos de que el ciberespacio no se utilice indebidamente para perpetuar las campañas de desinformación patrocinadas por el Estado, la incitación a la violencia, el discurso al odio y otras formas conexas de intolerancia, incluida la islamofobia.

Las Naciones Unidas tienen un papel central en la promoción del diálogo y la cooperación internacional entre los Estados Miembros para desarrollar un entendimiento común sobre aspectos clave, incluidos, sobre la aplicación del derecho y las normas internacionales, las reglas y los principios para el comportamiento responsable de los Estados, la promoción de medidas de fomento de la confianza y la transparencia y el apoyo a la creación de capacidades y la difusión de las mejores prácticas.

Con una población de más de 200 millones de personas y un floreciente panorama digital marcado por el creciente número de usuarios en línea, el Pakistán concede una inmensa importancia al aprovechamiento de las tecnologías digitales

para permitir el desarrollo socioeconómico y facilitar una gobernanza y una prestación de servicios públicos más eficaces y eficientes.

El Pakistán se ha comprometido a promover la cooperación internacional en materia de las TIC y la ciberseguridad como medio para reducir la brecha digital. Todos los países son partes interesadas por igual en el desarrollo de las normas que rigen la economía digital y la seguridad del ciberespacio y las TIC.

Anexo XLIX

Declaración de la Misión Permanente del Perú ante las Naciones Unidas

[Original: español]

El Perú saluda la iniciativa de la presidencia de Estonia de convocar a este debate abierto de alto nivel del Consejo de Seguridad sobre un asunto de creciente y primordial importancia para el mantenimiento de la paz y la seguridad internacional. Agradecemos las presentaciones de los distinguidos ponentes.

Somos conscientes de la relevancia del uso de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la seguridad internacional, su rápida evolución y los beneficios que generan. El escenario de crisis sanitaria a raíz de la pandemia de la enfermedad por coronavirus (COVID-19) ha puesto de relieve nuestra dependencia de los mismos, la urgencia de reducir la brecha digital y la importancia de proteger la infraestructura crítica.

Del mismo modo, conocemos también los peligros que se pueden derivar por el mal uso de las TIC, incrementándose así los riesgos de conflicto en el ciberespacio. Su utilización malintencionada por agrupaciones terroristas, organizaciones criminales, grupos armados y otros agentes constituyen graves amenazas sistémicas a la seguridad y paz internacional.

Teniendo en consideración que las amenazas no provienen de las tecnologías en sí mismas, sino del uso que se haga de ellas, resulta necesario que profundicemos nuestro entendimiento sobre su adecuada utilización y cómo evitar los usos deliberadamente maliciosos, promoviendo un ciberespacio abierto, libre, estable y seguro.

Con ese fin, reconocemos la primacía de la Carta de las Naciones Unidas, como una base firme en materia de seguridad, y respaldamos la aplicación del derecho internacional y del derecho internacional humanitario en el ciberespacio. Asimismo, estimamos primordial que se regule la normativa internacional sobre esta materia a través del establecimiento de obligaciones jurídicamente vinculantes.

Valoramos los esfuerzos y avances notables que se han logrado en las Naciones Unidas en la formulación de elementos para promover la aplicación del derecho internacional, la implementación de normas y el comportamiento responsable de los estados en el ciberespacio en el contexto de la seguridad internacional. En ese sentido, saludamos los informes sustantivos adoptados por el Grupo de Trabajo de Composición Abierta y por el Grupo de Expertos Gubernamentales, y esperamos que armonizando el trabajo de ambos procesos podamos contar con un solo discurso y curso de acción coherentes sobre ciberseguridad.

Además de los esfuerzos internacionales, consideramos fundamentales las acciones regionales y nacionales, en particular en la promoción de medidas de fomento de la confianza, la creación de capacidades, el intercambio de información y la divulgación de las mejores prácticas para garantizar la ciberseguridad. Para los países de menor desarrollo tecnológico nos resulta primordial que se concreten entendimientos y acuerdos que eviten que el ciberespacio se convierta en un escenario

de conflicto por los posibles efectos que tendrían debido a la insuficiente capacidad para evitarlos.

Tomando en cuenta la naturaleza interconectada y compleja del ciberespacio, las continuas innovaciones en materia de TIC, y la creciente incorporación de tecnologías emergentes, apoyamos la participación del sector privado, en particular de la industria informática, la sociedad civil y la academia para hacer frente a los desafíos. Estamos convencidos que sus contribuciones continuarán enriqueciendo las deliberaciones multilaterales sobre este asunto.

Concluimos subrayando la necesidad de que trabajemos de manera coordinada la comunidad internacional en su conjunto y adoptemos nuevas acciones para estudiar las amenazas existentes y las posibles medidas de cooperación para enfrentarlas. En ese sentido, el rol del Consejo de Seguridad en la prevención de conflictos y en el fomento de la paz y seguridad será fundamental para que se garantice un ciberespacio abierto, pacifico, seguro y provechoso, que fomente el desarrollo sostenible y el bienestar de los pueblos.

Anexo L

Declaración de la Misión Permanente de Polonia ante las Naciones Unidas

El primer debate abierto en el Consejo de Seguridad sobre la ciberseguridad constituye un hito importante en nuestra percepción de los desafíos contemporáneos para la paz y la seguridad internacionales.

Agradecemos y elogiamos a la Presidencia estonia por permitirnos abordar las cuestiones de ciberseguridad en este momento tan oportuno.

En 2019, cuando fue miembro del Consejo de Seguridad, Polonia le señaló los problemas de los ciberincidentes en Oriente Medio.

Ahora, es el momento de concienciar a la comunidad internacional en su conjunto ante el aumento constante de las actividades maliciosas en el ciberespacio. Desde hace dos décadas, paralelamente al desarrollo sin precedentes de las tecnologías digitales, observamos en todo el mundo ciberataques y ciberincidentes cada vez más sofisticados. Polonia los experimenta a diario.

Por supuesto, son de distinta naturaleza. Algunos tienen un trasfondo puramente delictivo, otros están motivados por objetivos económicos y, cada vez con más frecuencia, políticos. Sin embargo, hay un denominador común de estas actividades: todas son ilegales. Las actividades cibernéticas maliciosas no pueden ser, de ninguna manera, justificadas o defendidas.

Como usted, señora Presidenta, ha señalado acertadamente en su nota conceptual: “El derecho internacional vigente, en particular la Carta de las Naciones Unidas, proporciona suficiente orientación a los Estados sobre la realización de ciberactividades”. Es una gran tarea de la comunidad internacional elaborar un paradigma comúnmente aceptable de actividades en el ciberespacio.

Polonia apoya firmemente los logros de los Grupos de Expertos Gubernamentales y ha participado activamente en los trabajos del Grupo de Trabajo de Composición Abierta, que en su informe ha reafirmado la aplicación del derecho internacional en el ciberespacio. Esperamos que el 2º Grupo de Trabajo de Composición Abierta contribuya a una mejor comprensión común de la importancia del uso pacífico del ciberespacio. También concedemos una gran importancia al trabajo del Comité Ad Hoc dentro de la Tercera Comisión de la Asamblea General.

Además de la evaluación común de la situación, lo más importante es una acción común y bien orquestada. Por ello, Polonia apoya una amplia participación de las múltiples partes interesadas, las ONG, el sector privado y el mundo académico en el debate internacional sobre ciberseguridad.

También creemos firmemente que el trabajo crucial debe realizarse dentro de las regiones. Con el compromiso de las organizaciones regionales, los Estados individuales y los representantes de la sociedad civil, podemos desarrollar instrumentos útiles para la creación de capacidades o medidas de fomento de la confianza.

Para estimular los esfuerzos internacionales, tanto a nivel mundial como regional, necesitamos poner en común nuestros recursos y nuestra energía diplomática. Por ello, apoyamos y promovemos firmemente el establecimiento del programa de acción como formato definitivo de cooperación internacional en las actividades del ciberespacio.

Con este debate abierto, esperamos que la ciberseguridad ocupe su lugar permanente en la agenda del Consejo de Seguridad. Los costos políticos y económicos de las actividades maliciosas en el ciberespacio son demasiado elevados para que este importante organismo de las Naciones Unidas los pase por alto.

Tengan la seguridad de que Polonia no escatimará esfuerzos para contribuir a todos los procesos globales y regionales que conduzcan al fortalecimiento de la ciberorden sobre la base del respeto al derecho internacional y a las normas comúnmente acordadas.

Anexo LI

Declaración de la Misión Permanente de Qatar ante las Naciones Unidas

[Original: árabe]

Quisiera dar las gracias a la Alta Representante de las Naciones Unidas para Asuntos de Desarme, Izumi Nakamitsu, por su exposición informativa y por la labor que lleva a cabo la Oficina de Asuntos de Desarme para otorgar a la ciberseguridad el lugar que debe tener en la agenda de las Naciones Unidas para el desarme.

Cada día vemos el impacto transformador de un mundo que depende, en gran medida, del ciberespacio, pero las tecnologías digitales y la conectividad global también facilitan el mal uso del ciberespacio, lo que es preocupante, particularmente dado que las infraestructuras y los servicios públicos vitales dependen mucho de la esfera digital. El mal uso del ciberespacio y de la tecnología de la información y las comunicaciones (TIC) por parte de agentes gubernamentales y no gubernamentales constituye una amenaza a la seguridad nacional y afecta a la paz y la seguridad, tanto regionales como internacionales, y a las relaciones internacionales. Además de esto, los grupos terroristas aprovechan las tecnologías digitales emergentes para aumentar su capacidad para cometer sus delitos.

Está claro que ningún país es inmune a la amenaza del mal uso del ciberespacio y, por lo tanto, es necesario adoptar medidas colectivas para enfrentarse a este desafío mundial. Afortunadamente, el propio ciberespacio puede proporcionar una excelente herramienta para coordinar los esfuerzos internacionales a tal fin. Como hemos visto durante el año pasado, las plataformas digitales han sido un medio indispensable para continuar la labor de los órganos de las Naciones Unidas y otros foros de cooperación internacional.

