Naciones Unidas A/C.1/77/PV.19

Asamblea General
Septuagésimo séptimo período de sesiones

Documentos oficiales

Primera Comisión
19ª sesión plenaria
Lunes 24 de octubre de 2022, a las 15.00 horas
Nueva York

Presidencia: Sr. Pieris . . . . . (Sri Lanka)

Se abre la sesión a las 15.05 horas.

Temas 90 a 108 del programa (*continuación*)

Debate temático sobre cuestiones concretas y presentación y examen de los proyectos de resolución y de decisión presentados en relación con los temas del programa relativos al desarme y a la seguridad internacional

El Presidente (*habla en inglés*): La Primera Comisión continuará sus debates temáticos en relación con el grupo temático “Otras medidas de desarme y seguridad internacional”. Las delegaciones que deseen ejercer el derecho a contestar podrán hacerlo una vez que la Comisión haya agotado la lista de intervenciones sobre ese grupo. Si el tiempo lo permite, la Comisión comenzará esta tarde el examen del grupo temático “Desarme y seguridad regionales”.

Antes de comenzar, quisiera recordar a las delegaciones que durante el segmento temático las declaraciones se limitarán a cinco minutos cuando intervengan en nombre de su país y a siete minutos cuando lo hagan en nombre de varias delegaciones.

Sr. Lagardien (Sudáfrica) (*habla en inglés*): Sudáfrica se adhiere a la declaración formulada por la representación de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

Sudáfrica apoyó los resultados de 2021 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 del primer Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. No obstante, es importante permanecer unidos en torno a un único proceso, y esperamos con interés la labor de las sesiones cuarta y quinta del segundo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. En este sentido, felicitamos a los Estados Miembros por haber aprobado por consenso el informe anual de 2022 del Grupo de Trabajo de composición abierta sobre los progresos realizados (véase A/77/275) y esperamos llegar a un entendimiento común sobre la seguridad de las tecnologías de la información y las comunicaciones.

Sudáfrica sigue preocupada por la amenaza cada vez mayor que suponen los ciberataques para la infraestructura crítica y la infraestructura de la información. Aunque consideramos que debemos hacer frente a estas amenazas mediante una mayor cooperación y el desarrollo de mecanismos de mejores prácticas, debemos apoyar las prioridades y los esfuerzos nacionales que tienen como objetivo identificar y designar dichas infraestructuras. Los Estados, especialmente los países en desarrollo, se encuentran en distintos niveles de riesgo, dadas las diferentes capacidades de los Estados para responder a las amenazas que plantean los actos malintencionados en el ciberespacio. En ese contexto, Sudáfrica valora la importancia tanto de la aplicación como del desarrollo ulterior de las normas vigentes. Mi delegación da prioridad a la aplicación, que, a nuestro juicio, ayudará a comprender mejor las carencias de las normas

vigentes, si las hay, y de ese modo proporcionará información sobre la necesidad de elaborar nuevas normas. La aplicación es también una oportunidad para determinar prácticas eficaces y necesidades de capacitación.

Sudáfrica acoge con satisfacción los esfuerzos para elaborar un programa de acción como parte de la labor del Grupo de Trabajo de Composición Abierta. Esperamos que, a través de nuestros debates sobre la seguridad de las tecnologías de la información y las comunicaciones en el Grupo de Trabajo de Composición Abierta, podamos llegar a un entendimiento común sobre las amenazas y la vulnerabilidad de los Estados que deberán abordarse en dicho programa de acción. Aunque Sudáfrica apoya desde hace tiempo su elaboración, opinamos que el Grupo de Trabajo de Composición Abierta sigue siendo el foro adecuado para elaborar dicho programa de acción y su establecimiento. Por lo tanto, recordamos la recomendación incluida en el informe anual del Grupo de Trabajo de Composición Abierta sobre los progresos realizados de que se siga elaborando el programa de acción con miras a su posible establecimiento como mecanismo para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones, lo cual, entre otras cosas, apoyaría las capacidades de los Estados para cumplir sus compromisos relativos al uso de dichas tecnologías.

También consideramos que la colaboración de todos los agentes relevantes, incluidos la sociedad civil y el sector privado, para comprender el carácter de las amenazas y cooperar y responder adecuadamente, con toda la sociedad, frente a las amenazas que plantean los agentes estatales y no estatales, enriquecería este proceso impulsado por los Estados Miembros.

Sr. Röethlin (Austria) (*habla en inglés*): Austria se adhiere plenamente a la declaración formulada en nombre de la Unión Europea (véase A/C.1/77/PV.18). Deseo formular las siguientes observaciones en representación de nuestro país.

Desde el anterior debate dedicado a este grupo temático, en 2019, la importancia de la ciberseguridad ha aumentado considerablemente. Por desgracia, también hemos constatado el enorme daño que puede causar el comportamiento irresponsable e ilegal en el ciberespacio. Un ejemplo de ello son los ciberataques ilegales que se cometieron paralelamente a la invasión rusa de Ucrania, que no solo afectaron a ese país, sino también a otros por sus efectos indirectos.

Por ello, acogemos con agrado que las Naciones Unidas presten una mayor atención a la cuestión de la ciberseguridad y celebramos la importante labor que ha llevado a cabo el Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, que ha concluido en forma satisfactoria su primer año de deliberaciones con la aprobación de un informe sobre los progresos realizados (véase A/77/275), que se espera que la Comisión apoye por consenso. El informe y sus recomendaciones sientan las bases para la labor futura del Grupo. Acogemos con satisfacción la participación activa de diversas partes interesadas en el Grupo de Trabajo de Composición Abierta, pero también lamentamos que un gran número de interesados clave del sector, el mundo académico y la sociedad civil no hayan podido participar en su labor debido a vetos sin justificación. No podemos trabajar en el ámbito de la ciberseguridad sin interactuar con las partes interesadas que indudablemente le dan forma.

Austria seguirá abogando por un ciberespacio abierto, libre, estable y seguro, sobre la base de la plena aplicabilidad del derecho internacional, incluidos el derecho internacional humanitario y el derecho internacional de los derechos humanos, en un marco para el comportamiento responsable de los Estados en el ciberespacio, que ha sido aprobado por consenso.

Aún queda mucho por hacer, especialmente en lo que se refiere al alcance exacto de la aplicabilidad del derecho internacional, a la creación de capacidades y a las medidas de fomento de la confianza. Seguiremos esforzándonos con ese fin en el Grupo de Trabajo de Composición Abierta y esperamos que sea posible examinar las buenas prácticas existentes en esos ámbitos, por ejemplo, a través de intercambios con organizaciones regionales en el marco del propio grupo. Estamos convencidos de que un programa de acción puede ser un instrumento ideal para avanzar en la implementación del marco normativo, razón por la cual apoyamos el proyecto de resolución (A/C.1/77/L.73) relativo al programa de acción presentado por Francia.

Nos alienta observar que en los proyectos de resolución sobre este grupo temático se abarcan aspectos importantes de la labor en materia de desarme y seguridad internacional que se han descuidado durante demasiado tiempo. Me referiré brevemente a dos cuestiones.

En primer lugar, acogemos con agrado los importantes y cada vez mayores esfuerzos que en los últimos años ha venido realizando la Oficina de Asuntos de Desarme en la esfera de la educación para el desarme. En momentos en que las tensiones mundiales aumentan, es cada vez

más importante dar a conocer nuestra labor. Eso fomentará la concienciación y nos ayudará a formar a las próximas generaciones de expertos que tendrán a su cargo la realización de una labor vital en los asuntos de desarme.

En segundo lugar, en los últimos años el mundo no solo se ha enfrentado a conflictos armados, sino también a una pandemia mundial y a las consecuencias cada vez más graves del cambio climático. Sin embargo, la asignación de recursos entre estos tres polos de crisis no ha sido equitativa. Queremos reiterar el llamamiento que ya hicimos el año pasado para que abandonemos la idea peligrosa y errónea de que la seguridad solo se puede garantizar mediante el armamento militar. Las crisis no militares que estamos presenciando deberían ser una llamada de atención que nos lleve a tener una comprensión más amplia de la seguridad y a integrar mejor los instrumentos y medidas del desarme en todos los esfuerzos encaminados a consolidar y mantener la seguridad.

Sr. De Martin Topranin (Italia) (*habla en inglés*): Italia se suma a la declaración formulada en nombre de la Unión Europea (véase A/C.1/77/PV.18) y desea añadir las siguientes observaciones en nombre del país.

El desarrollo tecnológico y el progreso científico son fundamentales para el bienestar de la humanidad y deben ser considerados como un instrumento para promover la paz y el crecimiento sostenible. Las tecnologías de la información y las comunicaciones (TIC) e Internet se encuentran entre los mayores logros humanos de todos los tiempos y ofrecen oportunidades sin precedentes. Al trabajar en la esfera del desarme y la seguridad, tenemos la gran responsabilidad de garantizar que haya un marco adecuado para hacer posibles esos avances y evitar cualquier uso peligroso o negativo.

La cooperación internacional es crucial para el logro de ese objetivo, y necesitamos mejorar el diálogo, la transparencia y las medidas de fomento de la confianza para entender mejor los desafíos comunes que debemos afrontar. Italia sigue respaldando el concepto de la ciberestabilidad, a la vez que apoya los esfuerzos de la comunidad internacional en pro de un ciberespacio sustentando en la aplicabilidad y en el respeto del derecho internacional en su totalidad, empezando por la Carta de las Naciones Unidas y el derecho internacional humanitario y terminando por el derecho internacional de los derechos humanos.

Respaldamos resueltamente la labor que viene realizando el Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, y celebramos la conclusión satisfactoria de su tercer período de sesiones sustantivo, con la aprobación por consenso de un informe anual sobre los progresos realizados. Por consiguiente, apoyamos plenamente el proyecto de decisión presentado por Singapur, en nombre de la Presidencia, que tiene por objeto aprobar dicho informe (véase A/77/275) por consenso. Como firmes partidarios del multilateralismo y de unos métodos de trabajo que garanticen la inclusividad y se basen en el acervo existente, consideramos que hay que aprovechar al máximo los debates que se llevarán a cabo sobre esa cuestión. El diálogo institucional tiene que ser ordenado, previsible e inclusivo a fin de que podamos avanzar de forma constructiva y de que podamos ser conscientes de los tiempos y eficientes en la gestión de las finanzas.

Es importante reconocer que, junto con la intensificación y evolución de las TIC, también han aumentado las amenazas. Esa es otra cuestión esencial en la que el Grupo de Trabajo de Composición Abierta debería centrar su labor, sobre todo en lo que respecta a la ciberresiliencia de la infraestructura digital y a las amenazas que plantea el uso de la cibernética en los conflictos armados. Esas cuestiones son particularmente urgentes en el complejo entorno geopolítico actual y tras la guerra de agresión no provocada e injustificada de Rusia contra Ucrania.

Ese brutal acto ha servido para poner de relieve hasta qué punto las actividades fundamentales de las sociedades conectadas dependen de la infraestructura digital, en particular de la infraestructura de telecomunicaciones, y de las vulnerabilidades que ello implica. Por eso, Italia subraya la importancia de proteger la infraestructura digital frente a injerencias malintencionadas e insta a todos los agentes a que contribuyan de forma prioritaria a la resiliencia de la infraestructura de la información, las comunicaciones y las telecomunicaciones. Eso es esencial para garantizar el acceso a Internet a escala mundial, lo que garantiza el acceso a la información, incluida la información que puede salvar vidas y empresas.

Estamos decididos a aumentar la ciberresiliencia de la infraestructura digital, mejorando y compartiendo la información para generar conciencia sobre las ciberamenazas y ampliando nuestra ciberrespuesta coordinada en consonancia con nuestros marcos de ciberseguridad y seguridad nacional, así como con las iniciativas de fomento de la cooperación y las alianzas actuales y futuras.

El ámbito cibernético ha demostrado ser un contexto muy dinámico, y creemos que es necesario seguir

trabajando para traducir nuestro debate en medidas tangibles que mejoren la cooperación internacional en materia de ciberseguridad. En ese sentido, Italia apoya la propuesta de establecer un programa de acción sobre la promoción del comportamiento responsable en el ciberespacio como iniciativa necesaria que complemente una agenda orientada a la acción (A/C.1/77/L.73). Ese proceso debe ser y será un proceso inclusivo que estará impulsado por los Estados Miembros de las Naciones Unidas. Consideramos que, en esta coyuntura tan delicada, debemos unirnos y dar una dimensión operacional a nuestro diálogo institucional.

Por ese motivo, apoyamos plenamente el programa de acción cibernética y encomiamos que se trate de un proyecto muy sensato, inclusivo y equilibrado que puede proporcionarnos un diálogo operacional centrado en la aplicación, sobre la base de nuestro acervo. Hablando de acción, permítaseme subrayar que la creación de capacidades es crucial para lograr un ciberespacio seguro.

Sr. Shin (Federación de Rusia) (*habla en ruso*): Para comenzar, nos gustaría subrayar una vez más que la Federación de Rusia siempre ha promovido una agenda unificadora en la esfera del control de armamentos, el desarme y la no proliferación. Presentamos el proyecto de resolución A/C.1/77/L.66, titulado “Fortalecimiento y desarrollo del sistema de tratados y acuerdos sobre el control de armamentos, el desarme y la no proliferación”. Esperamos que se apruebe por consenso y tenga un efecto positivo en la cooperación constructiva en toda la gama de cuestiones relacionadas con la paz y la seguridad internacionales.

En relación con el tema 94 del programa, a iniciativa de la Federación de Rusia y con el apoyo abrumador de los Estados Miembros de las Naciones Unidas, en 2020 se creó el Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones (TIC) y de su uso (2021-2025). El Grupo de Trabajo de Composición Abierta es el único mecanismo de negociación sobre esas cuestiones en el sistema de las Naciones Unidas. Ese formato debe valorarse porque permite a todos los Estados, sin excepción, participar de manera directa en el proceso de adopción de decisiones sobre cuestiones que afectan a la seguridad nacional y debatir todas las iniciativas pertinentes de los Estados sobre una base verdaderamente democrática, abierta y transparente.

En ese contexto, acogemos con agrado y compartimos las muestras de apoyo al Grupo de Trabajo de Composición Abierta expresadas por la representación de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18), la representación de Filipinas en nombre de la Asociación de Naciones de Asia Sudoriental (véase A/C.1/77/PV.18), la representación de Belice en nombre de la Comunidad del Caribe (véase A/C.1/77/PV.18) y la representación del Iraq en nombre del Grupo de los Estados Árabes (véase A/C.1/77/PV.18), así como la voluntad de esas entidades de seguir trabajando de manera constructiva en ese formato.

En su primer año de trabajo, el 29 de julio, el Grupo de Trabajo de Composición Abierta aprobó su informe anual sobre los progresos realizados (véase A/77/275), que contiene importantes disposiciones que permiten crear una base para el desarrollo de un régimen jurídico internacional que regule el uso de las TIC y fomente la cooperación interestatal en ese ámbito. La Federación de Rusia considera que es esencial no solo consolidar el éxito ya alcanzado, sino también que el Grupo de Trabajo de Composición Abierta se centre en la celebración de nuevas negociaciones constructivas con miras a acordar medidas específicas destinadas a fortalecer la paz y la seguridad en el espacio de la información y abordar cuestiones relativas al desarrollo digital.

Con ese fin, Rusia presentó el proyecto de resolución A/C.1/77/L.23/Rev.1, titulado “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, cuyas versiones anteriores ha presentado nuestro país anualmente desde 1998. El proyecto de resolución A/C.1/77/L.23/Rev.1 es universal, no conflictivo y no politizado. Complementa el proyecto de decisión A/C.1/77/L.54, presentado por Singapur, por el que se aprueba el informe anual sobre los progresos realizados del Grupo de Trabajo de Composición Abierta y se acogen con agrado los esfuerzos de la Presidencia del Grupo, que apoyamos plenamente. El proyecto de resolución A/C.1/77/L.23/Rev.1 se basa en las disposiciones de resoluciones que ya había aprobado la Asamblea General, así como en los informes de consenso del primer Grupo de Trabajo de Composición Abierta y del actual. El objetivo es salvaguardar al Grupo como la principal plataforma de negociación que se ocupa de toda la gama de cuestiones propias de la seguridad de la información internacional bajo los auspicios de las Naciones Unidas y evitar su fragmentación en formatos paralelos que se dupliquen entre sí. Esa es la aspiración de la comunidad internacional en general, y el Grupo representa su consecución.

El proyecto de resolución A/C.1/77/L.23/Rev.1 confirma el anterior acuerdo consensuado de seguir perfeccionando en el marco del Grupo de Trabajo de

Composición Abierta todas las iniciativas nacionales relativas a la seguridad en el uso de las TIC. En el proyecto de resolución están contenidas propuestas específicas sobre la creación de capacidades en el uso de las TIC y se confirma la necesidad de adoptar una decisión sobre el futuro formato del diálogo institucional periódico sobre esas cuestiones sobre una base verdaderamente universal, en el seno del Grupo existente. Además, cualquier mecanismo de este tipo solo se pondrá en marcha una vez concluida la labor del Grupo de Trabajo de Composición Abierta en 2025. Debemos dar al Grupo la oportunidad de desarrollar plenamente su potencial en los tres años que le quedan de mandato.

La aprobación del proyecto de resolución A/C.1/77/L.23/Rev.1, que Rusia presentó, es crucial este año porque un grupo de Estados ha presentado un proyecto de resolución (A/C.1/77/L.23) en el que esencialmente se propone crear una alternativa al formato del Grupo de Trabajo de Composición Abierta. Consideramos que se trata de otro intento de apropiarse de las actividades del Grupo para politizar las negociaciones e imponer a la comunidad internacional una decisión prematura sobre el formato de la labor futura en esa esfera. Consideramos que ese enfoque es inaceptable. No es lógico y no sirve a los intereses de la inmensa mayoría de los países. Exhortamos a los Estados Miembros de las Naciones Unidas a que apoyen el proyecto de resolución A/C.1/77/L.23/Rev.1, cuyo objetivo es mantener y proteger el formato actual del Grupo de Trabajo de Composición Abierta. Un voto a favor del proyecto de resolución A/C.1/77/L.23/Rev.1 no es un voto a favor de Rusia, es un voto a favor de continuar la interacción constructiva interestatal y las negociaciones orientadas a resultados en interés del fortalecimiento de la paz, la seguridad y la estabilidad en el espacio de la información.