Es necesario evaluar las posibles amenazas y el impacto de la piratería electrónica y el mal uso del ciberespacio sobre la paz y la seguridad y realizar esfuerzos colectivos para reforzar el entorno de la seguridad regional e internacional para enfrentarse a dichas amenazas y fomentar el uso pacífico del ciberespacio y de las tecnologías digitales avanzadas relacionadas.

En este sentido, hay que prestar la debida consideración a la aplicación del derecho internacional al uso de la tecnología de la información y las comunicaciones por parte de los estados y al fomento de un comportamiento responsable por parte de los países en relación con el ciberespacio en el marco de la seguridad internacional.

Y, al mismo tiempo, deben mantenerse el libre flujo de la información y el respeto a los derechos humanos y las libertades fundamentales en un entorno digital abierto, seguro y accesible para todos.

Además de los marcos internacionales, las estrategias nacionales son importantes para orientar la labor y la coordinación entre los interesados, incluido el sector privado cuyo papel se considera fundamental en todo aquello relacionado con la tecnología digital.

Qatar da prioridad a la protección de la seguridad de la información y a su infraestructura y, con este fin, está adoptando medidas integrales y ha desarrollado sus capacidades en este sentido, trabajando por reforzar la cooperación internacional y el fomento de las capacidades.

La cuestión de la seguridad de la información y de la ciberseguridad figuran en el programa de las Naciones Unidas desde hace muchos años, pero los rápidos avances en este campo requieren medidas que la acompañen. Por ello, acogemos con satisfacción la atención que el Secretario General de las Naciones Unidas, quien ha hecho del fortalecimiento de un entorno pacífico de la tecnología de la información y las comunicaciones una de sus prioridades principales, ha prestado a esta cuestión. También nos complace ver que se ha vuelto a llegar a un consenso en el Grupo de Expertos Gubernamentales (GEG). También esperamos con interés el próximo período de sesiones del Grupo de Trabajo de Composición Abierta OEWG con el fin de contribuir a ampliar el campo del consenso internacional a este respecto.

Por último, quisiera reiterar de nuevo que el Estado de Qatar continuará esforzándose incansablemente, y a diferentes niveles, para contribuir a los esfuerzos mundiales para reforzar la paz, la seguridad y la estabilidad del ciberespacio.

Anexo LII

Declaración del Representante Permanente de la República de Corea ante las Naciones Unidas, Cho Hyun

En primer lugar, quisiera agradecerles por celebrar el oportuno debate abierto de hoy sobre “El mantenimiento de la paz y la seguridad internacionales en el ciberespacio”. Mi agradecimiento también va dirigido a la Alta Representante para Asuntos de Desarme, Sra. Nakamitsu, su detallada exposición informativa.

En las últimas dos décadas, la raza humana ha sido testigo de un avance tecnológico en el campo de la tecnología digital como nunca antes. El concepto de ciberespacio, que antes solo estaba en la imaginación de la ciencia ficción, se ha convertido desde entonces en una realidad cotidiana para todos nosotros; con el espacio virtual y físico que nos rodea integrado en un ecosistema. Y, por mucho que este avance nos haya aportado prestaciones económicas y sociales sin precedentes, también nos hemos vuelto cada vez más vulnerables frente a las ciberactividades maliciosas. En el último año, en medio de la pandemia mundial, nuestras vidas se han vuelto aún más susceptibles a las ciberamenazas, ya que hay más personas conectadas. Al mismo tiempo, el creciente número de ciberataques contra la infraestructura crítica, incluidas las infraestructuras e instalaciones médicas de todo el mundo, es cada vez más preocupante.

En este contexto, me gustaría destacar las siguientes cuatro observaciones que son de especial importancia para mi delegación.

En primer lugar, la República de Corea apoya el papel central de las Naciones Unidas en los debates en curso sobre la forma de abordar los desafíos que se plantean y avanzar en el comportamiento responsable de los Estados en el ciberespacio. A este respecto, mi delegación se congratula de la adopción del informe de consenso a principios de este año del Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, así como del cuarto informe de consenso de los Grupos de Expertos Gubernamentales (Grupo de Expertos Gubernamentales), adoptado el mes pasado. Estos logros reflejan el progreso que se ha realizado en el marco acumulativo y evolutivo del comportamiento responsable de los Estados en su uso de las TIC y, a través de estos ejercicios, ha mejorado la comprensión de la comunidad internacional en su conjunto en esta área crítica.

Como todos los Estados Miembros acordaron por consenso en el anterior informe del Grupo de Trabajo de Composición Abierta, el derecho internacional se aplica al uso de las TIC por parte de los Estados, y deben guiarse por el marco de comportamiento responsable de los Estados en el uso de las TIC, tal como se indica en los informes del Grupo de Expertos Gubernamentales. La primacía del derecho internacional y el orden basado en normas deben aplicarse igualmente al ciberespacio para garantizar la paz y la seguridad.

En segundo lugar, mi delegación aprecia mucho el reciente informe de consenso del Grupo de Expertos Gubernamentales que presenta una capa adicional de entendimiento sobre las normas de comportamiento responsable de los Estados, las medidas de fomento de la confianza, la creación de capacidades y la forma en que el derecho internacional se aplica al uso de las TIC por parte de los Estados. El informe

reafirmó la aplicabilidad del derecho internacional, incluida la Carta de las Naciones Unidas, y en particular, el derecho internacional humanitario en situaciones de conflicto armado. También apoyamos firmemente la recomendación del Grupo de Expertos Gubernamentales de que los Estados que sean parte de cualquier disputa internacional, incluidas las que impliquen el uso de las TIC, busquen primero una solución por medios pacíficos, como se describe en el artículo 33 de la Carta de las Naciones Unidas.

En concreto, mi delegación se alegra de que el informe profundice en la norma de que los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer actos ilícitos internacionales con el uso de las TIC. Este principio de "diligencia debida", sugerido por la República de Corea y reflejado por primera vez en el informe del Grupo de Expertos Gubernamentales de 2015, señala que cada Estado debe adoptar medidas apropiadas y razonables para hacer frente a la situación si tiene conocimiento o si se le notifica un hecho internacionalmente ilícito.

En tercer lugar, debemos redoblar nuestros esfuerzos para fomentar la confianza y promover el entendimiento común. La República de Corea, como Estado Miembro responsable y nación líder en el sector digital y tecnológico, ha participado y contribuido activamente en diversos foros regionales y multilaterales. La semana pasada, el 22 de junio, la República de Corea, en estrecha colaboración con la Organización para la Seguridad y la Cooperación en Europa, organizó con éxito las "Terceras Conferencias Interregionales sobre Seguridad Cibernética/TIC" para debatir las tendencias actuales en materia de ciberseguridad y promover la cooperación en este ámbito entre las organizaciones regionales. También acogimos la 19ª Conferencia Conjunta de la República de Corea y las Naciones Unidas sobre Desarme y No Proliferación, centrada en el desarrollo y el impacto de las tecnologías emergentes en 2020, y copresidiremos la Reunión Internacional del ARF sobre seguridad de las TIC para el período 2021-2023. Además, el próximo mes de noviembre, la República de Corea pondrá en marcha un foro internacional para seguir dinamizando los debates sobre las nuevas amenazas a la seguridad, incluidos los ciberataques y el uso malicioso de las nuevas tecnologías en el contexto de la paz y la seguridad internacionales. Bajo los principios de inclusividad, transparencia y apertura, el Foro proporcionará una plataforma internacional acogedora y accesible a las distintas partes interesadas.

En cuarto lugar, nunca se insistirá lo suficiente en que la ciberseguridad requiere un enfoque de múltiples partes interesadas, ya que la dimensión de la seguridad internacional del ciberespacio abarca múltiples ámbitos y disciplinas. Aunque los gobiernos siguen siendo el centro, solo podemos ser verdaderamente eficaces si implicamos en el proceso a otras partes interesadas clave, como el sector privado, el mundo académico, la sociedad civil y la comunidad técnica. También debemos tener en cuenta que el compromiso con otras partes interesadas puede contribuir significativamente a promover un entendimiento común y la aplicación del marco de comportamientos responsables en el ciberespacio.

En el cierre, me gustaría aprovechar esta oportunidad para reafirmar el compromiso de la República de Corea de trabajar con las Naciones Unidas y todos los Estados Miembros para fomentar aún más un ciberespacio abierto, seguro, estable, accesible y pacífico.

Anexo LIII

Declaración de la Misión Permanente de Rumania ante las Naciones Unidas

Elogiamos a Estonia por su iniciativa de organizar el primer debate abierto sobre la ciberseguridad como cuestión formal específica en el programa del Consejo de Seguridad. Se trata de una iniciativa oportuna para seguir reforzando el orden internacional basado en normas, así como nuestra cooperación multilateral en un tema de máxima importancia para el mantenimiento de la paz y la seguridad internacionales.

El debate de hoy refuerza los notables progresos realizados por los Estados Miembros en los últimos informes de consenso del GEG y del Grupo de Trabajo de Composición Abierta en la consolidación del marco normativo para el comportamiento responsable de los Estados en el ciberespacio, basado en el derecho internacional existente, las normas, las medidas de fomento de la confianza y la creación de capacidades.

En un entorno de seguridad internacional en constante evolución, las tecnologías de la información y las telecomunicaciones (TIC) presentan tanto ventajas destacadas como algunas de las amenazas más destacadas y agudas de la actualidad. Dichas amenazas provienen tanto de actores estatales como no estatales, y se dirigen a diversos sectores clave, como la energía, el transporte, las finanzas y la salud, que dependen de infraestructuras clave tanto físicas como digitales para prestar servicios a nivel nacional, regional o mundial. Las tecnologías digitales también pueden ser utilizadas indebidamente para intentar debilitar nuestras instituciones democráticas y erosionar la confianza pública en los principios democráticos. Además, pueden utilizarse para explotar las vulnerabilidades del sistema con fines geopolíticos. La pandemia de enfermedad por coronavirus (COVID-19) es un ejemplo reciente y funesto del impacto destructivo de las ciberoperaciones destinadas a comprometer o alterar la información estratégica sobre la investigación y distribución de vacunas.