Sr. Aidid (Malasia) (*habla en inglés*): Malasia se adhiere a las declaraciones formuladas por la representación de Indonesia en nombre del Movimiento de Países No Alineados y por la representación de Filipinas en nombre de la Asociación de Naciones de Asia Sudoriental (véase A/C.1/77/PV.18).

Los rápidos avances en el ámbito de las tecnologías de la información y las comunicaciones (TIC) han brindado sin duda oportunidades inestimables a todos los pueblos del mundo, fomentando el crecimiento socioeconómico y la interacción transfronteriza en diversos ámbitos. Las plataformas de TIC desempeñaron un papel fundamental al facilitar el funcionamiento continuado de entidades públicas y privadas a escala nacional, regional e internacional durante todo el período de la pandemia de enfermedad por coronavirus (COVID-19), lo que mitigó los costos que acarrearían una perturbación enorme a la sociedad mundial. La dependencia de las TIC en nuestro mundo contemporáneo, que no tiene precedentes en la historia de la humanidad, es un trágico recordatorio del tipo de desafíos que entrañan y de la importancia de adoptar medidas colectivas para afrontarlos. Ahora que abordamos los efectos multidimensionales de la pandemia de COVID-19, debemos garantizar que nuestros escasos recursos en el ámbito de la seguridad de las TIC se utilicen de manera óptima. Se debe prestar una atención especial a las necesidades de los países en desarrollo, tanto en lo que se refiere a la aplicación de las reglas, normas y principios existentes como al debate mundial sobre su desarrollo futuro.

La complejidad y la sofisticación crecientes de las amenazas emergentes en el ciberespacio son motivo de preocupación. Debemos estar atentos a cualquier uso malintencionado de las TIC, en particular contra la infraestructura crítica y los servicios esenciales. El diálogo y la acción permanentes a través de plataformas multilaterales son esenciales para reducir las brechas en materia de desarrollo y sacar el máximo partido de las TIC. A ese respecto, Malasia subraya el papel central que desempeña 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), y acoge con agrado la aprobación de su informe anual de 2022 sobre los progresos realizados (véase A/77/275). Como plataforma universal, el Grupo de Trabajo de Composición Abierta sirve de foro a todos los Estados Miembros para, entre otras cosas, seguir desarrollando las reglas, normas y principios de comportamiento responsable de los Estados, así como sus medios de aplicación. El Grupo de Trabajo de Composición Abierta también ofrece a los Estados Miembros una vía para la colaboración sostenida con las partes interesadas que desempeñan un papel esencial en el desarrollo, el funcionamiento y la seguridad de las plataformas de TIC.

El año pasado, Malasia tuvo el placer de copatrocinar la resolución 76/19, en la que, entre otras cosas, se destaca el apoyo de los Estados Miembros al actual Grupo de Trabajo de Composición Abierta y a su mandato. La aprobación de esa resolución sin someterla a votación fue un acontecimiento positivo, ya que refleja la voluntad común de los Miembros de las Naciones Unidas de abordar las cuestiones relacionadas con las TIC en una plataforma única, tras varios años de discrepancias sobre distintos mecanismos. En el actual período de sesiones de la Primera Comisión, hemos visto, lamentablemente,

las recomendaciones de varias delegaciones sobre la intención subyacente y el mérito sustantivo de las propuestas presentadas por otros. Por desgracia, se trata de un patrón con el que estamos familiarizados. Malasia espera fervientemente que las partes interesadas hagan todo lo posible por colaborar de forma constructiva y evitar que se deshaga el consenso que tanto ha costado lograr y que, por frágil que sea, ha contribuido al avance de la labor del Grupo de Trabajo de Composición Abierta. Es evidente que todas las partes reconocen el valor del Grupo de Trabajo de Composición Abierta y lo indispensable que es mantener su integridad y credibilidad. Como muchos otros, Malasia está absolutamente convencida de que el Grupo de Trabajo de Composición Abierta es el órgano más adecuado para abordar los desafíos que se plantean en el ámbito de la seguridad de las TIC. Seguiremos participando de manera activa en las reuniones del Grupo de Trabajo de Composición Abierta, que es en sí mismo una medida fundamental de fomento de la confianza cuyas posibilidades deben aprovecharse al máximo, de conformidad con su mandato.

Sr. Li Song (China) (*habla en chino*): Hago uso de la palabra para explicar la posición de China con respecto a los usos pacíficos y a la seguridad de las tecnologías de la información y las comunicaciones. El uso de la ciencia y la tecnología con fines pacíficos, así como la cooperación internacional al respecto, son un derecho inalienable de todos los países. Lamentablemente, durante muchos años, el derecho de los países en desarrollo a utilizar la ciencia y la tecnología con fines pacíficos y a la cooperación internacional sin discriminación no ha estado en absoluto garantizado. En el documento final de la cumbre del Movimiento de Países No Alineados celebrada en Bakú se determinaron claramente las restricciones poco razonables a las que siguen enfrentándose los países en desarrollo para exportar materiales, equipo y tecnología para fines pacíficos. China considera que es preciso responder al llamamiento de los miembros del Movimiento de Países No Alineados, respetar el derecho legítimo de los países en desarrollo a utilizar la ciencia y la tecnología con fines pacíficos y abordar cuanto antes las restricciones indebidas a dichos usos.

El año pasado, la Asamblea General aprobó la resolución 76/234, titulada “Promoción de la cooperación internacional para los usos pacíficos en el contexto de la seguridad internacional”, que dio pie al diálogo sobre los usos pacíficos y la cooperación internacional pertinente. De conformidad con esa resolución, el Secretario General recabó opiniones de todas las partes y presentó un informe (A/77/96) que contó con una participación muy amplia y recibió el mayor número de aportaciones de todos los informes sobre desarme publicados el año pasado, lo que demuestra claramente que en general existe la voluntad de entablar un diálogo sobre las cuestiones pertinentes y que se trata de algo urgente. De nuevo este año, China presentó un proyecto de resolución sobre ese tema (A/C.1/77/L.56). Al tiempo que nos adherimos al propósito y al concepto central de la resolución del año pasado, hemos prestado la máxima atención a las propuestas de todas las partes, y nos proponemos continuar el proceso de diálogo en el marco de la Asamblea General y proporcionar una plataforma en la que todas las partes puedan debatir sobre cuestiones relevantes, desafíos y oportunidades de cooperación.

A algunos países les preocupa que con su iniciativa China esté tratando de obstaculizar el actual régimen de control de las exportaciones para prevenir la proliferación. Eso no tiene ningún sentido. China no provocó el enfrentamiento en torno al proyecto de resolución sobre usos pacíficos, y este no debería continuar durante el actual período de sesiones. Por el contrario, el proceso de diálogo establecido bajo los auspicios de las Naciones Unidas, según lo estipulado en el proyecto de resolución, debería servir para facilitar la comunicación y el diálogo entre el régimen de control de las exportaciones y los países en desarrollo. Quisiera subrayar que la no proliferación y los usos pacíficos no deberían verse como enemigos; sino más bien como asociados que van de la mano. China pide a los países en desarrollo que presten un mayor apoyo al proyecto de resolución, insta a los países occidentales a que no obstruyan el proceso de diálogo en el marco de las Naciones Unidas y exhorta a los Estados Miembros de la Organización a que realicen esfuerzos concertados para promover, de forma equilibrada, tanto los usos pacíficos como la no proliferación, dos objetivos que no se excluyen entre sí.

En la actualidad, el panorama mundial de la ciberseguridad está experimentando cambios profundos, con un enorme déficit de gobernanza cibernética y digital, lo que se suma a importantes factores de inestabilidad e incertidumbre en el ciberespacio. China considera que todas las partes deben anteponer el interés general de la comunidad internacional a sus propios intereses geopolíticos, así como la unidad y la cooperación a las divisiones y el enfrentamiento; practicar el verdadero multilateralismo; y elaborar y respetar de consuno unas normas internacionales consensuadas que rijan el ciberespacio. Todos los países, en particular los más importantes, deben cumplir con seriedad sus obligaciones internacionales; esforzarse por tener un ciberespacio

pacífico, seguro, abierto y cooperativo; y trabajar de manera colectiva por que se respete el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones, sin limitarse únicamente a aplicarlo. Los países deben abstenerse de llevar sus diferencias ideológicas al entorno del ciberespacio; de politizar, instrumentalizar y utilizar como armas las cuestiones científicas, tecnológicas, económicas y comerciales; de fragmentar Internet; y de desestabilizar las cadenas de suministro industrial.

El futuro del ciberespacio deben planificarlo todos los países de manera colectiva, ya sea a través del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional o del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. El consenso entre los países es que debería haber un único proceso sobre ciberseguridad en las Naciones Unidas. Este año, el Grupo de Trabajo de Composición Abierta elaboró con éxito su primer informe anual sobre los progresos registrados (véase A/77/275), lo que no es poco dadas las circunstancias actuales y demuestra la confianza de todas las partes en el Grupo de Trabajo.

Todas las partes deberían acoger con agrado el fuerte impulso que experimenta la labor del Grupo de Trabajo y respetar su autoridad como único proceso sobre la seguridad de las tecnologías de la información y las comunicaciones en las Naciones Unidas, de conformidad con su mandato establecido en virtud de la resolución 75/240, y deberían participar en debates sobre futuros diálogos institucionales en el marco del Grupo de Trabajo. Todas las partes deben abstenerse de intentar crear un nuevo programa de acción al margen del Grupo, y deben evitar que trabajando de forma paralela se duplique el proceso de las Naciones Unidas relativo a la ciberseguridad. China colaborará con todas las partes a fin de aprovechar plenamente el mecanismo del Grupo de Trabajo; fortalecer la comunicación y los intercambios; y construir de manera conjunta un ciberespacio más justo, razonable, abierto, inclusivo, seguro, estable y dinámico.

Sra. Lõhmus (Estonia) (*habla en inglés*): Estonia se adhiere a la declaración formulada en nombre de la Unión Europea (véase A/C.1/77/PV.18), y quisiera hacer las siguientes observaciones en representación de mi país.

Estonia asigna la máxima importancia a los esfuerzos dirigidos a prevenir y encarar las amenazas a la paz y la seguridad internacionales que se derivan del uso malintencionado del ciberespacio. Desde febrero, hemos sido testigos de la brutal agresión de Rusia contra Ucrania, en la que Rusia ha estado llevando a cabo, junto con su guerra cinética, ciberoperaciones maliciosas contra la infraestructura crítica y los servicios esenciales de Ucrania, así como campañas de desinformación. La ciberoperación maliciosa de Rusia contra la red de satélites KA-SAT tuvo efectos significativos en términos de cortes e interrupciones indiscriminados de las comunicaciones en todas las entidades públicas y privadas de Ucrania. El ataque también afectó a terceros países, lo que demuestra las peligrosas repercusiones indirectas que tienen los ciberataques.

Estonia condena enérgicamente esas ciberoperaciones malintencionadas y considera que esas operaciones menosprecian deliberadamente el marco de comportamiento responsable de los Estados previsto por las Naciones Unidas. En ese sentido, reiteramos que el derecho internacional —incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional de los derechos humanos y el derecho internacional humanitario— es plenamente aplicable al comportamiento de los Estados en el ciberespacio. Como se refleja en el informe de consenso de 2021 del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, que refrendó la resolución 76/135, los Estados Miembros acordaron que los Estados no deben realizar ni apoyar de forma deliberada actividades relacionadas con las tecnologías de la información y las comunicaciones que contravengan las obligaciones que les incumben en virtud del derecho internacional, que perjudiquen intencionadamente la infraestructura crítica o que dificulten de otro modo su utilización y funcionamiento para prestar servicios al público.

Estonia valora muy positivamente la labor del Grupo de Trabajo de Composición Abierta y acogió con agrado la aprobación de su informe anual sobre los progresos realizados (véase A/77/275) en julio de 2022. A pesar de la grave situación geopolítica, ese informe deja ver claramente la necesidad y la voluntad que tienen los miembros de las Naciones Unidas de seguir debatiendo sobre la elaboración y la aplicación de normas de comportamiento responsable de los Estados. Alentamos a los Estados a que prosigan los debates constructivos para llegar a un entendimiento general sobre la manera de mitigar con eficacia las ciberamenazas y contribuir a aumentar la ciberresiliencia mundial. Con el fin de avanzar en los debates sobre la aplicación del marco

acordado para el comportamiento responsable de los Estados y apoyar los esfuerzos de creación de capacidades, Estonia expresa su firme apoyo al establecimiento de un programa de acción permanente, inclusivo y orientado a la acción. Por consiguiente, apoyamos el proyecto de resolución A/C.1/77/L.73, que tiene por objeto iniciar las actividades del programa de acción una vez que concluya el mandato del Grupo de Trabajo de Composición Abierta en 2025 y basarse en la labor de este último, así como en la del Grupo de Trabajo de Composición Abierta anterior y en la del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional.

Por último, subrayamos el carácter del ciberespacio como un entorno que es inherentemente de múltiples partes interesadas y acogemos con beneplácito una mayor cooperación con el sector privado y la sociedad civil. El alto nivel de conocimientos especializados y la diversidad de puntos de vista de las distintas partes interesadas permiten que los debates sobre ciberseguridad en el seno de las Naciones Unidas estén mejor informados. Estonia considera esencial que los miembros de esa comunidad de múltiples partes interesadas tengan una oportunidad adecuada de expresar sus opiniones durante los próximos debates del Grupo de Trabajo de Composición Abierta.

Sr. Molla (Bangladesh) (*habla en inglés*): Bangladesh hace suya la declaración formulada por la representante de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

El discurso sobre desarme sigue redefiniéndose por los rápidos avances tecnológicos, incluidas las nuevas tecnologías armamentísticas, la inteligencia artificial y la biotecnología. En particular, la revolución de la esfera de las tecnologías de la información y las comunicaciones (TIC) e Internet han cambiado nuestro modo de vida de manera radical. Si bien la conectividad digital está revolucionando la vida humana, no hay que subestimar los riesgos que plantea para la paz y la seguridad internacionales. Por lo tanto, debemos permanecer alertas para detectar usos malintencionados de la tecnología que puedan poner en peligro nuestra seguridad colectiva.

El ciberespacio tiene que considerarse un bien público mundial del que deben beneficiarse todos, en todas partes, sin discriminación alguna. Para poder aprovechar plenamente los beneficios de las tecnologías digitales la comunidad internacional debe desarrollar unas TIC seguras, abiertas y dignas de confianza que estén sustentadas en la aplicabilidad del derecho internacional al ciberespacio, debe elaborar normas bien definidas para garantizar el comportamiento responsable de los Estados, debe concebir medidas sólidas de fomento de la confianza y debe impulsar la creación coordinada de capacidades. La ciberseguridad es una cuestión asociada a la paz y la seguridad internacionales, por lo que requiere una estrecha cooperación internacional. El Secretario General también define la ciberguerra como un riesgo estratégico fundamental en su informe “Nuestra Agenda Común” (A/75/982). Ningún país puede responder por sí solo a la amenaza de los ciberataques. Por ello, los Estados Miembros deben crear un clima en el que todos los Estados puedan disfrutar plenamente de las ventajas del ciberespacio. Nuestra única esperanza de crear un entorno de las TIC libre, seguro, estable, accesible y pacífico pasa por el multilateralismo. Hacemos hincapié en que las Naciones Unidas deben desempeñar un papel de liderazgo en el desarrollo de normas cibernéticas internacionales.

Bangladesh considera que 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 se creó en virtud de la resolución 73/27, es un mecanismo importante e inclusivo en el marco de las Naciones Unidas. Reafirmamos nuestro respaldo constructivo al éxito del actual Grupo de Trabajo y acogemos con agrado la conclusión por consenso de su primer informe anual de situación (véase A/77/275), que, a nuestro juicio, servirá de hoja de ruta para nuestros futuros debates. Apoyamos el proyecto de decisión A/C.1/77/L.54, presentado por Singapur. Además, reconocemos la labor de anteriores Grupos de Expertos Gubernamentales y sus informes, que contienen recomendaciones importantes para promover un entorno de las TIC abierto, seguro, estable, accesible y pacífico.

A falta de una estructura normativa aceptada en el plano mundial, apoyamos la aplicación de los principios de la Carta de las Naciones Unidas y del derecho internacional pertinente al ciberespacio con el fin de mantener la paz y la estabilidad. En Bangladesh, estamos trabajando para crear una sólida cultura de ciberseguridad en todas las instancias del Gobierno y en la sociedad. Hemos establecido las políticas, las estrategias y los marcos necesarios y seguimos perfeccionándolos. Abogamos por la cooperación internacional en nuestros esfuerzos, en especial en la creación de capacidades y en las medidas de fomento de la confianza.

Bangladesh concede gran importancia a la integración y la preservación de las normas ambientales

pertinentes en el régimen jurídico internacional relativo al desarme y al control de armamentos. La aplicabilidad o la pertinencia de esas normas jurídicas en relación con el desarme en los fondos marinos y el espacio ultraterrestre debería ser objeto de más investigaciones y análisis fundamentados.

Bangladesh reitera la importancia de la educación para el desarme y la no proliferación. La educación desempeña un papel fundamental para fomentar la comprensión de las consecuencias humanitarias y económicas de las armas. Deseamos dejar constancia de nuestro agradecimiento por la labor útil que sigue desempeñando el Instituto de las Naciones Unidas de Investigación sobre el Desarme. Insistimos en la necesidad de contar con una cantidad de recursos que sea mayor y previsible a fin de que el Instituto pueda cumplir sus mandatos y contribuir así a ampliar y gestionar su base de conocimientos para consumo general de todos los Estados Miembros.

Para concluir, insisto en la necesidad de situar a las personas en el centro de nuestros esfuerzos de desarme y de garantizar un desarme que salve vidas ahora y en el futuro. Debemos seguir aunando esfuerzos para garantizar un mundo más seguro.

Sr. Diack (Senegal) (*habla en francés*): El Senegal se adhiere a la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

Nos complace participar en el debate temático sobre otras cuestiones de desarme y seguridad internacional. Mi delegación desea aprovechar la oportunidad para compartir sus puntos de vista sobre algunas de las cuestiones que figuran en la agenda del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones (TIC) y de su uso (2021-2025), entre ellas la aplicación del derecho internacional, las medidas de fomento de la confianza, la creación de capacidades y el establecimiento de un diálogo periódico bajo los auspicios de las Naciones Unidas.

En relación con la aplicación del derecho internacional, el Senegal señala que aún no se han resuelto algunas cuestiones, como la aprobación de un nuevo instrumento jurídico internacional o la decisión de que el derecho internacional positivo rija en el ciberespacio. A ese respecto, consideramos necesario seguir debatiendo para evitar malentendidos y promover una comprensión mejor de cómo debe aplicarse el derecho internacional a las actividades cibernéticas. El Senegal considera que hay dos cuestiones que merecen especial atención.

La primera se refiere a la aplicación del derecho internacional humanitario. Cabe señalar que la aplicación del derecho internacional humanitario no debe interpretarse como un elemento de legitimación de la guerra en el ciberespacio, sino más bien como una manera de garantizar el cumplimiento estricto de los principios de necesidad, distinción, humanidad y proporcionalidad en todas las ciberactividades que tienen lugar en el contexto de un conflicto armado.

La segunda cuestión se refiere a la aplicación de contramedidas en respuesta a los ciberataques, incluidas las contramedidas colectivas. A ese respecto, es imprescindible alcanzar un consenso claro para garantizar un equilibrio entre el reconocimiento de la legalidad de esas contramedidas, en particular en lo que atañe a la protección de los países que carecen de conocimientos tecnológicos especializados, y la necesidad de regular el uso de esas contramedidas para que no provoquen conflictos en el ciberespacio. Al entablar esos debates, somos partidarios de recurrir a los conocimientos especializados de las instituciones pertinentes, como la Comisión de Derecho Internacional.

En cuanto a las medidas de fomento de la confianza, el Senegal acoge con satisfacción la propuesta de crear un directorio mundial de puntos de contacto nacionales y apoya la recomendación formulada en el primer informe anual de actividades del Grupo de Trabajo de Composición Abierta de celebrar debates más centrados en la puesta en funcionamiento del directorio. Para promover el intercambio de información, sería pertinente trabajar en la elaboración de modelos y en la normalización de las contribuciones de los Estados, incluidas las contribuciones al informe del Secretario General relativo a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y promoción del comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (véase A/77/92) y al Portal de Política Cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme. Ese modelo podría incluir el suministro de información sobre políticas de ciberseguridad, marcos jurídicos, estructuras administrativas y ciberamenazas, así como sobre necesidades específicas de respuesta a las ciberamenazas.

Ahora bien, siempre hay que tener en cuenta las dificultades técnicas a las que se enfrentan algunos Estados. Por ello es pertinente la creación de capacidades como un desafío principal, en especial para los países en desarrollo. El Senegal es consciente de ello y ha adoptado una estrategia nacional de ciberseguridad que define

cinco objetivos estratégicos: reforzar el marco jurídico e institucional de la ciberseguridad**,** proteger las infraestructuras críticas de información y los sistemas de información del Estado, promover una cultura de ciberseguridad, crear capacidades y mejorar los conocimientos técnicos especializados en materia de ciberseguridad y participar en las iniciativas regionales e internacionales en materia de ciberseguridad.

Nuestro país se ha esforzado por adaptar el marco jurídico para el uso de la tecnología digital y su estructura institucional, en particular mediante la creación de un servicio técnico central para la seguridad de los sistemas de codificación e información, una división especial para la lucha contra la ciberdelincuencia y una comisión para la protección de datos personales. Cabe decir lo mismo del refuerzo de la capacitación en seguridad informática. Se han creado varias instituciones de capacitación, en particular el Institut Professionnel pour la Sécurité Informatique y la Escuela Nacional de Ciberseguridad de Dakar, de orientación regional, como resultado de nuestra cooperación con Francia. Al emprender esos esfuerzos, el Senegal sigue respaldando todos los instrumentos jurídicos pertinentes, como la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, aprobado en Malabo; el Convenio del Consejo de Europa sobre la Ciberdelincuencia, firmado en Budapest; el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; y la directiva C/DIR/1/08/11, de 19 de agosto de 2011, de la Comunidad Económica de los Estados de África Occidental relativa a la lucha contra la ciberdelincuencia.

En cuanto al establecimiento de un diálogo periódico bajo los auspicios de las Naciones Unidas, mi delegación acoge con beneplácito el programa de acción de las Naciones Unidas sobre ciberseguridad y el proyecto de resolución A/C.1/77/L.73, relativo a su aplicación. Nos congratulamos de que en las consultas sobre el proyecto de resolución se hayan tenido en cuenta aspectos como el reconocimiento del Grupo de Trabajo de Composición Abierta como principal mecanismo de las Naciones Unidas en materia de ciberseguridad, la marcha de los debates sobre el programa de acción en el contexto del Grupo de Trabajo y el hecho de que, una vez en funcionamiento, el programa de acción tendrá en cuenta los resultados consensuados del Grupo.

Mi delegación está convencida de que las medidas en materia de ciberseguridad no deben estar dirigidas a restringir el desarrollo digital ni a menoscabar las oportunidades de innovación y desarrollo que ofrecen las TIC. Como medio para prevenir y combatir los usos malintencionados del ciberespacio, esas medidas deben tener como único propósito promover un entorno digital accesible, seguro, pacífico y próspero, que no deje a nadie atrás, de conformidad con la Meta 9.c de los Objetivos de Desarrollo Sostenible.

En relación con todas esas cuestiones, el Senegal reitera su determinación y su voluntad de trabajar en el seno del Grupo de Trabajo de Composición Abierta, que es el único marco para el debate sincero y constructivo sobre la ciberseguridad.

Sr. Zlenko (Ucrania) (*habla en inglés*): Ucrania se adhiere a la declaración formulada por la observadora de la Unión Europea (véase A/C.1/77/PV.18) y desea formular la siguiente declaración en nombre del país.

El rápido desarrollo de las tecnologías de la información y las comunicaciones (TIC) condujo de manera progresiva a la reformulación del espacio de Internet. En la actualidad, ya no es solo una plataforma cómoda para la comunicación, sino también una auténtica arma cada vez más peligrosa en manos de piratas informáticos, delincuentes y algunos agentes estatales y sus apoderados. Por desgracia, a pesar de las normas jurídicas vigentes y de los mecanismos institucionales creados para combatir los ciberataques en los planos nacional, regional e internacional, con frecuencia se abusa de las ventajas del nuevo entorno digital, que se manifiestan en el aumento de los ciberataques, que se han convertido en un nuevo método de guerra.

Ucrania es un Estado donde a partir de 2014 los ciberataques se transformaron en uno de los principales elementos de los esfuerzos externos por socavar nuestra soberanía. A lo largo del período comprendido entre 2014 y 2021, Ucrania enfrentó un número sin precedentes de ciberoperaciones contra objetos vitales de su infraestructura crítica, entre las que destaca el ciberataque con el programa malintencionado NotPetya en junio de 2017. Los autores de la mayoría de esos ataques fueron grupos de piratas informáticos que responden a la Federación de Rusia. Desde el comienzo de la agresión militar a gran escala de Rusia contra Ucrania, el 24 de febrero de 2022, los ciberdelincuentes han atacado al Gobierno y a las autoridades locales. También se encuentran entre sus principales objetivos las instituciones comerciales y financieras, el sector de la seguridad y la defensa, el sector energético y la industria del transporte, precisamente toda la infraestructura que sirve de base a los medios de subsistencia de la población. De

hecho, Ucrania se convirtió en el primer país del mundo que se ve como participante en una ciberguerra en toda regla. Desde la Segunda Guerra Mundial, la humanidad nunca se había enfrentado a dificultades tan graves hasta que Rusia atacó nuestro país. En lo que respecta al ciberespacio, la guerra es un reto completamente nuevo. Durante ocho meses de guerra, el Equipo de Respuesta a Emergencias Informáticas del Gobierno de Ucrania registró más de 1.000 ciberataques.

A pesar de la agresión militar rusa, Ucrania sigue reforzando su sistema de ciberseguridad con la asistencia material y de asesoramiento de sus asociados. El sistema nacional de ciberseguridad establecido como parte de la estrategia de ciberseguridad de Ucrania se basa en el Ministerio de Defensa, el Servicio Estatal de Comunicaciones Especiales y Protección de la Información, el Servicio de Seguridad de Ucrania, la Policía Nacional de Ucrania y el Banco Nacional de Ucrania. El sistema nacional de ciberseguridad garantiza la colaboración entre todos los organismos gubernamentales, las autoridades locales, las unidades militares, los organismos encargados de hacer cumplir la ley, las instituciones educativas y de investigación, los grupos civiles, las empresas y otras partes interesadas. El objetivo de la actual estrategia de ciberseguridad de Ucrania, definida para el período 2021-2025, es crear las condiciones necesarias para el funcionamiento seguro del ciberespacio y su uso en beneficio de las personas, la sociedad y el Estado. El documento se basa en los principios de disuasión, ciberresiliencia e interacción.

En cuanto al plano internacional, hacemos hincapié en que debe prestarse especial atención a la formulación de normas unificadas para la lucha contra las ciberamenazas; compartir las mejores prácticas; fomentar la confianza mutua en el ámbito de la ciberseguridad; prevenir el uso del ciberespacio con fines políticos, terroristas y militares; y proporcionar asistencia financiera y técnica para mejorar las capacidades nacionales para resistir las ciberamenazas, mitigar los riesgos y reforzar la resiliencia. Además, reviste especial importancia garantizar la rendición de cuentas en los casos en que se determine que un Estado concreto o agentes estatales están detrás de la preparación o el uso malintencionado selectivo de las TIC o de la difusión de mentiras con fines hostiles. Al fin y al cabo, los esfuerzos internacionales al respecto son simplemente vanos si no existen mecanismos confiables para detectar, castigar y enjuiciar a los individuos y a los Estados pertinentes, responsables de coordinar y financiar actividades ilícitas en el ciberespacio mundial.

Como uno de los copatrocinadores del proyecto de resolución A/C.1/77/L.73 que apoya plenamente el establecimiento de un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio, y busca crear un mecanismo inclusivo permanente orientado a la acción en el seno de las Naciones Unidas, compartimos los objetivos principales de esa iniciativa de garantizar el apoyo a los Estados en la aplicación del marco para el comportamiento responsable de los Estados en el ciberespacio y el fortalecimiento del diálogo en cooperación con las partes interesadas pertinentes. A ese respecto, nuestra delegación apoya con firmeza el proyecto de resolución A/C.1/77/L.73, presentado por Francia.

Sr. Khaldi (Argelia) (*habla en inglés*): El imperativo de consolidar y mantener la paz, la seguridad, la cooperación y la confianza internacionales entre los Estados en el entorno de las tecnologías de la información y las comunicaciones (TIC) nunca ha sido tan claro. De hecho, la evolución de las amenazas derivadas del uso malintencionado de las tecnologías de la información y las comunicaciones, así como el creciente número de ciberataques contra la infraestructura crítica de los Estados, son muy preocupantes y requieren una respuesta colectiva. En ese contexto, Argelia no puede dejar de insistir en la importancia crucial de velar por que en la utilización de las TIC se respeten plenamente los propósitos y principios de la Carta de las Naciones Unidas y del derecho internacional —en especial los principios de soberanía, igualdad soberana, no injerencia en los asuntos internos, abstención de la amenaza o del uso de la fuerza en las relaciones internacionales, la solución pacífica de las controversias y los derecho de los derechos humanos— y se siga cumpliendo el principio de coexistencia pacífica entre los Estados.

A Argelia le alientan los avances positivos que se aprecian en la conclusión satisfactoria en 2021 de las labores 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. La aprobación por consenso de sus informes finales generó un impulso positivo en los esfuerzos multilaterales sobre las TIC en el contexto de la seguridad internacional y proporcionó una base importante para proseguir nuestras deliberaciones al respecto. En ese sentido, Argelia apoya y celebra el lanzamiento, bajo los auspicios de las Naciones Unidas, del

nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y su uso, creado en virtud de la resolución 75/240, bajo la Presidencia de Singapur, como único mecanismo inclusivo, basado en el consenso, con la participación activa e igualitaria de todos los Estados. Por ello, Argelia sigue convencida de que el actual Grupo de Trabajo de Composición Abierta representa un hito importante en la cooperación internacional para el establecimiento de un entorno de las TIC abierto, seguro, estable, accesible y pacífico. Queda mucho por hacer, pero el nuevo Grupo de Trabajo vuelve a ofrecer un foro único no solo para comprender mejor las cuestiones cruciales relacionadas con la evolución de las amenazas que se derivan del uso malintencionado de las TIC, sino también seguir aunando esfuerzos para superar esos desafíos.

Al tiempo que reiteramos nuestro apoyo firme al nuevo Grupo de Trabajo de Composición Abierta y nuestra intención de seguir colaborando de manera constructiva con todos los Estados Miembros para su éxito en 2025, acogemos con agrado la aprobación por consenso, en julio de 2022, del primer informe anual sobre los avances del Grupo de Trabajo (véase A/77/275). Confiamos sinceramente en que ese espíritu de consenso prevalecerá durante los períodos de sesiones restantes del Grupo de Trabajo de Composición Abierta, que constituye una importante medida de fomento de la confianza. Asimismo, esperamos que las organizaciones regionales y subregionales sigan desempeñando un papel importante para impulsar ese proceso.

La capacidad de la comunidad internacional para prevenir o atenuar las repercusiones de las actividades malintencionadas en la esfera de las TIC depende de la capacidad que tenga cada Estado para prepararse y responder a ellas. Por lo tanto, urge crear y fortalecer las capacidades de los Estados en ese ámbito.

En ese sentido, Argelia considera que el actual Grupo de Trabajo de Composición Abierta debe poder determinar, antes de que finalice su mandato, los mecanismos adecuados para garantizar la prestación de asistencia y cooperación por parte de los Estados y del sector privado a los países en desarrollo que lo soliciten. Esa asistencia también debe incluir recursos financieros, programas de creación de capacidad y transferencia de tecnología en la esfera de las TIC, teniendo en cuenta las necesidades específicas y las particularidades de cada Estado receptor.

Al mismo tiempo, el actual Grupo de Trabajo de Composición Abierta sigue siendo la mejor plataforma para abordar y emprender todas las iniciativas pertinentes de los Estados Miembros destinadas a mantener la paz y la seguridad en el ciberespacio.

Por último, mi delegación se suma a las declaraciones formuladas anteriormente en nombre del Movimiento de Países No Alineados y del Grupo de los Estados Árabes en relación con este grupo temático (véase A/C.1/77/PV.18).

Sra. Page (Reino Unido de Gran Bretaña e Irlanda del Norte) (*habla en inglés*): El Reino Unido está decidido a promover una conducta estatal responsable en un ciberespacio libre, abierto, pacífico y seguro.

A lo largo de muchos años, los Estados han expresado constantemente su preocupación por el hecho de que las TIC puedan utilizarse con fines incompatibles con la paz y la seguridad internacionales y de que la utilización de esas tecnologías en futuros conflictos entre Estados sea cada vez más probable.

Eso es una realidad. Hoy vemos cómo Rusia —miembro permanente del Consejo de Seguridad— utiliza cibercapacidades sofisticadas y guerras de información para socavar la paz y la seguridad internacionales. También hemos empezado a ver cómo los Estados utilizan las cibercapacidades en otros conflictos del mundo.

El Reino Unido se congratula de la inclusión de una referencia clara e histórica a la aplicabilidad del derecho internacional humanitario en el primer informe anual consensuado sobre la marcha de los trabajos del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. El mundo debe unirse para promover la aplicación y la observancia del derecho internacional humanitario tanto en el mundo físico como en el virtual.

Es acertado que el Presidente del Grupo de Trabajo de Composición Abierta haya presentado una decisión para facilitar una vía de aprobación por consenso del informe anual sobre la marcha de los trabajos del Grupo. Exhortamos a todos los Estados a que respalden ese enfoque y se mantengan fieles a la buena labor que hemos desempeñado de consuno durante el primer año del Grupo.

Sin embargo, aunque apoyamos los resultados del actual Grupo de Trabajo de Composición Abierta, no podemos pasar por alto los desafíos que encaramos en el proceso de avanzar juntos. El Reino Unido es una ciberpotencia responsable, decidida a defender su marco compartido del comportamiento responsable de los Estados en el ciberespacio a través de la acción positiva.

En primer lugar, cuando los Estados utilicen el marco de manera indebida, lo diremos. En los últimos ocho meses, hemos atribuido al Estado ruso múltiples ataques perturbadores contra infraestructuras ucranianas críticas y hemos sido testigos de cómo la República Popular Democrática de Corea, el Irán y China han hecho posible que se lleven a cabo ciberactividades temerarias. Ese tipo de actividades tiene repercusiones en el mundo real. Los efectos en cascada en las infraestructuras críticas pueden exacerbar las tensiones y podrían tener consecuencias devastadoras en materia de seguridad, economía, cuestiones sociales y asistencia humanitaria.

También hemos presenciado el cierre y la restricción de Internet por motivos políticos, así como la interrupción de las comunicaciones móviles, durante las protestas que han tenido lugar recientemente en el Irán. El hecho de restringir el acceso de las personas a Internet menoscaba su capacidad para ejercer sus derechos humanos, en particular las libertades de expresión y asociación, y su capacidad para hacer que los Gobiernos rindan cuentas. Exhortamos a todos los agentes estatales responsables a que pongan fin a esas actividades malintencionadas.

En segundo lugar, cuando podamos respaldar la aplicación del marco y proteger a todos los Estados de las actividades malintencionadas en el ciberespacio, también lo haremos. Nos complace que el Grupo de Trabajo de Composición Abierta haya dado un paso importante para respaldar el objetivo compartido de los Estados Miembros de mantener un comportamiento responsable de los Estados en el ciberespacio mediante la creación de un directorio mundial de puntos de contacto.

Por último, el Reino Unido, al igual que otros países, seguirá elaborando y compartiendo su propia interpretación del marco, más recientemente en su nueva declaración de mayo sobre la forma en que se aplica el derecho internacional vigente a la actividad de los Estados en el ciberespacio. Esa es otra base importante de nuestra futura labor conjunta.