En este entorno, no se puede sobrestimar el valor de la cooperación multilateral entre Estados responsables, ni el de las asociaciones reforzadas entre la administración pública, el sector privado, la sociedad civil y el mundo académico. Tenemos que trabajar juntos para compartir información confiable, precisa, oportuna y fidedigna sobre las amenazas y las respuestas creíbles, y para coordinar nuestros esfuerzos y reforzar los mecanismos de prevención pertinentes a nivel mundial, regional y nacional. Y lo que es más importante, debemos concentrar nuestros esfuerzos en el desarrollo de la resiliencia de nuestras sociedades ante el impacto de las amenazas a nuestras infraestructuras críticas, ya sean físicas, digitales o institucionales.

En este sentido, cabe destacar que en el marco de su actual presidencia de la Comunidad de Democracias, Rumania promueve activamente el vínculo entre la tecnología y los procesos democráticos como una de sus principales prioridades; como anfitriona del recién creado Centro de Competencia Industrial, Tecnológica y de Investigación de la Ciberseguridad en Bucarest, Rumania acoge y promueve activamente las inversiones de asociación previstas entre los Estados miembros de la Unión Europea y la industria; como promotora y anfitriona del recién creado Centro

Euroatlántico para la Resiliencia, Rumania trabajará para generar nuevas ideas y estrategias de adaptación de las sociedades a los nuevos desafíos para la paz, la seguridad y la estabilidad democrática.

Como Estado miembro de la Unión Europea, Rumania está trabajando para promover y aplicar las principales dimensiones de la nueva Estrategia de Ciberseguridad de la Unión Europea para la Década Digital, especialmente la caja de herramientas de ciberdiplomacia, que incluye herramientas de ciberdisuasión y comunicación estratégica de la Unión Europea contra las ciberactividades maliciosas. La caja de herramientas de ciberdiplomacia de la Unión Europea tiene un papel importante para prevenir, disuadir y responder a los ciberincidentes que afectan a la seguridad de la Unión Europea y de los Estados Miembros.

Rumania aborda la ciberseguridad como una dimensión clave de la seguridad nacional y se esfuerza por garantizar el desarrollo y la adaptación de un marco jurídico nacional adecuado para facilitar la cooperación y el intercambio eficaz de información entre las autoridades competentes y cumplir con sus obligaciones internacionales. El comportamiento responsable de los Estados implica obligaciones positivas clave: disponer de una legislación, ciberestrategias e instituciones nacionales modernas y eficaces, promover y participar en una cooperación internacional sustancial y, lo que es muy importante, ser transparentes, defender las normas acordadas, promover los principios democráticos y respetar plenamente la dignidad humana.

La seguridad del ciberespacio representa para Rumania una de sus más altas prioridades políticas y diplomáticas, que se persigue mediante el fomento de un comportamiento responsable de los Estados y la consolidación de mecanismos preventivos y normativos a nivel mundial, regional y nacional. Nos comprometemos a respaldar un ciberespacio mundial, abierto, seguro y protegido, en el que se respeten plenamente los derechos humanos y las libertades fundamentales y el estado de derecho. También opinamos que un entorno en línea abierto, seguro, estable, accesible y pacífico no puede imaginarse fuera de un sistema internacional basado en normas, principalmente fundado en el derecho internacional.

Rumania participó activamente en los dos procesos de las Naciones Unidas destinados a consolidar el marco de la ciberseguridad (GEG y Grupo de Trabajo de Composición Abierta), que concluyeron con éxito su labor acordando importantes recomendaciones para prevenir los conflictos en el ciberespacio (desde la consolidación del entendimiento sobre la aplicación del derecho internacional en el ciberespacio, hasta normas voluntarias no vinculantes para el comportamiento responsable de los Estados, así como propuestas para un futuro diálogo institucionalizado).

De cara al futuro, Rumania opina que el establecimiento de un programa de acción de las Naciones Unidas para promover el comportamiento responsable de los Estados en el ciberespacio fomentaría la adopción de medidas prácticas concretas para el fomento de la capacidad y la confianza, y además facilitaría el acceso a las fuentes de financiación, de manera abierta, inclusiva y transparente, de forma permanente, ayudando así a todos los Estados Miembros en sus esfuerzos por prevenir conflictos, desarrollar percepciones comunes de las amenazas y aumentar su ciberresiliencia.

En todos los procesos futuros de las Naciones Unidas, Rumania promoverá activamente su posición de que el derecho internacional se aplica al ciberespacio. Nuestra firme convicción es que no hay motivos para considerar que el derecho internacional vigente podría no regir adecuadamente las relaciones entre Estados que se llevan a cabo en el ciberespacio o a través del medio del ciberespacio. Esto incluye al derecho internacional humanitario en el contexto de las ciberoperaciones llevadas a cabo como parte de un conflicto armado (tanto internacional como no internacional). En dichas circunstancias, la planificación y realización de ciberoperaciones deben realizarse de conformidad con los principios que rigen las hostilidades, es decir, distinción, proporcionalidad, necesidad y precaución.

Sin embargo, sostener más diálogo e intercambios entre Estados pueden ayudar a aclarar algunas de las circunstancias específicas de la aplicabilidad del derecho internacional al ciberespacio. Teniendo esto en cuenta, observamos que la opinión preliminar de Rumania sobre este tema se ha emitido con el fin de contribuir al trabajo del Grupo de Expertos Gubernamentales de conformidad con la resolución 73/266 de la Asamblea General.

Anexo LIV

Declaración de la Misión Permanente del Senegal ante las Naciones Unidas

[Original: francés]

En primer lugar, me gustaría dar las gracias a la Sra. Kaja Kallas, Primera Ministra de la República de Estonia, por presidir este importante debate abierto virtual de alto nivel sobre ciberseguridad, un tema que cobra cada vez más importancia en el sistema de las Naciones Unidas a la luz de las crecientes amenazas a la seguridad en el ciberespacio. Me gustaría dar las gracias asimismo a la Alta Representante de las Naciones Unidas para Asuntos de Desarme, la Sra. Izumi Nakamitsu, cuya intervención ha sido seguida con mucho interés por mi delegación.

La constatación es evidente: la proliferación de actividades maliciosas en el ciberespacio constituye una verdadera amenaza para la paz y la seguridad internacionales y requiere la atención del Consejo de Seguridad. El debate que nos reúne hoy indica que el Consejo tiene en cuenta esta amenaza, y es una prolongación de los esfuerzos incansables emprendidos desde hace más de un decenio por la Asamblea General en materia de ciberseguridad.

En este espíritu, los diferentes procesos de reflexión desarrollados en el marco de los cuatro Grupos de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, respectivamente, sobre el comportamiento responsable de los Estados en el ciberespacio y sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional son encomiables y constituyen una señal inequívoca de la voluntad de los Estados de encontrar un consenso sobre las modalidades de regulación del ciberespacio.

Al reconocer la aplicabilidad de varios principios y normas del derecho internacional vigente y proclamar la responsabilidad de los Estados por los actos internacionalmente ilícitos cometidos en el ciberespacio, las conclusiones de los informes del Grupo de Trabajo de Composición Abierta y del último Grupo de Expertos Gubernamentales adoptados, respectivamente, en marzo y mayo de 2021, constituyen una contribución adicional a la comprensión del ejercicio del derecho internacional en el ciberespacio.

Además, al igual que varios países, el Senegal considera que las medidas de fomento de la confianza y de transparencia son indispensables para promover un comportamiento responsable de los Estados en el ciberespacio y por ese motivo deberían reforzarse.

En efecto, mediante intercambios periódicos de información sobre sus actividades cibernéticas, los Estados pueden ayudar a evitar percepciones erróneas y malentendidos, prevenir y gestionar las crisis derivadas del uso del ciberespacio y, en su caso, sentar las bases para una cooperación digital fructífera.

Sin embargo, debido a la rápida evolución observada en el sector y a la aparición de nuevas ciberamenazas, el Senegal opina que las normas de derecho internacional con fuerza ejecutiva y las medidas de fomento de la confianza y de transparencia no bastarían, por sí solas, para regular de manera conveniente el ciberespacio. Así, deberían completarse con un instrumento jurídico internacional vinculante.

Por lo tanto, resulta pertinente un enfoque general que combine medidas proactivas de fomento de la confianza y de transparencia con una convención internacional vinculante, no solo para establecer las normas del ciberespacio, sino también para tener en cuenta las posiciones y los intereses de todos los Estados Miembros. Las reflexiones del nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) deberían orientarse hacia este enfoque.

Por su parte, el Gobierno del Senegal está firmemente comprometido a contribuir positivamente a la realización de este proyecto que sigue siendo una prioridad para él desde la adopción, en noviembre de 2017, de la Estrategia Nacional de Ciberseguridad 2022. Este documento, cuyo ideal consiste en establecer en 2022 un ciberespacio fiable, seguro y resiliente para todos en el Senegal, incluye una evaluación del contexto estratégico de la ciberseguridad en el Senegal que tiene en cuenta las amenazas actuales y futuras y define cinco objetivos estratégicos: el refuerzo del marco jurídico e institucional de la ciberseguridad; la protección de las infraestructuras de información críticas y los sistemas de información del Estado; el fomento de una cultura de ciberseguridad; la creación de capacidades y conocimientos técnicos sobre ciberseguridad en todos los sectores; y la participación en las iniciativas regionales e internacionales de ciberseguridad.

Con arreglo a este último objetivo, el Senegal ha sido el primer país en ser parte en la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo). También se ha adherido al Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, y al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108 del Consejo de Europa, STE núm. 108), así como a su Protocolo adicional sobre las autoridades de supervisión y los flujos transfronterizos de datos (STE núm. 181). Además, ha adoptado la directiva de la Comunidad Económica de los Estados de África Occidental sobre la lucha contra la ciberdelincuencia, de 19 de agosto de 2011, y ha respaldado el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, de 12 de noviembre de 2018, y el Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea, de 15 de mayo de 2019.