Con tantas cuestiones que abordar, está claro que es necesario entablar un diálogo institucional periódico sobre ese tema. Dicho diálogo seguirá evolucionando con el tiempo, pero debe estar firmemente arraigado en el marco consensuado de referencia. Por lo tanto, acogemos con beneplácito el proyecto de resolución de Francia (A/C.1/77/L.73), que ofrece una vía clara y transparente para que todos los Estados Miembros sigan analizando un posible programa de acción cibernética en el seno del Grupo de Trabajo de Composición Abierta y mediante contribuciones a un informe del Secretario General.

Ese diálogo debe encontrar un equilibrio entre prestar a los Estados Miembros el apoyo que necesitan para aplicar el marco y hacer frente a las amenazas a la paz y la seguridad internacionales en el ciberespacio, que son reales y van en aumento. No podemos perder de vista los nuevos retos que enfrentan la paz y la seguridad en el ciberespacio.

El Reino Unido está decidido a profundizar en las conversaciones con todas las partes interesadas para encontrar un consenso difícil de alcanzar sobre cuestiones complejas. Tenemos mucho trabajo por delante. A través de medidas positivas y prácticas, podemos corregir la disparidad entre las acciones de los Estados y su compromiso de aplicar el marco de comportamiento responsable de los Estados y hacer frente a las amenazas a la paz y la seguridad internacionales en el ciberespacio.

Por último, permítaseme decir unas palabras sobre los regímenes de control de la tecnología de misiles, que son una parte fundamental del sistema de no proliferación. Además de contribuir a la seguridad internacional, proporcionan un nivel de garantía de uso final, lo que da a los Estados la confianza necesaria para transferir la tecnología y facilita las exportaciones en todo el mundo. Al Reino Unido le preocupan los esfuerzos constantes de algunos Estados por socavar y desacreditar esos regímenes cruciales.

Sr. Albai (Iraq) (*habla en árabe*): En primer lugar, la delegación del Iraq quisiera sumarse a la declaración formulada en nombre del Grupo de los Estados Árabes y a la declaración formulada por la representante de Indonesia en nombre de los Estados miembros del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

La delegación del Iraq subraya que promover la universalidad de las convenciones y los tratados de desarme, en particular los relacionados con las armas de destrucción masiva, entre las que destacan las armas nucleares, es la única garantía de que no se utilicen esas armas ni se amenace con utilizarlas , a fin de evitar las consecuencias catastróficas que podrían derivarse del empleo de esas armas letales, que tienen una capacidad destructiva tanto para la humanidad como para el medio ambiente.

Las soluciones internacionales convenidas en el marco multilateral constituyen la única garantía sostenible para abordar las cuestiones de desarme y seguridad internacional. Por lo tanto, es necesario reiterar y cumplir los compromisos individuales y colectivos, en el contexto del marco multilateral internacional. También es necesario que las Naciones Unidas desempeñen un papel fundamental en la esfera del desarme y la no proliferación.

El Iraq expresa su creciente preocupación por la espiral de tensiones regionales e internacionales que está teniendo lugar en el plano internacional. Ello ha contribuido a incrementar el uso de las tecnologías de la información y las comunicaciones (TIC) en actividades que amenazan la paz y la seguridad regionales e internacionales. Por ello, las Naciones Unidas deben seguir elaborando normas vinculantes que controlen el comportamiento responsable de los Estados en esa esfera, que es de suma importancia. Las Naciones Unidas también deben seguir implantando controles en ese ámbito, con arreglo a la rápida evolución de la situación.

Asimismo, es necesario proseguir la cooperación internacional, preservando al mismo tiempo el papel central de las Naciones Unidas en tales empeños. En ese sentido, el Iraq acoge con agrado la aprobación por consenso del primer informe del Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 75/240, de 2020.

El Iraq expresa su pleno apoyo y disposición a hacer todo lo posible para garantizar el éxito de los períodos de sesiones cuarto y quinto, cuya celebración está prevista para el año próximo, de manera que se adopten recomendaciones para respaldar a los países en desarrollo a la hora de enfrentar los desafíos y peligros derivados del uso de las TIC, además de las amenazas cada vez mayores presentes en esa esfera.

Sr. Gunaratna (Sri Lanka) (*habla en inglés*): Sri Lanka hace suya la declaración formulada por la representante de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

En esta esfera interconectada de Internet, estamos igualmente seguros y somos igualmente vulnerables, a pesar de nuestras diferentes capacidades. Se dice que la tecnología es un buen siervo, pero un maestro peligroso. La tecnología de la información y las comunicaciones (TIC) demostró ser un asociado esencial para el desarrollo en muchos sectores durante la pandemia de enfermedad por coronavirus. La rápida transformación de la oferta educativa reviste especial importancia a ese respecto para mitigar cualquier retroceso importante de los logros alcanzados en ese sector.

La pandemia mundial también transformó el funcionamiento tradicional de Gobiernos y organizaciones, lo que permitió prestar servicios a distancia. Lamentablemente, con esos avances, los ciberataques se han convertido en una de las principales vulnerabilidades de las infraestructuras digitales críticas, lo que afecta a la prestación de servicios esenciales, el robo de datos delicados y el fraude.

Para que los países puedan aprovechar todo el potencial y los beneficios del uso de las TIC, Sri Lanka reitera la importancia de que todos los Estados Miembros adopten medidas de cooperación para garantizar la ciberseguridad. Es necesario intensificar los esfuerzos mundiales para fijar normas internacionales y elaborar marcos de gestión de los riesgos cibernéticos, con el fin de establecer una buena gobernanza y un entorno regulador en el ciberespacio. A ese respecto, Sri Lanka observa con aprecio la labor del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso.

En el plano nacional, Sri Lanka está aplicando la primera estrategia de información y ciberseguridad del país, que ha constatado la importancia de establecer un enfoque basado en alianzas para garantizar la ciberseguridad. Sri Lanka ha seguido fortaleciendo su marco jurídico para proteger a los usuarios informáticos, las infraestructuras nacionales críticas y el ciberespacio mediante la introducción de la ley sobre delitos informáticos, la ley sobre fraude de dispositivos de pago, la legislación sobre protección de datos y la ley sobre transacciones electrónicas. Sri Lanka está ultimando su proyecto de ley sobre ciberseguridad.

Hay que condenar el uso indebido de las TIC por parte de cualquier actor y con cualquier fin. En la era de la información, el uso indebido de ese recurso con fines malintencionados perjudica a todas las estructuras —sociales, económicas y políticas— y se convierte más en un instrumento de división que en un puente que acerque al mundo y a nuestros pueblos. Por lo tanto, la aplicación de normas, reglas y principios de comportamiento responsable y el cumplimiento de los tratados, los acuerdos, las obligaciones y los compromisos en esa esfera son esenciales para garantizar un ciberespacio seguro y contribuir a la paz y la seguridad internacionales.

En relación con el deterioro del contexto de seguridad internacional, somos testigos de una reducción de la cooperación basada en el consenso y de la orientación de las futuras hojas de ruta en ese ámbito, lo cual es lamentable y va en detrimento de todos los Estados. Eso solo conducirá a un mayor uso indebido del ciberespacio por los terroristas, los extremistas violentos y otros actores malintencionados que pretenden perturbar la seguridad de los usuarios de ese espacio y amenazar la paz y la estabilidad internacionales.

Por lo tanto, Sri Lanka subraya la importancia de la cooperación continua y el intercambio de mejores prácticas y capacidades entre países para abordar eficazmente

los retos de la ciberseguridad, reducir la brecha digital y permitir un progreso económico y social sin trabas. En nuestra incapacidad colectiva de unirnos, no debemos hacer revivir las palabras de Albert Einstein, pronunciadas antes de la era de Internet, en el sentido de que se había vuelto terriblemente evidente que nuestra tecnología había superado a nuestra humanidad.

Sr. Hovhannisyan (Armenia) (*habla en inglés*): Armenia está decidida a respaldar los esfuerzos de la comunidad internacional encaminados a mitigar los riesgos y contrarrestar las amenazas derivadas del uso de la tecnología de la información y las comunicaciones (TIC).

La crisis provocada por la pandemia de enfermedad por coronavirus puso de relieve el potencial cada vez mayor de las TIC para garantizar el funcionamiento adecuado y continuo de los Gobiernos y la prestación de servicios públicos y sociales. Sin embargo, las TIC también se utilizaron para incitar a la discriminación y al odio basado en la identidad y para difundir ideología extremista y prácticas violentas. La creciente utilización de las redes sociales para propagar la animadversión, fomentar los delitos de odio por motivos étnicos y religiosos y glorificar a sus autores, en particular cuando se promueven en el plano estatal, constituye una tendencia peligrosa que, si no se corrige, puede dar lugar a violaciones graves del derecho internacional humanitario y el derecho internacional de los derechos humanos.

El Cuarto Foro Mundial contra el Crimen de Genocidio, titulado “La prevención del genocidio en la era de las nuevas tecnologías”, que se celebrará en Armenia los días 12 y 13 de diciembre, se centrará en el potencial de las tecnologías innovadoras para la prevención de los crímenes atroces y los riesgos derivados de su uso con fines militares, así como para la aplicación de instrumentos y plataformas digitales como mecanismos de alerta temprana destinados a prevenir la violencia y los conflictos.

Quisiéramos reiterar que los principios y las normas del derecho internacional en su totalidad deben sentar la base del comportamiento responsable de los Estados en el ciberespacio.

Las organizaciones regionales desempeñan un papel importante para aplicar el marco de comportamiento responsable de los Estados en el uso de las TIC. A ese respecto, Armenia valora los continuos esfuerzos emprendidos en el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE) destinados a mejorar la transparencia, la previsibilidad y la estabilidad en el uso de las TIC, así como la plena aplicación de las medidas de fomento de la confianza de la OSCE para reducir los riesgos derivados del uso malintencionado de las TIC.

Subrayamos la importancia del respeto de los derechos humanos y las libertades fundamentales en el uso de las tecnologías de la información y las comunicaciones. Al analizar las amenazas existentes y potenciales en la esfera de la seguridad de la información, es importante no pasar por alto las repercusiones que el uso malintencionado de las TIC tiene para el disfrute de los derechos humanos, incluido el derecho a buscar, recibir y difundir información e ideas sin limitación de fronteras.

Armenia respalda las actividades del Grupo de Trabajo de Composición Abierta relativas a la seguridad de las tecnologías de la información y las comunicaciones y de su uso como plataforma inclusiva y transparente para promover el diálogo entre los Estados Miembros y otras partes interesadas sobre la aplicación de las reglas, las normas y los principios del comportamiento responsable de los Estados. El objetivo del Grupo es abordar la aplicabilidad del derecho internacional en la esfera de las TIC, determinar formas de prevenir y contrarrestar las amenazas en el ámbito de la seguridad de la información y promover medidas de fomento de la confianza y creación de capacidad. El informe anual sobre la marcha de los trabajos del Grupo constituye una buena base para seguir promoviendo los debates entre los Estados Miembros. Esperamos que las deliberaciones de su cuarto período de sesiones sustantivo, que se celebrará en marzo de 2023, sean constructivas y estén orientadas a la obtención de resultados.

Sra. Subhashini (India) (*habla en inglés*): Para comenzar, transmito a todos una cálida felicitación con motivo de la festividad de Divali.

La India se complace en presentar con arreglo a este grupo temático el proyecto de resolución A/C.1/77/L.59, titulado “Función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme”, que aborda la necesidad de los Estados de mejorar la cooperación internacional para utilizar la ciencia y la tecnología. con fines pacíficos.

En el proyecto de resolución se reconoce que los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y que hay que mantener y alentar el progreso científico y tecnológico al servicio de las aplicaciones civiles. El proyecto de resolución tiene presente la necesidad de regular la transferencia de tecnologías con fines pacíficos, de conformidad con las obligaciones internacionales pertinentes, para hacer frente al riesgo de proliferación por parte de Estados o de actores no estatales.

Subraya la importancia de que los Estados Miembros sigan esforzándose por aplicar los avances de la ciencia y la tecnología a fines relacionados con el desarme, así como por colaborar con expertos y con las partes interesadas pertinentes de la industria, el mundo académico y la sociedad civil para abordar eficazmente los retos que se plantean.

La India agradece al Secretario General que haya presentado el informe actualizado A/77/188, de conformidad con lo dispuesto en la resolución 76/24, de 2021. Nos complace que haya sido aprobada por consenso y que el año pasado contara con el apoyo de casi 40 Estados Miembros entre patrocinadores y copatrocinadores.

Como país en desarrollo, la India respalda la mejora de la cooperación internacional y la promoción de los usos pacíficos de la ciencia y la tecnología a través de los medios pertinentes, entre ellos la transferencia de tecnología, la difusión de información y el intercambio de equipo y materiales. Al mismo tiempo, la India considera imperativo que las transferencias internacionales de artículos y tecnologías de doble uso y de tecnología avanzada que tenga aplicaciones militares se regulen de manera eficaz, teniendo en cuenta las necesidades de legítima defensa de todos los Estados y las preocupaciones relativas a la no proliferación.

Los rápidos avances en diversas disciplinas, como las biociencias, las ciencias de los materiales, la inteligencia artificial y la aplicación de datos a tecnologías nuevas y emergentes, aportan importantes beneficios y también pueden plantear retos para la paz y la seguridad. La India reconoce la necesidad de un enfoque interdisciplinar para comprender las repercusiones de esos avances, así como para formular respuestas adecuadas que mitiguen sus efectos adversos.

La India respalda los debates relativos a las tecnologías emergentes en diversos foros multilaterales de las Naciones Unidas y organismos especializados y en el marco de los tratados internacionales de los que la India es parte, y participa activamente en ellos.

La India se compromete a promover un entorno abierto, seguro, estable, accesible y pacífico para las TIC. El uso malintencionado y con fines delictivos del ciberespacio por los terroristas y la interconexión que caracteriza al entorno de las TIC hacen necesario un planteamiento y una labor basados en normas y en la colaboración a fin de garantizar su apertura, estabilidad y seguridad.

A ese respecto, la India respalda la labor orientada a la acción del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, que preside Singapur. Acogemos con beneplácito la aprobación por consenso del informe anual de 2022 sobre la marcha de los trabajos del Grupo, que proporciona una base sólida para su labor de cara al próximo año.

Durante su mandato, el Grupo debe seguir siendo la principal plataforma para todas las deliberaciones intergubernamentales sobre cuestiones en materia de TIC relacionadas con su mandato. Desaconsejamos enérgicamente la creación de procesos paralelos oficiales mientras no finalice la labor del Grupo.

Reconociendo la disparidad que existe entre los Estados Miembros en lo que respecta a preparación cibernética para hacer frente a diversas ciberamenazas, y la necesidad de mejorar sus capacidades, la India ha propuesto la creación de un portal de cooperación mundial en materia de ciberseguridad basado en las Naciones Unidas que sirva como una plataforma global para la creación de capacidad y la cooperación internacional entre los Estados Miembros. Esperamos que el año que viene el Grupo de Trabajo de Composición Abierta celebre debates productivos y tome una decisión al respecto.

Habida cuenta de la pertinencia y la importancia de ese tema, es muy necesario que los Estados colaboren para hacer frente a los retos complejos que plantea. La India busca el apoyo constante de todos los Estados Miembros para que se apruebe por consenso este año su proyecto de resolución sobre la función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme. Asimismo, alentamos a los Estados Miembros a que copatrocinen el proyecto de resolución y se sumen a nosotros en este esfuerzo colectivo por contribuir de manera significativa a la paz y la seguridad mundiales.

Sra. Rodríguez Acosta (El Salvador): La interconectividad creciente y la dependencia de las tecnologías de la información y las comunicaciones (TIC) en todas las esferas de la vida llaman a todos los Estados a profundizar su interés y su conocimiento sobre lo que sucede en el ámbito de la seguridad de la información y la importancia de prevenir el uso malicioso de las tecnologías de la información y las comunicaciones.

Por dichas razones, mi país considera la ciberseguridad como parte fundamental de la seguridad internacional. Observamos con preocupación cómo incidentes recientes de operaciones de *ransomware* y otro tipo de ciberataques destinados a inhabilitar o ralentizar la prestación de servicios públicos tienen profundas

implicaciones para la seguridad internacional y ponen de relieve la urgencia de fortalecer la ciberresiliencia para protegernos de estas amenazas, que son globales. Este es un reto que los Estados no podemos emprender solos. Es necesaria la cooperación activa de toda la comunidad internacional para atajar esos desafíos.

Encomiamos, por lo anterior, la aprobación consensual del primer informe de progresos del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, en el que hemos venido participando activamente. Tal como lo expresó nuestra delegación en el compendio de explicaciones publicado sobre la aprobación del informe, este no pretendía ser un resumen exhaustivo de las labores del Grupo, sino que buscaba enumerar los avances logrados hasta la fecha y fijar una guía para avanzar en las futuras discusiones.

En esa línea, nos complacen los avances destinados al establecimiento de un directorio mundial de puntos de contacto, mencionado por nuestra delegación en las últimas sesiones de trabajo del Grupo. Consideramos que la iniciativa de fomento de la confianza puede ser una valiosa fuente de intercambio de información sobre amenazas, vulnerabilidades e incidentes de ciberseguridad en tiempo real. Asimismo, hemos sugerido que se estudie la posibilidad de establecer este directorio a nivel técnico y operativo, entre los equipos nacionales de ciberseguridad y los enlaces de ciberdiplomacia.

Esperamos poder presentar nuestras contribuciones nacionales en anticipación al cuarto período de sesiones del Grupo de Trabajo. Del mismo modo, tomamos debida nota de la presentación del proyecto de resolución A/C.1/77/L.73 para establecer el programa de acción para avanzar en el comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional. Esa iniciativa ha sido apoyada desde el inicio por El Salvador. Consideramos que la misma complementará los trabajos del Grupo de Trabajo actual y permitirá establecer en el futuro un mecanismo de discusión permanente para los Estados Miembros con una orientación directa a la acción.

Mi país espera continuar trabajando y aportando a las discusiones multilaterales destinadas a fortalecer el marco de comportamiento responsable de los Estados en el ciberespacio y seguir debatiendo sobre las amenazas reales y potenciales en los ámbitos de la seguridad y la información. Asimismo, reafirmamos la importancia de avanzar en un marco vinculante que permita la protección de infraestructuras críticas e infraestructuras críticas de información en materia de ciberamenazas y de identificar las vulnerabilidades con miras a proteger los activos estratégicos nacionales.

El Salvador está comprometido con el avance de su agenda de transformación digital desde una perspectiva de protección de datos personales y protección de infraestructura crítica con la finalidad de reforzar la confianza de la población en la prestación de los servicios digitales proporcionados a nivel de país. Es por eso que nos complace haber finalizado la consulta pública sobre la ley de ciberseguridad, liderada por la Secretaría de Innovación de la Presidencia. De igual manera, es importante seguir abogando por el desarrollo de medidas de fomento de la confianza, que permitan reducir tensiones y desescalar conflictos en el ciberespacio.

Hemos expresado activamente la importancia que brindamos a la amplia participación de otros actores en estos procesos. Los retos en el ciberespacio requieren de una colaboración activa de la sociedad civil, las organizaciones no gubernamentales, los organismos regionales y el mundo académico.

Para finalizar, mi delegación ha expresado cómo un enfoque transversal de género puede ayudarnos a comprender la prevalencia de los patrones relacionados con la violencia armada y el conflicto, que afectan diferencialmente a mujeres y hombres. En ese sentido, tenemos el trabajo de tomar decisiones asertivas sobre cómo abordar esos desafíos. Asimismo, los asuntos de género son igualmente relevantes en la ciberseguridad internacional.

La versión completa de esta declaración será publicada en la plataforma eStatements.

Sra. Lee (República de Corea) (*habla en inglés*): En los dos últimos decenios, la humanidad ha sido testigo de avances nunca vistos en la esfera de la tecnología digital. Si bien ese desarrollo nos ha aportado beneficios económicos y sociales sin precedentes, aumentando el número de personas con acceso a Internet desde la pandemia mundial, nos hemos vuelto cada vez más vulnerables a las actividades cibernéticas malintencionadas. El comportamiento de los agentes estatales y no estatales en el ciberespacio complica aún más el panorama de la seguridad internacional.

A pesar de la complejidad de los problemas a los que nos enfrentamos, la comunidad internacional debe trabajar de consuno por un ciberespacio abierto, seguro, estable, accesible y pacífico. En ese sentido, la República de Corea apoya el papel central que cumplen las

Naciones Unidas en las conversaciones en curso, orientadas a dar respuesta a las preocupaciones acuciantes y a fomentar un comportamiento responsable por parte de los Estados en el ciberespacio. En particular, quisiera destacar las siguientes cuestiones.

En primer lugar, la República de Corea saluda el informe anual de 2022 del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, y también celebra la decisión de la Presidencia de aprobar el informe. La República de Corea seguirá colaborando de manera constructiva con el grupo de trabajo, sobre la base ese informe, aprobado por consenso, en el que están recogidos los progresos realizados.

Como copatrocinadores del proyecto de resolución A/C.1/77/L.73, titulado “Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional”, presentado por Francia, quisiéramos insistir en la necesidad de establecer un mecanismo permanente en el seno de las Naciones Unidas, que sirva como programa de acción para mejorar la aplicación práctica de las normas y para fomentar el intercambio de mejores prácticas y el fomento de la capacidad.

En segundo lugar, la República de Corea considera que los resultados consensuados de los grupos de trabajo de composición abierta y de los anteriores Grupos de Expertos Gubernamentales (GEG) reflejan los progresos realizados en el marco acumulativo y evolutivo del comportamiento responsable de los Estados a la hora de emplear las tecnologías de la información y las comunicaciones (TIC). En consecuencia, como no debe existir un vacío legal en el ciberespacio, el derecho internacional —incluida la Carta de las Naciones Unidas en su totalidad— también debe aplicarse al ciberespacio. Además, los Estados deben respetar y aplicar con rigurosidad las normas voluntarias y no vinculantes establecidas en los informes de consenso de los GEG y de los grupos de trabajo de composición abierta. En particular, mi delegación considera que el principio de diligencia debida desempeña un papel crucial para garantizar la ciberseguridad y quisiera cooperar estrechamente con otros Estados Miembros para seguir elaborando e implementando las normas pertinentes.

En tercer lugar, la República de Corea está firmemente a favor de la aplicación de medidas de fomento de la confianza y para la creación de capacidades. Esas medidas pueden limitar el riesgo de que se produzcan conflictos a causa de malentendidos y errores de cálculo. La República de Corea también se esforzará por colmar la brecha existente en materia de capacidades de ciberdefensa. Estamos participando de forma activa en los importantes esfuerzos que se realizan en foros regionales como la Asociación de Naciones de Asia Sudoriental (ASEAN) y el Foro Regional de la ASEAN.

Mi delegación considera que la participación, el empoderamiento y la educación de la generación más joven pueden hacer valiosas contribuciones al régimen mundial de no proliferación. A partir de 2019, los Estados Miembros han venido aprobando por consenso una resolución bienal titulada “La juventud, el desarme y la no proliferación”. Asimismo, en el borrador del documento final de la última Conferencia de las Partes encargada del Examen del Tratado sobre la No Proliferación de las Armas Nucleares se reconoció la importancia de tomar en cuenta las distintas opiniones y se expresó la voluntad de empoderar a los jóvenes y de facilitar su participación en el ámbito del desarme y la no proliferación. Como defensora de la Acción 38 de la Agenda creada por el Secretario General, titulada “Asegurar nuestro futuro común: una agenda para el desarme”, la República de Corea seguirá liderando esa agenda y se consagrará a impulsar ese empeño.

Antes de concluir, mi delegación quisiera señalar que la República de Corea respeta el derecho de todos los Estados Miembros a tener acceso a equipos, materiales e información científica y tecnológica con fines pacíficos, y, en ese sentido, cree firmemente que los regímenes existentes de control de las exportaciones promueven ese propósito, ya que distinguen lo que puede exportarse de lo que no, en lugar de dar carta blanca a los países exportadores para que apliquen restricciones arbitrarias o concedan licencias inapropiadas.

Sr. Aydil (Türkiye) (*habla en inglés*): Hoy en día, la situación mundial en materia de paz, seguridad, derechos humanos y desarrollo económico se ve cada vez más afectada por el uso de las tecnologías de la información y las comunicaciones (TIC).

Türkiye sigue preocupada por el uso malintencionado de esas tecnologías y por el número y la gravedad cada vez mayores de los ciberataques en todo el mundo. La vida de nuestros ciudadanos se está viendo enormemente afectada por ciberataques dirigidos contra infraestructuras críticas como las comunicaciones electrónicas, la energía, las finanzas, el transporte, la gestión de los recursos hídricos y otros sectores fundamentales de los servicios públicos.

Hacer frente a esas amenazas y riesgos en el ciberespacio es fundamental para lograr que ese ámbito sea abierto, libre, estable y seguro a escala mundial.

Ya se han realizado numerosos trabajos en lo que respecta al comportamiento responsable de los Estados en el ciberespacio. Subrayamos el papel central de las Naciones Unidas en ese proceso. Consideramos que los ciberdebates celebrados con los auspicios de las Naciones Unidas han alcanzado cierto nivel de madurez. Por ello, tenemos que entablar un diálogo sobre cómo impulsar la implementación del marco normativo existente.

En el informe final del anterior grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso se indicaba que es cada vez más probable que en los conflictos futuros entre los Estados se empleen las TIC. La guerra en Ucrania ha confirmado esa preocupación, por lo urge emprender esa tarea.

En aras de aplicar mejor el marco acumulativo existente, una medida apropiada sería el establecimiento de un programa de acción sobre cuestiones relativas a la ciberseguridad. A ese respecto, apoyamos el proyecto de resolución A/C.1/77/L.73, presentado por Francia, y esperamos seguir dar continuidad a nuestras conversaciones a través del programa de acción como mecanismo permanente, inclusivo y orientado a la acción. Ese programa también ayudaría a fomentar el diálogo y la cooperación en cuestiones relativas a la creación de capacidad, que son fundamentales para la ciberresiliencia. Esa iniciativa no tiene por objeto sustituir o hacer la competencia al actual grupo de trabajo de composición abierta sobre la seguridad de las TIC, sino que ese grupo tendrá en cuenta sus conclusiones y contribuirá a sus esfuerzos de implementación.

Türkiye participa de forma activa en el actual grupo de trabajo de composición abierta. Nos satisface que este año el informe anual sobre la marcha de los trabajo haya sido aprobado por consenso. Estamos de acuerdo con la valoración de que el grupo de trabajo, con su composición universal, es una plataforma única y constituye en sí mismo una medida de fomento de la confianza.

La naturaleza de las ciberamenazas hace necesario adoptar medidas unificadas. Nos habría gustado que este año se adoptara un enfoque consensuado en la Primera Comisión, como sucedió el año pasado. En ese sentido, una vez más, hacemos un llamamiento a favor de un espíritu de cooperación.

Sr. Ogasawara (Japón) (*habla en inglés*): El ciberespacio se ha convertido en una infraestructura económica y social indispensable para todas las actividades, y es, por tanto, un espacio público en el que todos los ciudadanos pueden participar. Esa transformación económica y social también nos ha hecho vulnerables a los ciberataques, que plantean para todos un grave riesgo de seguridad. Desde el punto de vista de la seguridad nacional, nos preocupan en especial las actividades cibernéticas malintencionadas generadas desde otros Estados, con apoyo o no de esos Estados, que dañan infraestructura crítica.

Es difícil que un solo país pueda responder por sí solo a esas amenazas a la ciberseguridad. La cooperación y la colaboración entre los Estados es primordial para proteger y fomentar un ciberespacio libre, abierto y seguro.

Con respecto a cómo aplicar el derecho internacional a las ciberoperaciones, la posición del Japón no deja lugar a dudas: el derecho internacional vigente es aplicable a todas esas actividades. También apoyamos firmemente la elaboración de normas voluntarias de comportamiento estatal responsable. Hacer valer el estado de derecho en la comunidad internacional es sumamente importante para estabilizar las relaciones entre los países y lograr el arreglo pacífico de controversias.

El Japón también considera importante promover el estado de derecho en el ciberespacio. Considera que el informe anual sobre la marcha de los trabajos, aprobado por consenso 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) es parte de los esfuerzos para lograr ese objetivo y conseguir un ciberespacio libre, justo y seguro. Como proceso orientado a la acción, es importante que el grupo de trabajo de composición abierta logre resultados concretos basados en el resultado de las conversaciones anteriores, tal y como se refleja en sus informes y en los del Grupo de Expertos Gubernamentales. En ese sentido, apoyamos con firmeza la decisión de la Presidencia del grupo de trabajo de composición abierta de aprobar el informe anual sobre los progresos realizados.

Asimismo, respaldamos el proyecto de resolución A/C.1/77/L.73, presentado por Francia, relativo al establecimiento de un programa de acción destinado a promover el comportamiento responsable de los Estados en el ciberespacio.

También quisiera abordar la cuestión de la educación para el desarme y la no proliferación, que el Japón ha venido promoviendo como un medio útil y eficaz para avanzar hacia un mundo libre de armas nucleares.

En ese sentido, es esencial que concienciemos a la opinión pública de las consecuencias humanitarias catastróficas de todo tipo de uso de las armas nucleares y de la amenaza que se deriva de los diversos riesgos que plantea la proliferación de armas nucleares, así como de los pasos necesarios para superar esos retos.

La educación para el desarme y la no proliferación y la concienciación deben llevarse a cabo de forma inclusiva y colaborativa. Diversos agentes, como las instituciones educativas y de investigación, los grupos de reflexión, la comunidad científica, la sociedad civil, el sector privado, los medios de comunicación, las comunidades locales, las organizaciones internacionales y los Gobiernos, deberían aprender los unos de los otros y crear sinergias para promover las iniciativas educativas.

Desde esa perspectiva, el Japón propone mencionar algunas iniciativas concretas en ese sentido en el párrafo 11 de la parte dispositiva del proyecto de resolución A/C.1/77/L.61, titulado “Pasos para construir una hoja de ruta común hacia un mundo sin armas nucleares”, que el Japón presentó este año a la Comisión.

El Japón ha participado activamente en diversas iniciativas de educación para el desarme y la no proliferación. En particular, en la Conferencia de las Partes encargada del Examen del Tratado sobre la No Proliferación de las Armas Nucleares (TNP), celebrada en agosto, el Primer Ministro Kishida anunció la creación del Fondo de Líderes Juveniles en favor de un mundo sin armas nucleares. En la Conferencia, el Japón también encabezó la declaración conjunta sobre educación para el desarme y la no proliferación, que recabó el apoyo de 89 Estados partes en el TNP.

El Japón cree firmemente en el poder de la educación para el desarme y la no proliferación y en el potencial de las generaciones venideras para lograr la consecución de nuestro objetivo común: hacer realidad un mundo sin armas nucleares.

La versión completa de esta declaración se publicará en el *Diario de las Naciones Unidas.*

Sra. Romero López (Cuba): Apoyamos la intervención de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

Reiteramos el compromiso de Cuba con el desarme general y completo, que permita alcanzar un mundo libre de armas de destrucción masiva en beneficio de las generaciones presentes y futuras. Abogamos por la adopción de otras medidas de desarme y seguridad internacionales que nos permitan avanzar en la construcción de un mundo de paz.

Se precisa reducir cuanto antes los cuantiosos recursos que hoy se destinan a los presupuestos militares. Los mismos recursos y progresos científicos y tecnológicos que hoy se dedican a financiar el complejo militar industrial y se utilizan para el desarrollo, la producción y el perfeccionamiento de armas cada vez más mortíferas y sofisticadas generarían cuantiosos beneficios a la humanidad si se reorientaran en función del desarrollo sostenible.

Los Estados Miembros debemos continuar trabajando para preservar el multilateralismo como principio básico de las negociaciones en materia de desarme y control de armamentos. Recordamos que estas deben observar las normas ambientales internacionales vigentes.

Abogamos por la negociación de iniciativas legalmente vinculantes para prohibir la militarización del espacio ultraterrestre, del ciberespacio y las armas letales autónomas. Se precisa alcanzar acuerdos que regulen las armas parcialmente autónomas y los drones militares de ataque.

Reiteramos nuestro compromiso con las labores del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso para el período 2021-2025. Apoyamos las discusiones en ese formato, con la participación de todos los Estados en igualdad de condiciones.

Las tecnologías de la información y las comunicaciones no deben utilizarse como medio de guerra, sino para fines exclusivamente pacíficos. Rechazamos el uso hostil de las telecomunicaciones con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, así como para cometer o alentar actos de terrorismo.

Nos oponemos a la consideración del uso de la fuerza como una respuesta legítima a un ataque cibernético. Reiteramos nuestra preocupación por la estrategia cibernética de los Estados Unidos, que autoriza el uso de armas cibernéticas ofensivas y la realización de operaciones ciberofensivas, incluidos los ciberataques preventivos para disuadir a los adversarios de ese país.

Rechazamos los métodos de guerra no convencional que el Gobierno de los Estados Unidos continúa aplicando contra Cuba y los recursos millonarios que destina a ese fin. Condenamos el empleo de las nuevas tecnologías de la información y otras plataformas digitales para intentar desestabilizar nuestro país, difundir noticias falsas y promover un cambio de régimen en Cuba. Nos oponemos a la Fuerza de Tarea de Internet para Cuba, que viola las normas internacionalmente acordadas en

la materia. Llamamos a los Estados Unidos a poner fin de inmediato al bloqueo económico, comercial y financiero impuesto contra Cuba, que limita considerablemente el acceso, uso y disfrute de las tecnologías de la información y las comunicaciones para el bienestar de la población cubana.

Estamos convencidos de que el desarme general y completo es necesario y posible. Cuba continuará promoviendo la adopción de medidas eficaces que nos permitan alcanzar ese noble fin.

Sr. Salmeen (Kuwait) (*habla en árabe*): La delegación de mi país hace suyas las declaraciones formuladas en nombre del Movimiento de Países No Alineados y del Grupo de los Estados Árabes, respectivamente (véase A/C.1/77/PV.18).

La ciberseguridad es uno de los nuevos problemas a los que hace frente el mundo, y muchos países sufren actualmente sus efectos negativos, entre ellos el Estado de Kuwait, que ha sido objeto en los últimos años de numerosos ciberataques, así como de actos de ciberpiratería, tanto de ataques individuales como de sabotaje patrocinados por grupos terroristas y criminales extranjeros. Ello se debe al carácter de doble uso del ciberespacio y a la utilización de microtecnología y de los recursos para desarrollar nuevos sistemas de armamento, que ha exacerbado las dudas y la falta de confianza entre los Estados.

A ese respecto, mi país insiste en la necesidad de garantizar las normas de seguridad y proporcionar protección contra los ciberataques y las violaciones programadas. Hacemos un llamamiento a todos los países para que cooperen y coordinen sus acciones a escala regional e internacional.

El Estado de Kuwait otorga una gran prioridad a la ciberseguridad, ya que se trata de una fuerza defensiva fundamental, sobre todo habida cuenta de que los delitos cibernéticos no solo van dirigidos contra personas e instituciones, sino que también pone en peligro la seguridad nacional y las instalaciones y economías de los Estados. Por esa razón, el Estado de Kuwait puso en marcha una estrategia nacional de ciberseguridad para 2017-2020 con el fin de reforzar la cultura de la ciberseguridad y promover el uso justo y seguro del ciberespacio kuwaití, así como de proteger las infraestructuras de información críticas y nacionales, entre otras cosas reforzando los mecanismos de intercambio de información entre las distintas partes interesadas, tanto locales como internacionales. Destacamos que nuestra estrategia se ajusta a políticas de seguridad y criterios globales estrictos en los que se garantiza la protección de la información contra todo tipo de piratería informática y un ciberespacio kuwaití seguro y sostenible.

En ese contexto, dado que los dirigentes políticos del Estado de Kuwait son conscientes del alcance de los retos que nos plantea el ciberespacio y habida cuenta de la intención de mi país de apoyar la transformación digital para promover nuestro desarrollo nacional como parte del nuevo Kuwait 2035, el Estado de Kuwait creó un centro nacional de ciberseguridad que comprende un centro de operaciones de ciberseguridad, así como un equipo de respuesta para las emergencias en el ciberespacio, con miras a crear una estrategia nacional integral en materia de ciberseguridad. Ello garantizará la protección de nuestras redes de información y telecomunicaciones y permitirá la recogida y el intercambio de información mediante el uso de cualquier tipo de dispositivo electrónico, en colaboración con todas las partes interesadas nacionales.