A nivel interno, mi país se ha dotado de un marco jurídico para regular la utilización de las tecnologías de la información y las comunicaciones. Además de la ley núm. 2008-08 de 25 de enero de 2008 sobre las transacciones electrónicas, cabe citar la ley de orientación núm. 2008-10 de 25 de enero de 2008 sobre la sociedad de la información, las leyes núm. 2008-11 y núm. 2008-12 de 25 de enero de 2008 sobre la ciberdelincuencia y sobre la protección de los datos personales, y la ley núm. 2018-28 de 28 de noviembre de 2018 sobre el código de comunicaciones electrónicas. Siguiendo esta misma estela, se ha revisado el Código de Procedimiento Penal para tener en cuenta el procedimiento en materia de infracciones cometidas por medio de TIC.

En paralelo, se ha reforzado la arquitectura institucional con la creación del Servicio Técnico Central de Códigos y Seguridad de los Sistemas de Información, la División Especial de Lucha contra la Ciberdelincuencia y la Comisión de Protección de Datos. Esta arquitectura debería enriquecerse pronto con la creación de un comité

consultivo nacional sobre ciberseguridad y una estructura nacional de ciberseguridad encargada de dirigir la aplicación de la Estrategia Nacional de Ciberseguridad 2022.

Además, la creación de cibercapacidades constituye otro desafío, sobre todo para los países en desarrollo. Por esta razón, el Senegal se ha esforzado mucho en materia de formación sobre seguridad de la información. De este modo, mi país cuenta, a día de hoy, con varios establecimientos de formación en esta materia, entre los cuales los más ilustres son la Escuela Nacional de Ciberseguridad con Vocación Regional de Dakar abierta en noviembre de 2018 y el Instituto Profesional para la Seguridad de la Información creado en octubre de 2015.

La ciberseguridad no debe frenar la innovación y las oportunidades de desarrollo que ofrecen las nuevas tecnologías de la información y las comunicaciones o utilizarse con el fin de restringir su desarrollo.

Las iniciativas de ciberseguridad, como medios de prevención y lucha contra el uso malicioso del ciberespacio, deben tener como objetivo último el fomento de un entorno digital accesible, seguro, pacífico y próspero, que no deje a nadie atrás, de conformidad con la meta 9c del Objetivo 9 de la Agenda 2030.

El Gobierno del Senegal, consciente de esta ambición, ha elaborado la Estrategia Senegal Digital 2016-2025, con arreglo al Plan Senegal Emergente. Este documento, que encarna la ambición del Senegal de mantener una posición de país líder innovador en África en el ámbito digital, se articula en torno al eslogan “Las TIC para todos y para todos los usos en 2025 en el Senegal con un sector privado dinámico e innovador en un ecosistema eficiente”.

Anexo LV

Declaración del Representante Permanente de Singapur ante las Naciones Unidas, Burhan Gafoor

Le agradezco por celebrar esta importante reunión, que representa la primera vez que el Consejo de Seguridad abordará formalmente la ciberseguridad.

Es un tema oportuno. La aceleración de la digitalización provocada por la pandemia de enfermedad por coronavirus (COVID-19) ha beneficiado nuestras vidas de nuevas maneras. También nos ha abierto a nuevas vulnerabilidades. Las ciberamenazas y las ciberactividades maliciosas son cada vez más frecuentes y sofisticadas y tienen consecuencias más graves. Se estima que, en 2020, las ciberactividades maliciosas habrán traído aparejadas pérdidas de casi $1 billón. La reciente oleada de actividades de este tipo es un claro recordatorio de que la comunidad internacional debe seguir protegiéndose y estar preparada para responder a estas amenazas mundiales y transfronterizas. En este sentido, quisiera destacar cinco aspectos.

En primer lugar, debemos reconocer que el ciberespacio es fundamentalmente una cuestión de gestión de los bienes comunes globales. Como Estado pequeño, Singapur siempre ha apoyado un sistema multilateral basado en reglas que tiene su origen en el respeto por el derecho internacional. Nuestro enfoque no es distinto con respecto al ciberespacio. Para mantener un ciberespacio seguro, confiable, abierto e interoperable, debemos adoptar un enfoque mundial, basado en reglas y normas mundiales y en la adhesión al derecho internacional. Hacerlo será un desafío, dado el telón de fondo de un panorama mundial inestable y díscolo causado por las crecientes tensiones geopolíticas. Sin embargo, no tenemos más opción que seguir defendiendo y apoyando la aplicabilidad del derecho y las normas internacionales para fomentar el comportamiento responsable de los Estados en el ciberespacio. Debemos redoblar la colaboración internacional para aumentar la ciberresiliencia y la estabilidad.

Singapur está comprometido con el papel de las Naciones Unidas, como único foro universal, inclusivo y multilateral, en el desarrollo de normas que rijan el ciberespacio. Nos sentimos alentados por la maduración de los debates sobre ciberseguridad en las Naciones Unidas. Desde la primera vez que se incluyó la seguridad de las tecnologías de la información y las comunicaciones (TIC) en la agenda de las Naciones Unidas en 1998, seis Grupos de Expertos Gubernamentales han estudiado las amenazas que plantea el uso indebido de las TIC en el contexto de la seguridad internacional y la forma de abordarlas. Cuatro de estos Grupos han acordado informes sustantivos, incluida la última iteración, que acaba de concluir sus trabajos.

Los debates sobre ciberseguridad se presentaron por primera vez a los miembros en general en la sesión de la Asamblea General. Esto se llevó a cabo mediante el establecimiento del Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Nos sentimos alentados por el éxito de la reciente aprobación del informe de consenso del Grupo de Trabajo de Composición Abierta. El informe contribuye a nuestro entendimiento común sobre muchas cuestiones e identifica áreas sobre las que es necesario seguir debatiendo.

Singapur participó activamente tanto en el Grupo de Trabajo de Composición Abierta como en el más reciente Grupo de Expertos Gubernamentales. Singapur también se honra en ser elegido Presidente del nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y su uso para el período 2021-2025. Como Presidente de este órgano, Singapur está firmemente decidido a continuar con los debates abiertos, inclusivos y transparentes sobre la ciberseguridad en las Naciones Unidas. Confiamos en que la labor del nuevo Grupo de Trabajo de Composición Abierta contribuya a un orden multilateral basado en normas en el ciberespacio y brinde a todos los Estados, grandes o pequeños, la confianza, la previsibilidad y la estabilidad que son esenciales para el progreso económico, la creación de empleo y la adopción de tecnología. Esperamos con interés colaborar en estrecha colaboración con todos los Estados Miembros en ese aspecto.

En segundo lugar, todos los Estados son vulnerables a la ciberactividad maliciosa, que está creciendo en escala y sofisticación. Sin embargo, los Estados pequeños son especialmente vulnerables, sobre todo los países en desarrollo y los países menos adelantados. Si de verdad queremos llegar a un enfoque mundial de la ciberseguridad, debemos centrarnos sobre todo en la creación de capacidades para los países que necesitan ayuda. Este es un ámbito en el que las Naciones Unidas pueden ayudar a coordinar los esfuerzos. Singapur colaboró con la Oficina de Asuntos de Desarme de las Naciones Unidas para elaborar un curso de capacitación en línea abierto a todos los Estados Miembros con el que promover una mayor comprensión del uso de las TIC y sus implicaciones para la seguridad internacional. Seguimos decididos a colaborar con las Naciones Unidas y prestarles apoyo para ofrecer más programas de desarrollo de capacidades.

En tercer lugar, Singapur considera que se puede hacer más para promover una mayor difusión y aplicación de las 11 normas de carácter voluntario y no vinculante de comportamiento responsable de los Estados en el uso de las TIC. Apoyamos el intercambio de mejores prácticas y experiencias sobre la aplicación de las normas. Esto ayudará a detectar los desafíos que debemos abordar y las brechas en las que pueden ser necesarias normas adicionales. Singapur está a favor de que se sigan desarrollando las normas existentes. Por ejemplo, la ciberactividad maliciosa contra cualquier Infraestructura Crítica de Información (CII) transfronteriza, como las nubes y los sistemas bancarios, puede causar interrupciones de gran alcance en los servicios esenciales de múltiples Estados, incluidos los relacionados con el comercio, el transporte y las comunicaciones internacionales. Los Estados deberían estudiar cómo mejorar la cooperación transfronteriza con los propietarios y operadores de las infraestructuras pertinentes para mejorar las medidas de seguridad de las TIC concedidas a dichas infraestructuras.

Esto me lleva a la cuarta observación sobre un mayor compromiso con otras partes interesadas, en particular el sector privado. Dado que una parte importante de la CII es propiedad del sector privado, la comunidad internacional debe encontrar maneras de cooperar estrechamente con el sector privado para prevenir y mitigar el impacto de estas disrupciones. Singapur apoya un enfoque de colaboración entre los sectores público y privado para intercambiar las mejores prácticas en apoyo de un marco sólido de ciberseguridad.

En quinto lugar, Singapur considera que las organizaciones regionales desempeñan un papel esencial de apoyo a los debates de las Naciones Unidas y de ayuda a la aplicación de las reglas y normas elaboradas en las Naciones Unidas. La ciberseguridad fue una prioridad para la Presidencia de la Asociación de Naciones del Asia Sudoriental (ASEAN), que ocupó Singapur en 2018. Ese año, la ASEAN se convirtió en la primera organización regional en suscribir en principio las 11 normas de carácter voluntario y no vinculante de comportamiento responsable de los Estados en el uso de las TIC. La ASEAN está elaborando un plan de acción para aplicar estas normas. Dentro de la ASEAN, Singapur también ha apoyado programas de desarrollo de capacidades. El Centro de Excelencia sobre Ciberseguridad de la ASEAN-Singapur se estableció en 2019 como un centro multidisciplinario para la creación de capacidades en áreas como las medidas de fomento de la confianza, la política, la estrategia, la legislación y las operaciones. Esperamos colaborar con los Estados Miembros para mejorar nuestros esfuerzos colectivos de creación de cibercapacidades.