Nos enfrentamos a una revolución tecnológica y a una transformación digital acelerada y sin precedentes, al tiempo que hacemos un uso cada vez mayor de Internet y de los medios de comunicación modernos. Hoy en día, el mundo está más interconectado que nunca, lo cual aumenta el riesgo de que se produzcan ciberataques, como el robo de información y la violación de la confidencialidad. Asimismo, existe un importante número de características de las armas avanzadas que dependen de la tecnología moderna. En ese contexto, al Estado de Kuwait le preocupan las armas autónomas y el empleo de la impresión 3D en el ámbito de las telecomunicaciones, que se han generalizado en los procesos de fabricación en todo el mundo. Si esas tecnologías cayeran en manos de grupos terroristas o grupos delictivos organizados o se emplearan de manera ilegal, se produciría una nueva amenaza para la paz y la estabilidad internacionales, lo cual sin duda acarrearía consecuencias desastrosas para la infraestructura primordial y para la circulación de artículos manufacturados en condiciones de seguridad. En ese sentido, mi país reitera su posición firme en materia de desarme y seguridad internacional. Consideramos que la circulación y la proliferación de armas van en contra de nuestro objetivo deseado de lograr la paz y la estabilidad internacionales.

Por ello, hacemos un llamamiento a todos los Estados para que se esfuercen por lograr un instrumento internacional vinculante y consensuado que regule el uso del ciberespacio y establezca mecanismos de intercambio de información entre los Estados partes. Ese instrumento debe además respetar la soberanía de los Estados en lo que respecta a los drones, que están

siendo ampliamente utilizados como un nuevo medio de guerra contra la población civil y la infraestructura estatal. El Estado de Kuwait hace hincapié en su condena de todos los ataques cibernéticos y electrónicos que implican el empleo de drones, habida cuenta de sus graves repercusiones en la esfera de la seguridad regional e internacional. En ese contexto, pedimos a los Estados que defiendan los principios de la Carta, incluidos los principios de buena vecindad y respeto de la soberanía, así como el principio de no intervención en los asuntos internos de otros Estados.

El Estado de Kuwait saluda los dos programas de acción sobre ciberseguridad puestos en marcha por el Secretario General António Guterres como parte de la agenda de desarme de 2018.

Para concluir, valoramos todos los esfuerzos internacionales relacionados con la cuestión de la ciberseguridad y hacemos un llamado a no politizarlos y a promover el principio de transparencia a ese respecto. Insistimos en nuestro apoyo continuo a todas las medidas internacionales que fomenten la confianza y la capacidad en aras de reducir las amenazas a la paz y la seguridad internacionales.

Sr. Jotterand (Suiza) (*habla en francés*): A Suiza le preocupa el creciente número de ciberoperaciones que se llevan a cabo en el conflicto armado de Ucrania, en especial las que están dirigidas contra la infraestructura crítica. Como resultado, aumentan las posibilidades de que se produzcan consecuencias involuntarias o comportamientos inapropiados. Suiza hace un llamamiento a todas las partes en el conflicto armado para que respeten el derecho internacional humanitario, así como el derecho internacional de los derechos humanos. Ello también se aplica al ciberespacio.

En nuestro mundo, que evoluciona rápidamente, los usos civiles y militares del ciberespacio son cada vez mayores, lo que plantea nuevos problemas para la paz y la seguridad internacionales. Esos problemas solo pueden abordarse si se respeta el marco acordado para el comportamiento responsable de los Estados en el ciberespacio. Como se confirma en los respectivos informes del Grupo de Expertos Gubernamentales y del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, aprobados por consenso, ese marco incluye la aplicación del derecho internacional en el ciberespacio y la entrada en vigor de las 11 normas voluntarias y de las demás medidas de fomento de la confianza y para la creación de capacidad.

Celebramos que en julio se aprobara por consenso el informe anual sobre la marcha de los trabajos del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, en el que se recogen —entre otros elementos— propuestas relevantes encaminadas a esclarecer la implementación del derecho internacional, incluidos el derecho internacional humanitario, y la entrada en vigor de las normas voluntarias relativas al comportamiento responsable de los Estados en el ciberespacio.

La labor crítica que lleva a cabo el grupo de trabajo actual ofrece una oportunidad invaluable para seguir ampliando el consenso respecto de la aplicación del derecho internacional en el ciberespacio. Con el fin de contribuir a nuestro objetivo común de alcanzar un acuerdo universal acerca de cómo se aplica el derecho internacional al ciberespacio, Suiza dio a conocer en 2021 su posición nacional sobre esa importante cuestión.

Alentamos a todos los Estados Miembros de las Naciones Unidas a que consideren la posibilidad de dar a conocer sus propias posiciones nacionales. Asimismo, esperamos con interés que prosigan las deliberaciones sobre todos los elementos del mandato del grupo de trabajo actual.

Saludamos la propuesta de la Presidencia del grupo de trabajo de composición abierta de celebrar consultas entre períodos de sesiones en 2023 y 2024 a fin de avanzar en las conversaciones, seguir trabajando a partir del informe anual sobre los progresos realizados y ayudar a que el grupo de trabajo de composición abierta prosiga su labor. A ese respecto, damos las gracias a la Presidencia del grupo por haber presentado a la Comisión un proyecto de decisión (A/C.1/77/L.54) que abarca tanto la aprobación de dicho informe como las consultas entre períodos de sesiones que he mencionado. Suiza apoya plenamente el proyecto de decisión y ese enfoque puramente procedimental y práctico.

Asimismo, debemos subrayar que el proyecto de resolución (A/C.1/77/L.23/Rev.1) sobre esa cuestión presentado por la Federación de Rusia nos genera serias dudas, ya que al mismo tiempo parece ser innecesario y replicar el texto de la Presidencia del grupo. El proyecto presentado por Rusia también genera dudas sobre cuestiones de fondo, sobre todo dado que no se basa en un lenguaje consensuado y utiliza un enfoque selectivo. Con ello, se corre el riesgo de socavar los enormes avances logrados hasta la fecha en el actual grupo de trabajo. Habida cuenta de la situación actual, Suiza no puede respaldar ese proyecto.

La creación de una plataforma para el diálogo institucional regular sobre cuestiones cibernéticas en el seno de las Naciones Unidas también merece toda nuestra atención. Suiza quisiera subrayar que las decisiones relativas al futuro de las conversaciones sobre actividades cibernéticas celebradas en las Naciones Unidas deben basarse en deliberaciones inclusivas que permitan a todos los Estados Miembros exponer su punto de vista. Además, consideramos que todo proceso futuro en las Naciones Unidas debe centrarse en apoyar a los Estados Miembros en sus esfuerzos por aplicar el marco existente para el comportamiento responsable de los Estados en el ciberespacio.

Es importante aprovechar y salvaguardar lo conseguido en los últimos años y hacer un uso eficaz de las recomendaciones acordadas. Por ello, apoyamos el proyecto de resolución A/C.1/77/L.73, relativo a un programa de acción orientado a promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, presentado por Francia, que permitirá a los Estados Miembros de la Organización hacer avanzar ese debate.

Sra. Vladescu (Rumania) (*habla en inglés*): Rumania se adhiere plenamente a la declaración formulada por la representante de la Unión Europea (véase A/C.1/77/PV.18) y desea hacer las siguientes observaciones en nombre del país.

Nos reunimos en un entorno de seguridad esencialmente alterado, que está marcado por el aumento de las tensiones y los problemas globales que siguen socavando la arquitectura del control de armamentos, el desarme y la no proliferación. La agresión militar ilegal, injustificada y no provocada de la Federación de Rusia contra su vecina Ucrania nos ha conducido a una escalada sin precedentes.

Desde el 24 de febrero, estamos siendo testigos de las consecuencias dramáticas de esa agresión, durante la cual Rusia ha recurrido a todo tipo de armas convencionales, así como a la desinformación y los ciberataques. Rumania condena firmemente la agresión de Rusia y reafirma su apoyo inquebrantable a la independencia, la soberanía y la integridad territorial de Ucrania dentro de sus fronteras reconocidas internacionalmente.

La seguridad del ciberespacio se ha convertido en una cuestión de prioridad máxima, dado que las actividades malintencionadas con base en las tecnologías de la información y las comunicaciones (TIC) por parte de actores que generan amenazas persistentes, incluidos Estados y otros agentes, pueden representar un riesgo significativo para la seguridad y la estabilidad internacionales, para el desarrollo económico y social, y para la seguridad y el bienestar de las personas.

Ahora más que nunca, es importante promover un ciberespacio abierto, seguro, estable, accesible y pacífico, adherirse plenamente al marco de las Naciones Unidas para el comportamiento responsable de los Estados y proseguir nuestra labor de contribuir a la seguridad y la estabilidad en la utilización de las TIC por parte de los Estados.

Rumania acoge con satisfacción el consenso alcanzado este año sobre el informe anual de situación del 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, establecido en virtud de la resolución 75/240. Reiteramos nuestro pleno apoyo a la decisión de la Presidencia del Grupo de Trabajo de Composición Abierta al respecto y a su llamamiento a una aprobación consensuada.

Alentamos a todos los Estados Miembros a respaldar el proyecto de resolución A/C.1/77/L.73, relativo a un programa de acción para promover el comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional, copatrocinado por un grupo transregional de Estados y que cuenta con el pleno apoyo de Rumania.

En estos tiempos de intensificación de las tensiones y los conflictos, la necesidad de solidez y transparencia, en particular en el ámbito de los gastos militares, es aún más pertinente. A este respecto, quisiéramos poner de relieve el proyecto de resolución de este año, titulado “Información objetiva sobre cuestiones militares, incluida la transparencia de los gastos militares” (A/C.1/77/L.63), presentado tradicionalmente por Rumania y Alemania. Instamos a los Estados Miembros de las Naciones Unidas a que apoyen el proyecto de resolución, que se basa en el principio fundamental de fomentar la confianza entre los Estados.

El sistema de las Naciones Unidas para la presentación normalizada de informes sobre gastos militares ha logrado un éxito notable a lo largo de muchos años y debería seguir siendo una de nuestras herramientas más importantes para reforzar la transparencia. Aprovechamos la ocasión para subrayar una vez más la importancia que sigue teniendo el Informe de las Naciones Unidas sobre Gastos Militares, más aún teniendo en cuenta las circunstancias actuales, y alentamos a todos los Estados a que participen activamente en la presentación de informes.

En vista de que no se han registrado novedades notables en cuanto al sistema normalizado de presentación de informes desde la aprobación, en 2019, de la anterior resolución sobre el tema, la resolución 74/24, debido también a la pandemia de coronavirus, hemos optado por conservar el texto tal como fue aprobado con anterioridad por la Primera Comisión y la Asamblea General y proponer una prórroga técnica con solo algunas actualizaciones técnicas menores. Esta resolución ha figurado en el programa de la Primera Comisión durante más de dos decenios y siempre ha gozado de apoyo abrumador por parte de los Estados Miembros de las Naciones Unidas. Esperamos que en esta sesión el proyecto de resolución reciba la misma respuesta y que los Estados Miembros muestren una vez más su apoyo aprobando el proyecto de resolución sin votación, como ha ocurrido en numerosas ocasiones en períodos de sesiones anteriores de la Primera Comisión.

Sr. Vidal (Chile): Chile suscribe la intervención realizada por Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

Valoramos los textos que están enfocados en la paridad de género y la igualdad y que refuerzan la promoción de los derechos humanos de las mujeres, las niñas y las disidencias en foros multilaterales y organismos internacionales, así como aquellos que contemplan una perspectiva de género en estas negociaciones.

En este sentido, recibimos con beneplácito el proyecto de resolución “Mujeres, desarme, no proliferación y control de armas”, presentado por Trinidad y Tabago y copatrocinado por mi país. Cabe recordar que la mención a temas de género es indispensable y se sostiene en mandatos existentes en el marco de las Naciones Unidas, especialmente en la esfera de la seguridad internacional. Se debe hacer de este un proceso inclusivo, equitativo y efectivo en materia de género.

Chile considera que las amenazas de las tecnologías de la información y las comunicaciones (TIC) pueden afectar de distinto modo a los Estados en función de sus niveles de digitalización, capacidad, seguridad y resiliencia de las TIC, su infraestructura y desarrollo. Las amenazas también pueden afectar de forma distinta a distintos grupos y entidades, teniendo especialmente presente a las mujeres y las niñas. Estados como el nuestro tienen otro tipo de amenazas y necesidades, por lo que se vuelve fundamental avanzar en mejorar nuestras capacidades, generando estructuras y planes de coordinación, no solamente a nivel de Gobierno, sino también desarrollar alianzas efectivas con la sociedad civil, el sector privado, y la academia.

Chile considera que el derecho internacional, y en particular la Carta de las Naciones Unidas, proporcionan el marco normativo aplicable que debe regular el comportamiento de los Estados en el ciberespacio, que incluye el derecho internacional humanitario, los derechos humanos y aquellas leyes que regulan la responsabilidad internacional de los Estados, por ser esenciales para mantener la paz y la estabilidad necesaria para promover un entorno abierto, seguro, estable, accesible y pacífico en las TIC.

Por todo lo anterior, apoyamos el trabajo que se desarrolla 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), dirigido por el Representante Permanente de Singapur, el programa de acción para promover el comportamiento responsable de los Estados en el uso de las TIC en el contexto internacional. Nuestro país, al igual que el resto de los miembros siempre apoyará aquellos textos que fomentan la confianza. Valoramos todas las instancias donde los Estados podemos intercambiar nuestras perspectivas, enfoques y necesidades, reforzando la seguridad, la resiliencia y el uso pacífico de las TIC en general.

Sr. Soares Damico (Brasil) (*habla en inglés*): En su informe “Asegurar nuestro futuro común: una agenda para el desarme”, el Secretario General reafirmó la necesidad de volver a situar la relación entre desarme y desarrollo en el primer plano de la conciencia internacional.

En consonancia con la opinión sostenida desde hace tiempo entre los países en desarrollo, el Brasil comparte la noción evidente de que existe una correlación positiva entre desarme y desarrollo. De hecho, la seguridad nacional e internacional son elementos esenciales para el crecimiento económico. Si los recursos financieros y tecnológicos invertidos en la ampliación de los arsenales convencionales y estratégicos se hubieran desviado a sectores cruciales de la vida humana como la educación, la sanidad y la protección del medio ambiente, habríamos estado mucho mejor. La conexión entre el desarme y los Objetivos de Desarrollo Sostenible, por tanto, debe ocupar un lugar central en nuestros esfuerzos.

El dividendo de la paz que hemos estado cosechando es bastante considerable. En 1960, el gasto militar medio representaba el 6,3 % del producto interno bruto (PIB). Sesenta años después, alcanzó su nivel más bajo: el 2,4 %. Eso significa que, en 25 años, estaríamos en condiciones de contar con un año de PIB para mejorar el bienestar social.

Sin embargo, las tensiones actuales han provocado una drástica inversión de esa tendencia. Para colmo, ello coincidió con un período de déficit públicos sin precedente, que en algunos países desarrollados alcanzaron niveles solo vistos durante la Segunda Guerra Mundial, como resultado de contrarrestar los efectos de la pandemia de enfermedad por coronavirus. El único consuelo que nos queda de esa situación es que, en un momento no muy lejano, los contribuyentes se verán obligados a decidir sobre el dilema de elegir entre la mantequilla y las armas.

El desarme, la no proliferación y el control de armamentos ya no pueden quedar confinados a la alta política. Más que nunca, reflejan opciones sociales, habida cuenta de sus enormes repercusiones en la vida cotidiana de millones de personas en todas partes, todos los días.

Nuestra actual agenda para el desarme abarca una nueva variedad de temas más cercanos a nuestras realidades, como las consideraciones de género, los debates sobre el acceso sin trabas a las tecnologías con fines pacíficos y los aspectos de seguridad de las tecnologías de la información y la comunicación. Ahora bien, esa proximidad no hace que esos temas sean menos complejos. Persiste una gran división en cuanto a la manera de abordarlos.

El Brasil considera que el debate sobre las tecnologías sensibles y emergentes ocupa un lugar destacado en las relaciones internacionales actuales. No solo hay que tener muy en cuenta las cuestiones de seguridad; también debemos abogar por un entorno abierto, accesible, pacífico y seguro para el desarrollo, el intercambio y la utilización de esas tecnologías. La prioridad es lograr un delicado equilibrio en el tratamiento de este tema para salvaguardar los incuestionables beneficios económicos y sociales que las tecnologías aportan a nuestros pueblos, así como frenar su uso malintencionado, ya sea por parte de Estados o de actores no estatales. Ese enfoque protege el derecho legítimo de todos los Estados a acceder a una tecnología que es crucial para su desarrollo, al tiempo que preserva los objetivos legítimos de la no proliferación y la seguridad internacional.

El desarrollo de las tecnologías de la información y la comunicación (TIC) se ha convertido en un tema central de debate en las sesiones de nuestra Primera Comisión. Desde 1998, se han convocado seis Grupos de Expertos Gubernamentales, de los cuales el Brasil presidió dos.

Esa determinación permanente de los miembros de mantener la cuestión de las TIC en su agenda activa es ilustrativa de su carácter estratégico y de lo urgente que resulta disponer de una regulación adecuada para preservar el ciberespacio como un entorno abierto, pacífico y accesible, así como de cuan necesario es evitar que el ciberespacio se convierta en un escenario de conflictos.

Para lograr esos objetivos, es esencial conciliar las distintas visiones del papel que desempeña el ciberespacio en nuestras sociedades y lo que queremos de él. Por su propio carácter, ese ejercicio intergubernamental se beneficiaría de las contribuciones procedentes de la sociedad civil, el mundo académico y la industria. Sin embargo, la base de ese debate descansa en la aplicabilidad del derecho internacional, especialmente de la Carta de las Naciones Unidas, y de la protección sin concesiones de los derechos humanos.

Esperamos que el actual Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones, junto con el mecanismo futuro de diálogo institucional que se establecerá con posterioridad, refuercen las nociones para el comportamiento responsable, la transparencia y las medidas de fomento de la confianza, así como la creación de capacidades, y que en ese empeño saquen provecho de la labor ya realizada en anteriores Grupos de Expertos Gubernamentales y que aparece recogida en los informes de los Grupos de trabajo de Composición Abierta aprobados por consenso.

No podemos dejar de destacar la labor realizada por el Embajador Burhan Gafoor, de Singapur, como Presidente del Grupo de Trabajo de Composición Abierta sobre la seguridad de las TIC. Acogemos con satisfacción la aprobación del informe anual en su última sesión. Esa aprobación es una buena base para la continuación de nuestra labor.

Sr. Sánchez Kiesslich: Los retos transversales relacionados con la seguridad internacional, requieren de medidas que sean integrales y vayan más allá de los entendimientos tradicionales sobre seguridad. Es por ello por lo que destacamos la importancia de todas las medidas que fortalecen los marcos regionales e internacionales existentes sobre seguridad internacional, el control de armas, el desarme y la no proliferación.

Los usos legítimos y pacíficos del ciberespacio, la resiliencia en el entorno digital y las posibilidades de las tecnologías de la información como habilitadoras del desarrollo sostenible solo pueden ser conservados y garantizados por la vía multilateral. La creciente y continua atención de la Primera Comisión a este tema debe ser interpretada como una muestra clara en el rol prioritario de las Naciones Unidas y del multilateralismo. Las

expectativas son muchas, pero serían más los retos y las amenazas sino logramos garantizar la arquitectura para el entorno digital del futuro.

Mi delegación aplaude los avances alcanzados en la inclusión de la perspectiva de género en diversas resoluciones de las Naciones Unidas y en tratados multilaterales relacionados con la Primera Comisión. Al igual que otras delegaciones consideramos que la participación plena, igualitaria y significativa de las mujeres en los esfuerzos encaminados al desarme y la no proliferación son un elemento fundamental para lograr la paz sostenible. Seguiremos promoviendo y apoyando aquellas iniciativas que aspiren a incrementar la participación de las mujeres en los procesos de toma de decisión en este campo. Es por ello por lo que este año, al igual que en otras ocasiones, nos complace copatrocinar el proyecto de resolución A/C.1/77/L.18, "Mujeres, desarme, no proliferación y control de armamentos".

Asimismo, México continúa firmemente comprometido con la educación para el desarme como medida de prevención. Consideramos que esta es una estrategia que fomenta la conciencia sobre el impacto del uso de cualquier tipo de arma en la sociedad y en nuestro entorno, además de que aporta a la formación de nuevas generaciones interesadas y como nuevos agentes de cambio en los asuntos de desarme y seguridad internacional.

Este año, nos complace presentar nuevamente los proyectos de resolución bienales sobre el Programa de las Naciones Unidas sobre Información para el Desarme (A/C.1/77/L.20) y el estudio de las Naciones Unidas sobre la educación para el desarme (A/C.1/77/L.15). Esperamos que dichos proyectos de resolución cuenten con el apoyo de todas las delegaciones.

Finalmente, nos enorgullece ver a tres mexicanos como parte de la iniciativa "#Leaders4Tomorrow", y esperamos que sus inspiradores proyectos lleguen a muchos más jóvenes y logren difundir la importancia del desarme en sus entornos.

Sr. Tun (Myanmar) (*habla en inglés*): Myanmar hace suyas las declaraciones formuladas en nombre del Movimiento de Países No Alineados y de la Asociación de Naciones de Asia Sudoriental (véase A/C.1/77/PV.18).

No cabe duda de que muchos aspectos de nuestras vidas se paralizarían si no existieran las tecnologías de la información y la comunicación (TIC). El crecimiento exponencial de las TIC nos ha permitido aprovechar oportunidades y avances socioeconómicos sin precedentes, que benefician a todos en todo el mundo, incluso a quienes no tienen acceso a las TIC o tienen una comprensión muy limitada de esa tecnología.

Al mismo tiempo, el ciberespacio es cada vez más susceptible a los actores maliciosos y no estatales, cuyo dominio de esa compleja tecnología crece al mismo ritmo que las propias TIC. Las omnipresentes ciberamenazas, que son transfronterizas, escurridizas y cambiantes, tienen graves consecuencias para la paz y la seguridad internacionales y para nuestra vida cotidiana. El ciberespacio ya se ha convertido en un foro para la guerra, como hemos podido comprobar en los dos últimos decenios.

De manera que es imprescindible que todos utilicemos las normas y los estándares internacionales como guías para minimizar las ciberamenazas y maximizar los beneficios de las TIC. A ese respecto, Myanmar desea subrayar el papel principal que desempeñan las Naciones Unidas y los esfuerzos multilaterales que realizan los Estados Miembros para hacer frente a los retos de la ciberseguridad y construir un entorno de seguridad protegido y estable. En consecuencia, Myanmar reitera su apoyo a la labor del Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones y de su uso 2021-2025 y acoge con satisfacción la aprobación por consenso, en julio de 2022, del primer informe anual sobre la marcha de los trabajos.

Pedimos a todas las partes que colaboren de buena fe y con la máxima flexibilidad para que el Grupo de Trabajo de Composición abierta siga avanzando. También apreciamos enormemente la importante labor del Grupo de Expertos Gubernamentales que ha hecho valiosas contribuciones en este ámbito.

Condenamos el uso de las TIC como arma para suprimir los derechos fundamentales y la libertad de expresión. En Myanmar, mi país de origen ya no es posible una Internet libre, segura y abierta, pues la Junta Militar ejerce una dictadura digital. Las escuchas telefónicas y los ciberataques contra su propio pueblo, incluidos los ciudadanos de Myanmar que viven en el extranjero, son la nueva norma. La Junta ha vigilado de manera continua las actividades de los funcionarios en las redes sociales. La Junta también está tratando de promulgar una ley de ciberseguridad draconiana que está específicamente concebida para eliminar cualquier disidencia o expresión en su contra. Instamos a la comunidad internacional y a la industria tecnológica a que ayuden a poner fin al uso indebido que hace la Junta de las TIC en su empeño por aferrarse al poder.

Aprovecho esta oportunidad para señalar a su atención, Sr. Presidente, los atroces crímenes cometidos recientemente por el régimen militar fascista contra la minoría étnica kachín. En la noche del 23 de octubre, aviones de combate militares terroristas bombardearon y atacaron un concierto de música que tenía lugar en A Nang Pa, en la Brigada 9 del Ejército Independiente Kachín, en el estado de Kachín (Myanmar), durante la celebración del 62º Día de la Organización Independiente Kachín, aniversario que se conmemora cada 25 de octubre. Según se informa, murieron aproximadamente 100 personas, entre ellas artistas, mujeres y niños, y muchas otras resultaron heridas. Eso es claramente un crimen de lesa humanidad y un crimen de guerra. No se trata de un incidente aislado. En los últimos 20 meses los militares terroristas han llevado a cabo más de 250 ataques aéreos contra la población civil en todo el país, en particular en las zonas étnicas, y han cometido varias masacres. Mientras los militares sigan teniendo acceso a las armas y a las tecnologías, seguirán cometiendo atrocidades brutales e inhumanas contra la población, lo que incluye a los niños. Quiero pedir a los Estados Miembros que exportan armas y tecnologías mortíferas a los militares que dejen de hacerlo de inmediato. Creemos que así se salvarán vidas en el pueblo de Myanmar.

Para concluir, reafirmamos nuestra voluntad de crear un ciberespacio seguro y pacífico en el que no se permitan infames que socaven la paz y la seguridad internacionales y en el que se promueva el derecho internacional, las libertades fundamentales y los derechos humanos.

Sr. Balouji (República Islámica del Irán) (*habla en inglés*): Mi delegación hace suya la declaración formulada por la representante de Indonesia en nombre del Movimiento de Países No Alineados (véase A/C.1/77/PV.18).

La República Islámica del Irán reitera una vez más que se mantiene firme en su posición de que el ciberespacio y el entorno de las tecnologías de la información y las comunicaciones, como patrimonio común de la humanidad, deben utilizarse exclusivamente con fines pacíficos y que los Estados deben actuar de forma cooperativa y respetando plenamente el derecho internacional aplicable. Partiendo de ese punto de vista, el Irán ha participado activamente en los procesos de negociaciones intergubernamentales pertinentes, bajo los auspicios de las Naciones Unidas, en favor de los derechos de todos, al tiempo que se determinan las responsabilidades adecuadas para todos. Después de la aprobación del primer informe anual del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, y de un compendio de declaraciones de los Estados Miembros en explicación de posición, incluida una declaración del Irán, consideramos que los avances futuros y el aumento de la eficiencia del Grupo dependerán de lo siguiente.

En primer lugar, es fundamental que en debates futuros se examine la lista de propuestas no exhaustivas y diversas formuladas sobre la elaboración de reglas, normas y principios de comportamiento responsable de los Estados, tal y como se refleja en el resumen de la Presidencia contenido en el informe del Grupo de Trabajo de Composición Abierta de 2021, y que se tome una decisión al respecto.

En segundo lugar, de conformidad con el mandato del Grupo de Trabajo de Composición Abierta, se debe entablar, bajo los auspicios de las Naciones Unidas, un diálogo institucional periódico con amplia participación de los Estados. En este sentido, todas las iniciativas nacionales deben ser tratadas por igual, al tiempo que se tienen en cuenta las preocupaciones e intereses de todos los Estados.

En tercer lugar, pedimos a los Estados que sigan participando de forma constructiva en las negociaciones durante las nuevas actividades del Grupo, incluso entre períodos de sesiones.

En cuarto lugar, pedimos al Grupo de Trabajo de Composición Abierta que establezca, de conformidad con su mandato, subgrupos temáticos para cumplir su mandato y facilitar el intercambio de opiniones entre los Estados, así como para elaborar los informes posteriores mediante negociaciones basadas en textos. Desde otra perspectiva, y habida cuenta de las realidades sobre el terreno, es importante señalar que países como los Estados Unidos no solo han comenzado a utilizar el ciberespacio como arma, sino que sus ejércitos también han empezado a realizar numerosos ciberataques. El régimen israelí también ha lanzado múltiples ciberataques contra el Irán.

Mi país viene siendo desde hace tiempo el blanco primordial y la principal víctima de ciberataques contra su infraestructura crítica, que han interrumpido la prestación de servicios públicos y las funciones gubernamentales. Los ataques perpetrados por el gusano informático Stuxnet contra las instalaciones nucleares que con fines pacíficos opera el Irán, al igual que los recientes ataques contra la infraestructura industrial, como las industrias siderúrgica y petroquímica, las gasolineras y los sistemas de servicios públicos municipales, son

algunos ejemplos de ese tipo de ciberataques. El régimen israelí ha admitido en repetidas ocasiones su participación en tales hechos internacionalmente ilícitos sirviéndose del entorno de las tecnologías de la información y las comunicaciones, y ha recibido el apoyo incondicional de los Estados Unidos. Condenamos todos esos ataques e instamos a la comunidad internacional a exigir cuentas a sus autores.

Lamentablemente, el Irán ha sido en los últimos tiempos objeto de acusaciones falsas y sin fundamento de haber estado implicado en un presunto ciberataque. Rechazamos cualquier acusación falsa basada en suposiciones erróneas e invenciones que se haga contra nuestro país con fines políticos. Habida cuenta el carácter y las características técnicas del ciberespacio y de las dificultades que plantea la atribución en el entorno de las tecnologías de la información y las comunicaciones, el Irán advierte sobre las repercusiones negativas que las atribuciones falsificadas y manipuladas pueden tener para los Estados. Si el Reino Unido estuviera realmente preocupado por los posibles efectos en la seguridad y las condiciones económicas, sociales y humanitarias, se abstendría de hacer acusaciones precipitadas que puedan difundir información falsa.

Para concluir, debo decir que para la República Islámica del Irán la mejor manera de garantizar un entorno seguro y protegido para las tecnologías de la información y las comunicaciones es seguir conformando un cuerpo de normas y reglas jurídicas internacionales que prevengan el uso malintencionado de esas tecnologías y del ciberespacio, y sirvan como un instrumento jurídicamente vinculante para el arreglo pacífico de controversias.

El Presidente (*habla en inglés*): Tiene ahora la palabra el observador de la Santa Sede.

El Arzobispo Caccia (Santa Sede) (*habla en inglés*): El Papa Francisco, en su encíclica *Fratelli Tutti*, escribió que el número cada vez mayor de interdependencias y de comunicaciones que se entrecruzan en nuestro planeta hace más palpable la conciencia de que todas las naciones de la tierra comparten un destino común. Sin embargo, esa unidad se ve amenazada por el creciente uso malintencionado de las tecnologías de la información y las comunicaciones por parte de agentes estatales y no estatales. Ese uso malintencionado de las tecnologías de la información y las comunicaciones se debe, en parte, a que nuestro inmenso desarrollo tecnológico no estuvo acompañado de un desarrollo en la responsabilidad, los valores y la conciencia humanos. A este respecto, la Santa Sede acoge con beneplácito la convocatoria del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, que brinda una oportunidad apropiada para corregir ese desequilibrio. Mi delegación ha seguido esas reuniones con gran interés y de cara al futuro seguirá participando activamente en sus deliberaciones. La red de sistemas interconectados que conforma el ciberespacio constituye un entorno compartido, cuyo mantenimiento exige que todos pasemos del paradigma de la competencia al de la cooperación. Llevar a cabo ese cambio exige un conjunto de principios comunes. Teniendo eso presente, permítase a mi delegación compartir algunas observaciones.

En primer lugar, el comportamiento de los Estados en el ciberespacio debe respetar la dignidad inherente que hay en cada persona. Para eso, los Estados deben promover y proteger la libertad de expresión en línea de todas las personas. Esa libertad, que es fundamental para la propia búsqueda de la verdad, también tiene sus límites, al verse restringida por el orden moral y el interés común. La defensa de la dignidad humana en el ciberespacio obliga a los Estados a respetar también el derecho a la privacidad, protegiendo a sus ciudadanos de la vigilancia intrusiva y permitiéndoles salvaguardar su información personal de accesos no autorizados.

En segundo lugar, los Estados deben garantizar que quienes se encuentren en una situación más vulnerable estén protegidos frente a cualquier daño. Eso significa no solo proteger la propia infraestructura crítica, como los hospitales, las redes de abastecimiento de agua, las centrales eléctricas y las instalaciones que contienen fuerzas peligrosas, sino también abstenerse de cualquier actividad que dañe intencionadamente la infraestructura crítica de otro Estado.

En tercer lugar, los Estados deben guiarse por la justicia, lo que exige que los Estados que estén en condiciones de hacerlo contribuyan de manera efectiva a los esfuerzos por cerrar la brecha digital. Esa división no solo conduce a la disparidad de los patrones de desarrollo humano, sino que también crea vulnerabilidades cibernéticas que amenazan a todos los países. Para hacer frente a esas vulnerabilidades, la Santa Sede alienta los esfuerzos de creación de capacidades en beneficio de los Estados que no participan en pie de igualdad de los frutos de la revolución digital. La creación de capacidades debe permanecer políticamente neutra y sin condiciones.

La humanidad ha entrado en una nueva era en la que nuestras proezas técnicas nos han llevado a una

encrucijada que en la que se nos presentan grandes oportunidades y grandes riesgos. Velar por que los nuevos avances en el ámbito de las tecnologías de la información y las comunicaciones contribuyan al desarrollo humano integral exige que constantemente evaluemos cómo aplicar los nuevos instrumentos de una manera que defienda la dignidad humana. Mi delegación espera que esos esfuerzos, así como la elaboración más detallada del marco de comportamiento responsable de los Estados por parte por el Grupo de Trabajo de Composición Abierta, nos permitan regocijarnos por esos avances y entusiasmarnos con las inmensas posibilidades que se siguen abriendo ante nosotros.

El Presidente (*habla en inglés*): La Comisión ha escuchado al último orador sobre el grupo temático "Otras medidas de desarme y seguridad internacional".

A continuación, daré la palabra a quienes hayan solicitado intervenir en ejercicio de su derecho a contestar. En ese sentido, quisiera recordar a las delegaciones las limitaciones de tiempo y pedirles que sean conscientes de ellas.

Sr. Shin (Federación de Rusia) (*habla en ruso*): Quisiera ejercer el derecho a contestar en respuesta a la retórica hostil contenida en algunas de las declaraciones que escuchamos hoy.

Debo admitir que me han molestado bastante las declaraciones de los representantes de los Estados Unidos, la Unión Europea, el Reino Unido, Australia y varios otros Estados, en las que afirmaron su apoyo al 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 hablaron de los aspectos positivos de ese mecanismo. Recuerdo claramente que fueron esos mismos países los que votaron en contra de la creación del Grupo de Trabajo de Composición Abierta, y no solo una vez, sino dos. ¿Significa eso que ahora no están diciendo la verdad? ¿Por qué debemos creer en sus palabras o acciones? Ahora promueven con firmeza el proyecto de resolución A/C.1/77/L.73, relativo a un programa de acción sobre cuestiones relacionadas con la cibernética, diciendo que lo hacen en interés del Grupo de Trabajo de Composición Abierta. Quisiera pedirles que aclaren exactamente de qué están hablando. Cuanto más oímos hablar del programa de acción, más preguntas tenemos.

No entendemos por qué se pide a los Estados Miembros de las Naciones Unidas que primero creen ese formato y entonces, después decidan lo que realmente va a hacer, lo que incluye el mecanismo de adopción de decisiones y la financiación del proceso. En esencia, se nos está pidiendo que pongamos la carreta delante de los bueyes. ¿Por qué no debatir primero esa iniciativa en el marco del Grupo de Trabajo de Composición Abierta, en pleno cumplimiento de su mandato y de los acuerdos de consenso anteriores? Consideramos que un período de tres años, hasta 2025, es tiempo más que suficiente para llegar de manera conjunta a un entendimiento respecto de la viabilidad de crear dicho formato y su posible alcance y modalidades.

Francamente, las acciones de Francia y sus asociados parecen un intento de crear un mecanismo que sería adecuado solo para unos pocos, predominantemente los Estados occidentales. En ese contexto, estarían tomando decisiones e imponiéndolas a la gran mayoría. Francamente, en ese sentido, tal iniciativa se asemeja a un manifiesto de cibercolonialismo. La decisión de que entidades no estatales participen en el Grupo de Trabajo de Composición Abierta es, como todos sabemos, un derecho soberano de los Estados.

Las solicitudes de muchas organizaciones rusas también se rechazaron sin explicación alguna. En nuestra opinión, antes de hablar de permitir la participación de organizaciones no gubernamentales en los procesos de negociación interestatales, primero habría que garantizar el acceso sin trabas de los Estados y sus delegaciones nacionales a la plataforma de las Naciones Unidas. En este sentido, quisiéramos protestar enérgicamente contra las medidas del Gobierno de los Estados Unidos, que, con su uso de los visados como arma, ha incumplido en forma sistemática sus obligaciones como Estado anfitrión de la Sede de las Naciones Unidas.