Permítaseme concluir afirmando que una infraestructura digital segura debe sustentar nuestras ambiciones para la economía digital. Es más importante que nunca que los Estados Miembros aborden juntos el reto de la ciberseguridad, de forma sostenida, holística y coordinada. Singapur está dispuesta a trabajar con todos los países para crear asociaciones y cooperar en pos de un ciberespacio seguro, confiable, abierto e interoperable.

Anexo LVI

Declaración del Representante Permanente de Eslovaquia ante las Naciones Unidas, Michal Mlynár

Eslovaquia se adhiere a la declaración formulada por la Unión Europea. Quisiéramos añadir algunas observaciones a título nacional.

Me gustaría agradecerle a la Presidenta por organizar este debate oportuno que nos brinda la oportunidad de reflexionar sobre los crecientes riesgos que plantean las actividades maliciosas en el ciberespacio y su repercusión sobre la paz y la seguridad internacionales, así como abordar las iniciativas mundiales encaminadas a promover la paz y la estabilidad en el ciberespacio.

La crisis de enfermedad por coronavirus (COVID-19) ha hecho aún más pertinente y apremiante la necesidad de reforzar la seguridad y la estabilidad del ciberespacio. La crisis ha puesto de manifiesto que la capacidad digital se ha vuelto crucial para la prestación de servicios esenciales, así como para mantener una gobernanza eficaz. La disrupción del funcionamiento de la infraestructura crítica puede tener graves consecuencias. Las actividades cibernéticas maliciosas contra los sectores y servicios vitales tienen efectos desestabilizadores y pueden, en última instancia, amenazar la paz y la seguridad internacionales.

Dado que las ciberamenazas son, en gran medida, de carácter transnacional, es importante mantener la cooperación internacional y el diálogo entre los Estados, así como entre los Estados y la comunidad de partes interesadas. Nuestra responsabilidad compartida y los esfuerzos conjuntos de los Gobiernos, el sector privado y la sociedad civil son la manera de apoyar eficazmente el mantenimiento de la paz y la seguridad internacionales y de proteger los derechos humanos.

Las Naciones Unidas desempeñan una importante función a la hora de impulsar debates internacionales para fomentar la conciencia sobre las amenazas cibernéticas a la paz y la seguridad mundiales y de avanzar en la promoción del comportamiento responsable de los Estados en el ciberespacio.

Eslovaquia apoya firmemente el multilateralismo, que ayuda a gestionar y afrontar los desafíos actuales y futuros del ciberespacio. Estamos convencidos de que la estabilidad en el ciberespacio debe basarse en el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos. Eslovaquia apoya plenamente la aplicabilidad del derecho internacional vigente al comportamiento de los Estados en el ciberespacio, tal como se reconoce en los tres informes aprobados por consenso de los Grupos de Expertos Gubernamentales aprobados por la Asamblea General en 2010, 2013 y 2015. Haremos todo lo posible por mantener debates transparentes y constructivos, de modo que podamos beneficiarnos mutuamente de la experiencia, las buenas prácticas y los conocimientos de los demás.

Eslovaquia también es copatrocinadora del programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio dentro del Grupo de Trabajo de Composición Abierta. Creemos en un diálogo institucional inclusivo y constructivo centrado en los resultados, la regularidad y el enfoque basado en el

consenso. En nuestra opinión, la propuesta de programa de acción ofrece las bases para ese diálogo entre todos los miembros de las Naciones Unidas.

En lo que respecta a las medidas de fomento de la confianza y la creación de capacidades en el ciberespacio, Eslovaquia opina que estas dos son las medidas más importantes para mantener la estabilidad en el ciberespacio. Las organizaciones regionales, como la Organización para la Seguridad y la Cooperación en Europa, se han convertido en herramientas muy útiles en la prevención de conflictos y en el fortalecimiento de la cooperación entre los Estados. La comunicación e interacción periódicas entre los Estados en el ciberespacio contribuyen a evitar conflictos y a disminuir las posibles tensiones crecientes y, al mismo tiempo, crean una plataforma de diálogo.

El derecho internacional es uno de los pilares principales de la estabilidad y la previsibilidad en las relaciones entre los Estados. Eslovaquia apoya firmemente a quienes reafirman que el derecho internacional vigente, en particular la Carta de las Naciones Unidas en su totalidad y el derecho internacional humanitario y de los derechos humanos, se aplica a las acciones de los Estados en el ciberespacio. La Carta de las Naciones Unidas establece las normas y principios del derecho internacional de especial importancia para el mantenimiento de la paz y la estabilidad. No hay duda de que los derechos humanos se aplican en línea al igual que fuera de ella y los Estados deben respetar y defender esos derechos.

Gracias, Señora Presidenta.

Anexo LVII

Declaración de la Misión Permanente de Eslovenia ante las Naciones Unidas

Eslovenia ve con buenos ojos el primer debate abierto del Consejo de Seguridad, dedicado a una cuestión temática específica de la ciberseguridad. Abordar la ciberseguridad es oportuno y beneficioso para todos los Estados Miembros. Un debate abierto en el Consejo de Seguridad sobre este tema está contribuyendo a la sensibilización en el marco de la paz y la seguridad internacionales. A este respecto, Eslovenia se congratula de los informes recientes acordados por consenso por el Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional (Grupo de Trabajo de Composición Abierta) y el Grupo de Expertos Gubernamentales de las Naciones Unidas para promover un comportamiento responsable de los Estados en el ciberespacio.

Eslovenia se alinea la declaración de la Unión Europea y quisiéramos hacer algunas observaciones adicionales a título nacional.

Vivimos en un mundo interconectado y que cambia rápidamente. Un ciberespacio mundial, abierto, libre, estable y seguro contribuye a las prestaciones económicas y sociales. Sin embargo, también hay ciberactividades maliciosas. El uso indebido del ciberespacio puede afectar a sectores económicos vitales y a servicios esenciales para el público, como la sanidad y la energía, así como a otras infraestructuras básicas. Los propósitos maliciosos en el uso de las TIC por parte de actores estatales o no estatales pueden socavar la confianza entre los gobiernos, con implicaciones negativas que conducen a la desestabilización de la paz y la seguridad internacionales.

Para mitigar las amenazas vigentes y emergentes, Eslovenia cree firmemente que el ciberespacio debe regirse por el pleno respeto del derecho internacional vigente, en particular la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y los derechos humanos, así como la aplicación de normas y reglas para un comportamiento responsable de los Estados. Para ello, nuestro primer objetivo debe ser promover la aplicación del derecho internacional vigente y centrar nuestros esfuerzos colectivos en el avance de la aplicación de las normas vigentes de comportamiento responsable de los Estados, incluido el enjuiciamiento penal de las entidades privadas que operan desde la jurisdicción de un país.

Las normas de comportamiento responsable del Estado van de la mano de la política de fomento de la confianza y de las medidas de creación de capacidades. Aquí es donde podemos marcar una diferencia real. Eslovenia apoya firmemente, dentro del marco de los 53 Estados Miembros, la propuesta de establecer un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio. El programa de acción se basará en el acervo existente de la Asamblea General. El programa de acción ofrecerá la oportunidad de fomentar los programas de creación de capacidades y proporcionará un mecanismo institucional dentro de las Naciones Unidas para la cooperación y el intercambio de mejores prácticas y la cooperación con otras partes interesadas.

Asimismo, al implementar normas de comportamiento responsable de los Estados, Eslovenia seguirá promoviendo y apoyando la importancia de una perspectiva de género para reducir la "brecha digital de género" y promover una la participación plena, efectiva y significativa de las mujeres en los procesos de toma de decisiones relacionados con el uso de las TIC en el contexto de la seguridad internacional.

Eslovenia, que ocupará la presidencia del Consejo de la Unión Europea a partir del 1 de julio de 2021, reforzará la cooperación en el ámbito de la ciberseguridad y agilizará las cuestiones cibernéticas entre la Unión Europea y la región de los Balcanes Occidentales. Acercar los Balcanes Occidentales al ciberecosistema europeo es un elemento importante para crear un entorno confiable y seguro para el desarrollo digital, una mejor conectividad y un mejor acceso a la economía y la sociedad digitales. También es una contribución a la estabilidad mundial en el ciberespacio.

Para ello, Eslovenia tiene previsto organizar la Cumbre de la Unión Europea y de los Balcanes Occidentales, de carácter oficioso, a principios de octubre de 2021. También organizará una Conferencia de Ciberseguridad: el evento sobre los Balcanes Occidentales en cooperación con el EUISS. Además, contribuiremos a la revisión y al progreso de la cooperación con los Estados de los Balcanes Occidentales en el ámbito de la prevención e investigación de los abusos sexuales y la explotación de los niños.

Eslovenia, que ocupará la presidencia entrante del Consejo de la Unión Europea, también promoverá los esfuerzos normativos europeos para reforzar la ciberresiliencia y la gestión de las cibercrisis, con la revisión de la Directiva de la Unión Europea relativa a la seguridad de las redes y sistemas de información (Directiva SRI 2), en la que se esbozan medidas para lograr un alto nivel común de ciberseguridad en toda la Unión, así como los esfuerzos para promover activamente la aplicación del conjunto de instrumentos de ciberdiplomacia de la Unión Europea como medio para contribuir a la prevención de conflictos, la mitigación de las amenazas a la ciberseguridad y una mayor estabilidad en las relaciones internacionales. Vamos a esforzarnos por aumentar la cooperación internacional y reducir el riesgo de percepciones erróneas, escaladas y conflictos.

Permítaseme concluir reiterando que el Consejo de Seguridad desempeña un papel fundamental en el apoyo a los esfuerzos en el ámbito de la ciberseguridad, que son cruciales para mantener la paz y la seguridad internacionales. Con la organización de este debate abierto, ustedes ya han alentado de forma activa el fomento de un entorno que conduzca a la promoción de la cooperación, a la creación de confianza relacionada con las TIC y al ciberespacio mundial, abierto, libre, estable y seguro.

Anexo LVIII

Declaración de la Misión Permanente de Sudáfrica ante las Naciones Unidas

Sudáfrica ha recibido con interés de la convocatoria de este debate abierto del Consejo de Seguridad para considerar, por primera vez como cuestión temática específica, el mantenimiento de la paz y la seguridad internacionales en el ciberespacio. También agradecemos a la Alta Representante para Asuntos de Desarme, Sra. Nakamitsu, por su exposición informativa.

Además, hemos tomado nota de las preguntas orientativas que se han planteado para el debate de hoy, que trataremos de responder en nuestra declaración.

Ante todo, Sudáfrica desea subrayar que la cuestión de la paz y la seguridad en el ciberespacio es un asunto omnipresente y complejo que requiere el pleno compromiso de todos los Estados Miembros de las Naciones Unidas. Por este motivo, creemos que el lugar adecuado para tratar este asunto es dentro de los trabajos de la Primera Comisión de la Asamblea General, que ya se ha ocupado de esta cuestión.

A este respecto, los Estados Miembros se han comprometido a través del trabajo de una serie de Grupos de Expertos Gubernamentales, el último de los cuales se centró en el avance del comportamiento responsable de los Estados en el ciberespacio, produciendo su informe aprobado por consenso a finales de mayo de 2021 bajo la hábil dirección del Embajador Guilherme de Aguiar Patriota del Brasil.

Además, la amplia participación de todos los Estados Miembros se ha llevado a cabo 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 desde 2019, que aprobó su Informe aprobado por consenso a finales de marzo de 2021; y el recientemente creado Grupo de Trabajo de Composición Abierta sobre la Seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), que estará dirigido por el Embajador Burhan Gafoor, Representante Permanente de la República de Singapur, en calidad de Presidente.

Por lo tanto, los miembros de las Naciones Unidas han recorrido un largo camino en el debate sobre las amenazas emergentes a la paz y la seguridad internacionales en el ciberespacio; los marcos de derecho internacional que rigen este aspecto de la paz y la seguridad internacionales; las normas, reglas y principios que guían a los Estados Miembros; las medidas de fomento de la confianza necesarias; los requisitos de creación de capacidades; así como las formas de continuar el diálogo en este sentido.

Permítanme hacer las siguientes breves observaciones en este contexto.

Sudáfrica cree que la multitud de amenazas emergentes requiere el compromiso de todos los actores relevantes, incluidos la sociedad civil y el sector privado. Esto será necesario tanto para comprender la naturaleza de estas amenazas como para cooperar con toda la sociedad para sobre las amenazas que plantean los actores estatales y no estatales en el ciberespacio y hacerles frente adecuadamente.

Sudáfrica desea hacer hincapié en la necesidad de superar las brechas digitales y de género, así como en la transformación de la brecha digital en oportunidades

digitales, lo que será clave para crear resiliencia y, al mismo tiempo, fomentar un mayor desarrollo. Sin embargo, la creciente sofisticación de los incidentes dañinos de las TIC son una preocupación para los países en desarrollo como Sudáfrica.

Sudáfrica sigue preocupada por la creciente amenaza de los ciberataques a la infraestructura crítica y a la infraestructura de información crítica. Aunque creemos que debemos hacer frente a estas amenazas mediante una mayor cooperación y el desarrollo de mecanismos de mejores prácticas, estos esfuerzos deben apoyar las prioridades y los esfuerzos nacionales para identificar y designar dichas infraestructuras. También somos conscientes de que, a pesar de la exposición a las amenazas, las oportunidades económicas y sociales positivas que pueden derivarse de las TIC no deben quedar eclipsadas por el uso malicioso de estas tecnologías. Por lo tanto, no son las tecnologías en sí mismas las que preocupan, sino el mal uso de estas.

Para regir el uso del ciberespacio y, especialmente, las amenazas que supone para la paz y la seguridad internacionales, Sudáfrica apoya la aplicabilidad del derecho internacional y, concretamente, de la Carta de las Naciones Unidas en su totalidad.

En vista del importante trabajo ya realizado, creemos que debemos centrarnos en la aplicación de las normas, reglas y principios existentes. Es un principio fundamental compartido por los países en desarrollo que también debemos reconocer el hecho de que todos estamos en diferentes posiciones de riesgo, dadas las diferentes capacidades de los Estados para protegerse de las amenazas que plantean los actos maliciosos en el ciberespacio. Por lo tanto, mi delegación desea hacer hincapié en la necesidad de programas de creación de capacidades, tanto por parte del Estado como de otras partes interesadas, para ayudar a los países a combatir las amenazas desestabilizadoras de los actores maliciosos en el ciberespacio. Sudáfrica cree que la creación de capacidades es fundamental para que los Estados estén a la altura de la mejora de la seguridad del ciberespacio mundial, ya que se trata realmente de un desafío mundial que requiere soluciones mundiales.

Por último, Sudáfrica sigue comprometida con el compromiso para abordar estas cuestiones, especialmente en el contexto del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y su uso, que comenzará su labor sustantiva en diciembre. Esto servirá como un camino único para debatir cómo todos podemos abordar las amenazas emergentes, complejas y omnipresentes a la paz y la seguridad internacionales en el ciberespacio.

Anexo LIX

Declaración de la Misión Permanente de Suiza ante las Naciones Unidas

[Original: francés]

Quisiera expresar mi agradecimiento a Estonia por haber organizado este debate abierto, así como a la Alta Representante por su intervención. El ciberespacio ya forma parte integral de nuestras sociedades y crea inmensas posibilidades de desarrollo social y económico. Al mismo tiempo, las ciberoperaciones maliciosas presentan un riesgo de inestabilidad y se han convertido en una amenaza para la paz y la seguridad internacionales. Nos preocupa que el ciberespacio se instrumentalice para la proyección del poder militar y esté cada vez más fragmentado y desestabilizado.

Un ciberespacio abierto, seguro, estable, accesible y pacífico beneficia a todos. La Organización de las Naciones Unidas desempeña un papel crucial a este respecto. Suiza se congratula de la reciente aprobación por consenso de los informes del Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta. Estos informes representan hitos esenciales para un comportamiento responsable de los Estados en el ciberespacio.

Para promover la paz y la estabilidad en el ciberespacio, quisiera destacar algunos puntos:

En primer lugar, el derecho internacional se aplica al ciberespacio. Su observancia es una condición esencial para prevenir conflictos y mantener la paz y la seguridad internacionales. La obligación de resolver las controversias por medios pacíficos se aplica también a las actividades de los Estados en el ciberespacio. Además, el derecho internacional humanitario es aplicable cuando existe de facto un conflicto armado, internacional o no internacional. Suiza se congratula de que el último informe del Grupo de Expertos Gubernamentales indique esto claramente. Se trata de un paso significativo. El derecho internacional humanitario y sus principios fundamentales plantean importantes límites a la ejecución de ciberoperaciones en el contexto de los conflictos armados.

En segundo lugar, a Suiza le preocupa la repercusión humanitaria de las ciberoperaciones maliciosas, que van en aumento desde la pandemia y a menudo tienen como objetivo infraestructuras médicas. Suiza subraya que están protegidas, como se demostró durante el debate abierto en abril. Los informes del Grupo de Expertos Gubernamentales proporcionan un marco para proteger las infraestructuras críticas contra las actividades cibernéticas maliciosas. Además, deben protegerse los datos recopilados con fines humanitarios. Alentamos a los Estados a cumplir también las normas voluntarias de comportamiento responsable en el ciberespacio y las orientaciones complementarias del Grupo de Expertos Gubernamentales para su aplicación, con el fin de evitar daños a las infraestructuras críticas, mitigar la repercusión humanitaria y garantizar la protección de los civiles.

En tercer lugar, las medidas de fomento de la confianza son importantes para prevenir un clima de desconfianza en el ciberespacio. A nivel regional, Suiza se ha comprometido a promover el papel de la Organización para la Seguridad y la

Cooperación en Europa para fomentar la ciberestabilidad. Está elaborando, junto con Alemania, una propuesta de aplicación de una medida de fomento de la confianza que prevé consultas en el contexto de un ciberincidente grave. Suiza está comprometida también con la transparencia y la creación de capacidades. Nuestro Centro Nacional para la Ciberseguridad presta apoyo técnico a otros Estados en caso de incidente y comparte datos e información sobre las posibles amenazas. El Consejo de Seguridad y las organizaciones de las Naciones Unidas deberán tener en cuenta las iniciativas regionales y las medidas de fomento de la confianza que han resultado útiles para promover la paz y la estabilidad en el ciberespacio.

Por último, las organizaciones de la sociedad civil, el mundo académico y técnico y el sector privado desempeñan un papel importante en el apoyo a la ciberestabilidad internacional, en particular por lo que se refiere al respeto de los derechos humanos y las libertades fundamentales dentro y fuera de Internet. Suiza, en calidad de miembro de la Coalición para la Libertad en Línea, colabora con más de 30 Gobiernos y una red de partes interesadas para promover la libertad de expresión en Internet. Alentamos al Consejo de Seguridad y a los Estados Miembros a hacer partícipes a los distintos actores en la aplicación del marco para un comportamiento responsable de los Estados en el ciberespacio.

La cooperación multilateral y la adhesión al derecho internacional, incluidos el derecho internacional humanitario y el derecho internacional de los derechos humanos, son esenciales para la paz y la seguridad en el ciberespacio. Suiza alienta a seguir trabajando en estos temas, en particular en el marco del nuevo Grupo de Trabajo de Composición Abierta y el futuro Programa de Acción para la Promoción de un Comportamiento Responsable de los Estados en el Ciberespacio. Como candidata al Consejo de Seguridad, Suiza espera con interés mantener un diálogo constructivo entre múltiples interesados, sobre la base de los logros existentes.

Anexo LX

Declaración de la Misión Permanente de Tailandia ante las Naciones Unidas

Tailandia agradece los esfuerzos de Estonia por organizar el debate abierto de alto nivel del Consejo de Seguridad: “Mantener la paz y la seguridad internacionales en el ciberespacio” en esta coyuntura tan relevante y oportuna. También elogiamos el liderazgo de Estonia, que ha sido la primera en celebrar una reunión oficial del Consejo sobre ciberseguridad. Esperamos que la seguridad y la prevención del uso indebido del ciberespacio y de las tecnologías de la información y las comunicaciones (TIC) sigan ocupando un lugar destacado en la agenda del Consejo, al tiempo que seguimos celebrando la participación de todos los miembros de las Naciones Unidas en estos importantes debates.

Tailandia opina que el ciberespacio ha beneficiado a la humanidad, como se puso de manifiesto durante la pandemia, al mantener a las personas conectadas con los servicios sociales básicos y, lo que es más importante, entre sí, además de contribuir al logro de la Agenda 2030 para el Desarrollo Sostenible. Sin embargo, los usos de las TIC por parte de Estados y actores no estatales, incluidos los terroristas con fines maliciosos como los ataques a infraestructuras civiles críticas, no solo socavan la paz y la seguridad internacionales, sino que también afectan a la seguridad de nuestra población. Por lo tanto, es responsabilidad de los Estados, de acuerdo con las leyes y normas internacionales pertinentes, abordar estas cuestiones.

Tailandia cree que las Naciones Unidas pueden desempeñar un papel importante en el apoyo a los esfuerzos para la creación de un ciberespacio estable y seguro. De hecho, la seguridad del ciberespacio lleva más de dos décadas en la agenda de los Estados Miembros. Los éxitos más evidentes han sido las recientes e históricas adopciones, por consenso, del informe del Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (2019-2021) y del informe del Grupo de Expertos Gubernamentales sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional (Grupo de Expertos Gubernamentales) (2019-2021).

Tailandia aplaude el nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Confiamos en que, bajo la capaz dirección del Sr. Burhan Gafoor, Representante Permanente de Singapur y Presidente del Grupo de Trabajo de Composición Abierta, los Estados entablarán debates fructíferos, entre otros, sobre el aumento de la confianza, la cooperación y la transparencia entre los Estados y la elaboración ulterior de normas sobre el comportamiento responsable de los Estados en el ciberespacio.

En el nuevo Grupo de Trabajo de Composición Abierta, Tailandia espera que se resuelvan o aclaren las siguientes cuestiones: seguir desarrollando orientaciones y recomendaciones sobre cómo hacer operativas las normas de comportamiento responsable de los Estados; llegar a un entendimiento común sobre cómo se aplica el derecho internacional en el ciberespacio y si existen brechas; crear medidas

sostenibles de fomento de la confianza basadas en la demanda, y adoptar un “Diálogo Institucional Regular”.

Tailandia también toma nota de los buenos esfuerzos de otros organismos intergubernamentales, del sector privado y de las organizaciones y procesos de la sociedad civil que han contribuido a nuestro esfuerzo colectivo en pos de un ciberespacio seguro y protegido. Tailandia apoya el enfoque multipartito en nuestro trabajo para garantizar la participación significativa de las partes interesadas y los asociados pertinentes de la sociedad, incluida la de las mujeres y los jóvenes.

Para ello, Tailandia apoya el fortalecimiento de las bases normativas mediante la mejora de la aplicación práctica de las normas acordadas, la superación de las divergencias existentes y las necesidades de capacidad, y la garantía de que los canales multilaterales y bilaterales existentes se mantengan abiertos para lograr un diálogo continuo. Todos los Estados deben seguir trabajando en conjunto para salvaguardar nuestra visión compartida de un ciberespacio y un entorno de TIC abierto, seguro, accesible y pacífico para todos.

Anexo LXI

Declaración de la Misión Permanente de Turquía ante las Naciones Unidas

Me gustaría agradecer a Estonia por organizar este debate abierto, que se centra en un tema crítico especialmente en las circunstancias actuales debido a la pandemia. También agradezco a la Alta Representante para Asuntos de Desarme, Señora Nakamitsu, por su exposición informativa.

El uso de las tecnologías de la información y las comunicaciones (TIC) repercute en la economía y el desarrollo en todo el mundo. La pandemia ha puesto de manifiesto nuestra gran dependencia de las tecnologías digitales. Garantizar un acceso libre, abierto y seguro a las TIC es, sin duda, crucial.

Turquía está preocupada por el creciente número de ciberataques. Las ciberactividades maliciosas dirigidas a la infraestructura crítica, el terrorismo, el espionaje digital, el fraude, el maltrato y la explotación infantil en línea y el uso indebido de datos personales son algunas de las amenazas actuales que también plantean un riesgo para la paz y la seguridad internacionales.

Debido a los avances tecnológicos, los ciberataques se han vuelto más fáciles de llevar a cabo, mientras que los efectos negativos y el costo para las víctimas aumentan rápidamente. Los ciberataques también se están volviendo más “orientados al objetivo”. El costo anual de los ciberataques está aumentando exponencialmente. La defensa contra estos ataques requiere métodos e instrumentos nuevos y actualizados.

Turquía ve con buenos ojos los informes de consenso del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional y recientemente, del Grupo de Expertos Gubernamentales de las Naciones Unidas para promover un Comportamiento Responsable de los Estados en el Ciberespacio. Estos informes son valiosas contribuciones al conjunto de trabajos vigente sobre ciberseguridad bajo la protección de las Naciones Unidas. Es igualmente importante que los informes del Grupo de Trabajo Abierto y del Grupo de Expertos Gubernamentales sean compatibles y complementarios para aumentar la estabilidad, la resiliencia y la cooperación internacional en el ciberespacio. Esperamos ver una mayor cohesión en estos esfuerzos de ahora en adelante.

Con su rápido ritmo de digitalización, Turquía se ha centrado en tomar las medidas necesarias para mejorar su ciberseguridad nacional. Actualmente, se está aplicando la Estrategia Nacional de Ciberseguridad y el Plan de Acción, que abarca el período 2020-2023. Los principales objetivos estratégicos de este Plan de Acción son la protección de infraestructura crítica y el aumento de la resiliencia, la creación de capacidades, la red de ciberseguridad orgánica, la seguridad de las tecnologías de nueva generación (es decir, IoT, 5G, computación en la nube, etc.), la lucha contra la ciberdelincuencia, el desarrollo y el fomento de las tecnologías nacionales e internas, la integración de la ciberseguridad en la seguridad nacional y la mejora de la cooperación internacional.

Además, el Equipo Nacional de Respuesta a Ciberemergencias de Turquía desempeña un papel fundamental en la aplicación y coordinación de medidas preventivas contra las ciberamenazas.

Los programas de formación y los ejercicios de ciberseguridad nacionales e internacionales complementan nuestros esfuerzos. La Autoridad de Tecnologías de la Información y las Comunicaciones (BTK) de Turquía ofrece programas de formación abiertos al público y en línea sobre ciberseguridad y otras áreas relacionadas. Más de 5.000 personas han sido capacitadas en diferentes ámbitos de la ciberseguridad en los últimos cuatro años.

El “Día de Internet Segura”, organizado anualmente, es una de las actividades de sensibilización de la BTK, cuyo objetivo es aumentar la conciencia sobre el uso consciente y seguro de Internet. Además, Turquía toma medidas para contrarrestar el aumento de los riesgos de seguridad digital para la ciberseguridad y ha tomado medidas en cooperación con las partes interesadas pertinentes, con el fin de garantizar la continuidad del negocio, la accesibilidad y la protección de los consumidores durante la pandemia.

También hemos adoptado para reforzar nuestro marco legislativo nacional.

Dada la naturaleza transfronteriza de los ciberriesgos, es crucial aumentar la cooperación internacional. Con este entendimiento, Turquía participa en el intercambio de información sobre ciberamenazas y contribuye a las políticas y estrategias de cooperación en organizaciones regionales e internacionales, incluida la Organización para la Seguridad y la Cooperación en Europa, el G20 y la OCDE. Turquía también participa en ejercicios internacionales, incluidos los de la UIT y la OTAN.

Las Naciones Unidas tienen un papel central en el logro de una cooperación más estratégica y eficaz en el uso de las TIC por parte de los Estados. Turquía apoya la aplicabilidad del derecho internacional en el ciberespacio. Ya es hora de que nos basemos en el trabajo previo realizado en el sistema de las Naciones Unidas y encontremos formas significativas de hacer operativas las reglas, normas, principios y recomendaciones para lograr un comportamiento responsable de los Estados en el ciberespacio.

Un área prioritaria para nuestro trabajo futuro es forjar un entendimiento común sobre cómo se aplica el derecho internacional en el ciberespacio. Esto es realmente necesario para disminuir los malentendidos y promover la rendición de cuentas en el ciberespacio.

También es necesario establecer canales de comunicación entre los Estados Miembros en situaciones de emergencia y compartir información y recursos a través de esos canales. Esto contribuiría en gran medida a la creación de capacidad y aceleraría nuestros esfuerzos en la creación de capacidades.

Además, también tenemos que revisar y reforzar urgentemente los instrumentos internacionales vigentes para mejorar la cooperación en el marco de las nuevas tecnologías, como la computación en la nube, Internet de las cosas, 5G y la inteligencia artificial.

Realizar un estudio sobre los enfoques normativos nacionales para garantizar la seguridad de las nuevas tecnologías y preparar códigos de conducta para orientar e

informar los marcos nacionales pueden ser herramientas útiles. Además, tenemos que llegar a un entendimiento común y a definiciones de las amenazas.

En el contexto de la creación de capacidades, creemos que tanto las Naciones Unidas como las organizaciones regionales pueden promover programas de intercambio de expertos en ciberseguridad y establecer plataformas comunes de formación. Deben fomentarse los ejercicios internacionales para mejorar las capacidades nacionales de preparación y respuesta ante los ciberincidentes.

Dado que el ciberespacio es un campo sin fronteras y la ciberseguridad es una cuestión que afecta a múltiples partes interesadas, las autoridades nacionales deben colaborar con los usuarios, el sector privado, las ONG y sus homólogos internacionales para luchar contra las ciberamenazas. Los vendedores mundiales, los proveedores de servicios y las empresas de seguridad también deberían cooperar de forma más eficaz con los gobiernos y las organizaciones internacionales para contribuir a la ciberseguridad mundial.

Turquía se compromete a mantener su compromiso y el diálogo para promover la ciberseguridad regional y mundial.

Anexo LXII

Declaración de la Misión Permanente de Ucrania ante las Naciones Unidas

Damos las gracias a Estonia por haber propiciado una reunión tan importante del Consejo de Seguridad, así como a la Sra. Nakamitsu, Alta Representante para Asuntos de Desarme, por su exposición informativa.

El rápido desarrollo de las tecnologías de la información y las comunicaciones ha derivado progresivamente en la "reformulación" del espacio de Internet: hoy en día ya no es una plataforma cómoda para la comunicación, sino también un arma real, que se vuelve cada vez más peligrosa en manos de piratas informáticos, delincuentes, algunos actores estatales y sus apoderados.

Desgraciadamente, a pesar de las normas legales vigentes y de los mecanismos institucionales establecidos para combatir los ciberdelitos a nivel nacional, regional e internacional, se abusa con demasiada frecuencia de las ventajas del mundo digital moderno, con el aumento de los ciberataques, que se han convertido en un nuevo método de guerra híbrida.

La política internacional es cada vez más vulnerable a las ciberamenazas. En los últimos años, varios Estados del mundo se han convertido en objetivos lucrativos de los ciberataques.

Ucrania es el Estado donde los ciberataques desde 2014 se convirtieron en uno de los principales elementos del intento externo de socavar nuestra soberanía. En el período 2014-2021, Ucrania se ha enfrentado a un número sin precedentes de ciberoperaciones contra objetos vitales de nuestra infraestructura crítica. La mayoría de estos ataques fueron realizados por grupos de hackers controlados desde la Federación de Rusia.

Las operaciones cibernéticas contra las principales instalaciones de infraestructura crítica, los sectores de la energía, el transporte, el petróleo y el gas son desafíos y amenazas a la paz y la seguridad internacionales. Recientemente, Colonial Pipeline ha sido objeto de un ciberataque que ha afectado gravemente a los equipos informáticos que gestionan el oleoducto, lo que ha tenido graves consecuencias.

En tiempos de la pandemia de enfermedad por coronavirus (COVID-19), el impacto devastador de las ciberoperaciones maliciosas es evidente. Algunos actores estatales y no estatales abusan de la crisis mundial para lanzar ciberoperaciones, incluso contra el sector de la salud, lo que constituye una preocupación urgente para la comunidad internacional.

Sin embargo, no solo la infraestructura crítica, sino también la política internacional es cada vez más vulnerable al uso malicioso de unas capacidades de las TIC cada vez más complejas y sofisticadas, lo que ha sido confirmado por los casos de interferencia en las principales campañas electorales y en los perfiles de los candidatos cometidos por los hackers del Kremlin.

Por lo tanto, la ciberestabilidad se ha convertido en un componente crucial para garantizar la paz y la seguridad en general, que requiere una estricta adhesión al derecho internacional, cuya aplicación en el ciberespacio se ha reafirmado

recientemente en los informes del Grupo de Trabajo de Composición Abierta y del Grupo de Expertos Gubernamentales, la aplicación adecuada de normas, reglas y principios de comportamiento responsable, así como el fortalecimiento de la cooperación internacional para preservar un ciberespacio libre, abierto, estable y seguro.

Hacemos hincapié en que debe prestarse especial atención a la elaboración de normas unificadas para combatir las ciberamenazas, a compartir las mejores prácticas, a fomentar la confianza mutua en el ámbito de la ciberseguridad, a prevenir el uso del ciberespacio con fines políticos, terroristas y militares, así como a proporcionar asistencia financiera y técnica para mejorar las capacidades nacionales al resistir las ciberamenazas, mitigar los riesgos y reforzar la resiliencia.

A día de hoy, las ciberoperaciones contra la infraestructura crítica y los organismos gubernamentales, así como las campañas de desinformación, que pueden incitar al terrorismo, son un método muy utilizado para interferir en los asuntos internos de Estados soberanos, incluida Ucrania.

Sin duda, Rusia utiliza las altas tecnologías para conseguir sus propios objetivos políticos y geopolíticos, concretamente apoyando y exacerbando los conflictos en los Estados vecinos con agresivas guerras de información.

Alentamos encarecidamente a la comunidad internacional a que considere a fondo la cuestión de la responsabilidad en los casos de identificación de un Estado o de actores estatales concretos que estén detrás de la preparación o el ejercicio del uso malicioso selectivo de las TIC o de la difusión de mentiras con fines hostiles.

Después de todo, los esfuerzos internacionales realizados en este ámbito son simplemente vanos si no existen mecanismos confiables para detectar, castigar y llevar ante la justicia a los individuos y a los Estados pertinentes, responsables de coordinar y financiar actividades ilícitas en el ciberespacio mundial.

Anexo LXIII

Declaración de la Misión Permanente de los Emiratos Árabes Unidos ante las Naciones Unidas

La pandemia de enfermedad por coronavirus (COVID-19) ha puesto de relieve cuánto depende el mundo de las tecnologías de la información y las comunicaciones, que fueron esenciales para mantenernos informados y conectados entre nosotros, incluso cuando estábamos físicamente separados.

Durante los últimos dieciocho meses, hemos sido testigos de una tendencia en aumento de ciberoperaciones maliciosas dirigidas a instalaciones médicas, incluidas las organizaciones dedicadas a la investigación y al desarrollo de vacunas para combatir la COVID-19. Vivimos en una región volátil, y Oriente Medio no es inmune al riesgo que plantea la ciberactividad maliciosa: suele ser el objetivo de importantes ciberoperaciones y espionaje. En los últimos años, nuestra región ha sido testigo de graves incidentes que han afectado a los sectores bancario, público y de las telecomunicaciones. Las instalaciones de petróleo y gas natural también han sido objeto de ataques, y esto ha causado cientos de millones en daños. Esta actividad cibernética maliciosa en la infraestructura crítica de la región puede desencadenar un conflicto en un entorno ya tenso y plantear una amenaza para la paz y la seguridad internacionales.

Los Emiratos Árabes Unidos se comprometen a crear la infraestructura y los mecanismos necesarios para mejorar sus capacidades de ciberseguridad, tanto para protegerse a sí mismos contra las ciberamenazas como para trabajar mejor con otros para abordar los desafíos compartidos. En noviembre de 2020, creamos el Consejo de Ciberseguridad de los Emiratos Árabes Unidos, que desarrollará una estrategia nacional integral de ciberseguridad y un plan nacional de respuesta a ciberincidentes. Acogemos las mayores conferencias sobre ciberseguridad y transformación digital, como GITEX, GISEC y Cybertech, para crear capacidad nacional, y hemos desarrollado una plataforma de alianza público-privada para facilitar el intercambio de información. También colaboramos con Estados, organizaciones internacionales y entidades del sector privado para compartir información tanto a nivel político como técnico. Por ejemplo, los Emiratos Árabes Unidos contribuyen al trabajo de las organizaciones regionales, como la nueva plataforma conjunta de análisis de programas maliciosos del Consejo de Cooperación del Golfo, y son un miembro activo del Equipo de Respuesta a Emergencias Informáticas de la Organización de Cooperación Islámica (OCI-EREI). Estas medidas de fomento de la confianza de cooperación y transparencia son algunas de las formas en que los Emiratos Árabes Unidos están haciendo su parte para reducir los ciberriesgos para la paz y la seguridad internacionales.

Los Emiratos Árabes Unidos celebran las recomendaciones de los informes del Grupo de Trabajo de Composición Abierta sobre las TIC y del Grupo de Expertos Gubernamentales, que subrayan la importancia de apoyar los esfuerzos para fomentar la aplicación de las normas voluntarias de comportamiento responsable de los Estados en el ciberespacio, así como la necesidad de desarrollar entendimientos comunes sobre la aplicabilidad del derecho internacional a la actividad en línea. Sin embargo, es necesario hacer más, tanto para alentar y apoyar a los Estados en la aplicación de las recomendaciones como para proporcionar más orientación en un entorno que

evoluciona rápidamente. El programa de acción para el comportamiento responsable de los Estados en el ciberespacio constituye una hoja de ruta ideal para los trabajos futuros y contribuirá a abordar los ciberriesgos para la paz y la seguridad internacionales.

Minimizar el ciberriesgo para la paz y la seguridad internacionales seguirá siendo un desafío. Los Emiratos Árabes Unidos proponen dos recomendaciones que pueden ayudar en esta tarea.

En primer lugar, los Estados deben proporcionar formación y creación de capacidades a nivel bilateral, regional e internacional, incluso mediante programas de formación y el desarrollo de orientaciones para ayudar a aplicar las normas de comportamiento responsable de los Estados. Estas acciones pueden actuar como medidas de fomento de la confianza, respondiendo a la desconfianza y los malentendidos entre los Estados en el ciberespacio, que pueden plantear un riesgo para la paz y la seguridad internacionales.

En segundo lugar, los Estados deben seguir compartiendo sus opiniones y evaluaciones con el Secretario General y participar activamente en los foros internacionales relacionados con la cibernética y en los formatos interregionales. La puesta en común de las mejores prácticas y los intercambios de experiencias pueden ayudar a los Estados a adaptarse a la evolución de las normas y a convertirse en actores responsables en el ciberespacio.

Todos los Estados tienen la responsabilidad de promover la paz y la seguridad internacionales, tanto en línea como fuera de línea. El mejor punto de partida es el cumplimiento de las normas de comportamiento responsable de los Estados, junto con las obligaciones derivadas del derecho internacional.