Seguimos escuchando acusaciones absolutamente infundadas contra Rusia en relación con la ciberagresión, incluido en el contexto de la operación militar especial en Ucrania. En lugar de utilizar los canales de comunicación establecidos de los organismos competentes, nuestros colegas occidentales han pasado a criticar a determinados Estados que les desagradan sobre la base de afirmaciones infundadas, distrayendo a la opinión pública mundial de sus propias acciones. El objetivo de su retórica es encubrir una campaña de ciberagresión sin precedentes contra Rusia y otros Estados. Hay muchas pruebas que demuestran que los servicios de inteligencia de los Estados Unidos y los países de la OTAN han realizado actividades sistemáticas y agresivas en el ciberespacio. Recuerdo las revelaciones de Edward Snowden y, como otro ejemplo, el informe publicado recientemente por nuestros colegas chinos sobre los ciberataques contra la Universidad Politécnica

Northwestern, que se llevaron a cabo con la participación directa de la Agencia de Seguridad Nacional de los Estados Unidos. No ocultan sus esfuerzos para practicar la guerra cibernética y realizar ejercicios, además de invitar a representantes ajenos a su bloque para que asistan a ellos. Además, el Comandante del Comando Cibernético de los Estados Unidos, Paul Nakasone, ha reconocido públicamente que su país está llevando a cabo ciberoperaciones ofensivas contra Rusia, incluso, principalmente, utilizando el ejército de tecnología de la información de Ucrania, creado por los propios estadounidenses.

Desde principios de este año, el número de ataques a los recursos de la red rusa se ha multiplicado por más de cuatro en relación con el mismo período del año pasado. La mayoría de esos ataques tienen su origen en los Estados Unidos o en países de la Unión Europea. La magnitud de las ciberagresiones demuestra que los Gobiernos de los países occidentales la llevan a cabo de forma coordinada, en cooperación con comunidades de *hackers* y empresas privadas. Desgraciadamente, no dispongo de tiempo suficiente para entrar en detalles sobre el tema, pero es importante entender que una escalada de tensiones en el ciberespacio no redunda en interés de la comunidad internacional, que se beneficiaría más de la prevención de conflictos y del uso de las tecnologías de la información y las comunicaciones con fines pacíficos y de desarrollo.

Sr. Kim Song (República Popular Democrática de Corea) (*habla en inglés*): Mi delegación se siente obligada a hacer uso de la palabra para ejercer su derecho de réplica en respuesta a la observación irresponsable de la representante del Reino Unido.

Rechazamos categóricamente la acusación infundada formulada por el Reino Unido contra la República Popular Democrática de Corea. Conocemos bien el mal hábito del Reino Unido de acusar temerariamente a otros sin pruebas concretas. Por otra parte, el Reino Unido está participando activamente en diferentes tipos de actos maliciosos en el ciberespacio a través de herramientas como Cinco Ojos para inmiscuirse en los asuntos internos de los Estados soberanos. La acusación del Reino Unido es como si la parte culpable presentara primero una demanda.

No esperamos nada diferente del Reino Unido, que sigue ciegamente los pasos de la política hostil de los Estados Unidos contra la República Popular Democrática de Corea, cuyo objetivo es demonizar a nuestro país en el ámbito internacional e imponer la llamada cooperación internacional para ejercer presión sobre la República Popular Democrática de Corea. La acusación infundada del Reino Unido revela con claridad un prejuicio y una hostilidad extremos contra la República Popular Democrática de Corea. Instamos encarecidamente al Reino Unido a que recupere la cordura y reflexione sobre su comportamiento imprudente e indignante.

Sr. Li Song (China) (*habla en chino*): China toma nota de las acusaciones infundadas de la representante del Reino Unido contra las actividades cibernéticas de China y rechaza firmemente a esas acusaciones.

China está firmemente decidida a preservar la ciberseguridad. También es una de las principales víctimas de los ciberataques. De conformidad con la ley, el Gobierno de China se opone y combate con firmeza a todas las formas de ciberataque, lo que demuestra plenamente nuestra actitud responsable en el ámbito de la ciberseguridad.

China desea subrayar que la ciberseguridad es un desafío común al que se enfrentan todos los países. Todos los países deben, sobre la base del respeto mutuo, la igualdad y el beneficio mutuo, buscar el diálogo y la cooperación para responder de manera conjunta a las amenazas a la ciberseguridad. Instamos a los países en cuestión a que pongan fin a sus calumnias y acusaciones infundadas contra China con respecto a la cuestión de los ciberataques y adopten efectivamente una actitud responsable, colaborando con todas las partes a fin de salvaguardar la paz y la seguridad en el ciberespacio.

Sr. Bourgel (Israel) (*habla en inglés*): Me veo obligado a hacer uso de la palabra en relación con las referencias relativas a mi país formuladas por el representante de la República Islámica del Irán. Israel rechaza esas acusaciones fraudulentas. Teniendo en cuenta el comportamiento del Irán en el ciberespacio, y sobre todo su reciente y peligroso ciberataque contra la infraestructura de Albania, sus observaciones no dejan de ser absurdas.

En este sentido, permítaseme también condenar los dos recientes ciberataques contra las operaciones de las Naciones Unidas para el mantenimiento de la paz, ambos perpetrados por el régimen iraní y sus agentes. Como en tantas otras cuestiones que debate la Comisión, el Irán está trabajando de manera sistemática contra la comunidad internacional para provocar el colapso de los foros de control de armamentos. Del mismo modo que el Irán patrocina y apoya a grupos terroristas para suscitar el temor entre los Estados de toda la región, intenta utilizar herramientas maliciosas en el ámbito de la tecnología de la información y las comunicaciones, así

como generar el miedo y la destrucción entre los Estados de todo el mundo.

Sra. McIntyre (Francia) (*habla en francés*): Deseo ejercer el derecho de mi país a contestar a las observaciones formuladas por la delegación de la Federación de Rusia en relación con el proyecto de resolución A/C.1/77/L.73, presentado por mi país, sobre un programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

Como saben los miembros, Francia propuso —a todos los Estados Miembros de las Naciones Unidas, de manera transparente y abierta— un proyecto de resolución cuyo objetivo es establecer un programa de acción para la creación de capacidad en cuestiones relacionadas con la cibernética. El proyecto de resolución se debatió abierta y extensamente durante cuatro rondas de consultas abiertas celebradas aquí en Nueva York y anteriormente en Ginebra. El proyecto de resolución se ha mejorado considerablemente a fin de tener en cuenta las numerosas propuestas formuladas por las delegaciones, por lo cual les estamos muy agradecidos.

El proyecto de resolución se basa en las consultas celebradas anteriormente para establecer el Programa de Acción para Prevenir, Combatir y Eliminar el Tráfico Ilícito de Armas Pequeñas y Ligeras en Todos Sus Aspectos. Quisiera recordar a los miembros el proceso observado al respecto, que supuso, en primer lugar, un informe del Secretario General y, después, dos años de consultas con el fin de tener en cuenta las sugerencias de todos los Estados Miembros en relación con el contenido del Programa de Acción. Por último, el Programa de Acción se aprobó en una conferencia internacional celebrada al final del proceso. Esa es precisamente la secuencia de acontecimientos que proponemos seguir en el examen del proyecto de resolución A/C.1/77/L.73, confiando al Secretario General la tarea de presentar el año próximo un informe en el que se especifiquen las modalidades y el contenido del futuro programa de acción, todo ello respetando plenamente las prerrogativas del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso para el período de 2021 a 2025, que, por supuesto, también deberá debatir las modalidades del programa de acción antes de que los Estados Miembros procedan a su aprobación, si así lo desean.

Por consiguiente, recuerdo que nuestro proceso es abierto, transparente e inclusivo y tiene como objetivo respetar todo el proceso acordado por los Estados Miembros, incluso en el seno del Grupo de trabajo de composición abierta. Seguiremos adoptando ese enfoque transparente e inclusivo hasta que concluyan los debates.

Sr. Balouji (República Islámica del Irán) (*habla en inglés*): Me veo obligado a hacer uso de la palabra para rechazar las acusaciones del representante israelí contra mi país.

No nos sorprenden esas mentiras difundidas por el representante del régimen, ya que el régimen no respeta el derecho internacional. Ha iniciado continuamente ciberataques contra numerosos sectores en el Irán, que van desde las instalaciones nucleares pacíficas hasta los servicios públicos, como es el caso de la ayuda de emergencia. Conocemos bien el carácter opresivo y discriminatorio del régimen israelí, su oscuro historial en materia de derechos humanos y su menosprecio por los llamamientos internacionales a adherirse al Tratado sobre la No Proliferación de las Armas Nucleares, la Convención sobre las Armas Químicas y la Convención sobre Armas Biológicas, entre otros.

Israel ha violado 29 resoluciones del Consejo de Seguridad, que son jurídicamente vinculantes para los Estados Miembros en virtud del Artículo 25 de la Carta de las Naciones Unidas, incluidas las resoluciones 54 (1948), 111 (1956), 233 (1967), 234 (1967), 236 (1967), 248 (1968), 250 (1968), 252 (1968), 256 (1968), 262 (1968), 267 (1969), 270 (1969), 280 (1970), 285 (1970), 298 (1971), 313 (1972), 316 (1972), 468 (1980), 476 (1980) y —por último, pero no por ello menos importante— la resolución 2231 (2015), que no ha perdido oportunidad ni escatimado esfuerzos para convertirla en letra muerta. Un régimen así no tiene base moral para hablar de respeto de las normas del derecho internacional ni de adhesión al derecho internacional.

Cuando se trata de ciberseguridad, la situación es aún peor. Lo que hemos dicho no son acusaciones, ya que todos los observadores internacionales han confirmado las acciones irresponsables de Israel, que condenamos con firmeza.

El Presidente (*habla en inglés*): Hemos escuchado al último orador en el ejercicio del derecho de respuesta.

Disponemos de un poco de tiempo, así que tratemos de aprovechar al máximo esos pocos minutos. Permítaseme la indulgencia de retomar el grupo temático “Desarme regional y seguridad”. Tenemos una larga lista de oradores para el grupo temático, por lo que pido la cooperación plena de las delegaciones.

Sra. Kristanti (Indonesia) (*habla en inglés*): Tengo el honor de hablar en nombre del Movimiento de Países No Alineados (MNOAL).

El Movimiento de Países No Alineados reitera su profunda preocupación por el hecho de que se recurra cada vez más al unilateralismo y, en ese contexto, subraya que el multilateralismo y las soluciones acordadas de forma multilateral, de conformidad con la Carta de las Naciones Unidas, constituyen el único método sostenible para abordar las cuestiones relativas al desarme y la seguridad internacional. El MNOAL también subraya su posición de principio con respecto al no uso o la amenaza de uso de la fuerza contra la integridad territorial de cualquier Estado.

Los Estados del MNOAL que son partes en el Tratado sobre la No Proliferación de las Armas Nucleares están profundamente preocupados por las doctrinas de defensa estratégica de los Estados poseedores de armas nucleares y de ciertos Estados no poseedores de armas nucleares que suscriben las garantías ampliadas de seguridad nuclear proporcionadas por los Estados poseedores de armas nucleares. Estos no solo establecen justificaciones para el empleo o la amenaza de empleo de armas nucleares, sino que también mantienen postulados injustificables en materia de seguridad internacional basados en la promoción y el establecimiento de alianzas militares y políticas de disuasión nuclear. Por lo tanto, el MNOAL insta a los Estados en cuestión a que excluyan por completo el empleo o la amenaza de empleo de armas nucleares de sus doctrinas militares y de seguridad.

El MNOAL reitera su pleno apoyo al establecimiento en Oriente Medio de una zona libre de armas nucleares y todas las demás armas de destrucción masiva. Como medida prioritaria para tal fin, el MNOAL reafirma la necesidad de que se establezca rápidamente en Oriente Medio una zona libre de armas nucleares, de conformidad con la resolución 487 (1981) del Consejo de Seguridad y el párrafo 14 de la resolución 687 (1991) del Consejo de Seguridad, así como con las resoluciones pertinentes de la Asamblea General. El MNOAL exhorta a todas las partes interesadas a tomar medidas urgentes y prácticas encaminadas al cumplimiento de la propuesta presentada por el Irán en 1974 con miras a establecer dicha zona.

Los Estados del MNOAL que son partes en el TNP reiteran su profunda decepción por el hecho de que no se haya implementado el Plan de Acción de 2010 sobre la creación en Oriente Medio de una zona libre de armas nucleares y de todas las demás armas de destrucción masiva. Esos Estados rechazan firmemente las trabas que impiden que se aplique el Plan de Acción de 2010 y la resolución de 1995 relativos a Oriente Medio. El MNOAL insiste en la responsabilidad especial que incumbe a los Estados copatrocinadores de la resolución de 1995 relativa a Oriente Medio en lo referente a su aplicación. Al MNOAL le preocupa que el hecho de que siga sin aplicarse la resolución de 1995, contraria a las decisiones aprobadas en las correspondientes conferencias de examen del TNP, socave la eficacia y credibilidad del TNP y perturbe el delicado equilibrio existente entre sus tres pilares.

En ese sentido, el MNOAL saluda la convocatoria del primer período de sesiones de la Conferencia sobre la Creación en Oriente Medio de una Zona Libre de Armas Nucleares y Otras Armas de Destrucción Masiva, de conformidad con la decisión 73/546, que presidió el Reino Hachemita de Jordania, y el hecho de que la Conferencia haya aprobado una declaración política. Asimismo, el MNOAL acoge con beneplácito la convocatoria del segundo período de sesiones de la Conferencia presidida por el Estado de Kuwait y sus resultados, entre ellos la aprobación del reglamento y el establecimiento de un comité de trabajo oficioso. Además, el MNOAL espera con interés la celebración del tercer período de sesiones de la Conferencia y reitera su llamamiento a todos los Estados de la región, sin excepción, para que participen de forma activa en ese encuentro, negocien de buena fe y firmen un tratado jurídicamente vinculante sobre el establecimiento de la zona.

El MNOAL considera que las zonas libres de armas nucleares establecidas por los Tratados de Tlatelolco, Rarotonga, Bangkok y Pelindaba, el Tratado sobre la zona libre de armas nucleares de Asia Central y el estatuto de Mongolia como país libre de armas nucleares constituyen pasos positivos y medidas relevantes encaminadas a reforzar el desarme nuclear y la no proliferación nuclear a escala mundial. En el contexto de las zonas libres de armas nucleares, es fundamental que los Estados poseedores de armas nucleares ofrezcan garantías incondicionales contra el uso o la amenaza del uso de armas nucleares a todos los Estados de las zonas bajo cualquier circunstancia. El MNOAL hace un llamamiento a todos los Estados poseedores de armas nucleares para que ratifiquen los protocolos relacionados con todos los tratados por los que se establecen zonas libres de armas nucleares, retiren toda reserva o declaración interpretativa incompatible con el objeto y propósito de los tratados, y respeten el carácter desnuclearizado de esas zonas. El

MNOAL insta a los Estados a celebrar acuerdos libremente concertados entre los Estados de una región interesada con miras a establecer nuevas zonas libres de armas nucleares en las regiones donde no existan.

Para concluir, el MNOAL subraya la importancia de las actividades que desarrollan las Naciones Unidas en el plano regional, encaminadas a aumentar la estabilidad y la seguridad de sus Estados Miembros, actividades que podrían promoverse de manera sustantiva manteniendo y revitalizando los tres centros regionales para la paz y el desarme.

Sr. Fuller (Belice) (*habla en inglés*): Tengo el honor de intervenir en nombre de los 14 Estados miembros de la Comunidad del Caribe (CARICOM) en el marco del grupo temático regional sobre el desarme y la seguridad.

Los Estados miembros de la CARICOM han adoptado un enfoque cooperativo, coordinado y práctico en los planos regional y subregional a fin de hacer frente a las diversas amenazas a la seguridad que se ciernen sobre la región. La CARICOM está plenamente determinada a desempeñar el papel que le corresponde en los esfuerzos globales orientados a velar por nuestra seguridad colectiva mediante el cumplimiento de nuestras obligaciones internacionales. Los enormes esfuerzos encaminados a lograr el desarme regional complementan nuestra labor global.

La seguridad es un pilar esencial de nuestra integración regional. La CARICOM ha establecido un marco institucional regional orientado a apoyar la cooperación regional, en el que se incluye su Agencia de Implementación para el Crimen y la Seguridad, que es supervisada por el Consejo de Ministros para la Seguridad y la Aplicación de la Ley y complementado por otras instituciones regionales, como el Sistema de Seguridad Regional.

Las corrientes ilícitas de armas de fuego y municiones a través de la región siguen siendo un desafío importante y se identifican como una amenaza de primer nivel en la Estrategia de Seguridad Regional de la CARICOM. De cada diez homicidios que se producen en la región, siete están relacionados con el uso de armas pequeñas y armas ligeras. Se calcula que solo en Haití circulan más de medio millón de armas de fuego ilegales. Las armas de fuego ilegales desempeñan un papel clave en todos los aspectos de la delincuencia organizada transnacional y como instrumento de apoyo a los comportamientos delictivos y fuera de la ley. Por ello, tiene efectos socioeconómicos y costos humanos considerables.

Ningún Estado miembro de la CARICOM fabrica ni importa una cantidad significativa de armas de fuego. Para la región, es sumamente prioritario cortar e impedir la introducción de armas de fuego y municiones ilegales a través de nuestras fronteras. A pesar de las numerosas iniciativas y mecanismos destinados a abordar los problemas relacionados con la violencia armada, en la región persisten niveles elevados de delitos asociados a las armas de fuego.

En la Estrategia para el Crimen y la Seguridad de la CARICOM se señala que, si bien la región respeta los derechos de otros Estados a establecer políticas liberales sobre el acceso a las armas, las repercusiones negativas de esas políticas no se limitan a las fronteras de los Estados, sino que tienen consecuencias de suma gravedad para otros países, entre los que se encuentran los miembros de la CARICOM. Por lo tanto, prevenir el tráfico ilícito de armas es una responsabilidad común no solo de los Estados de la CARICOM, sino también de los países de los que proceden esas armas. Por otra parte, durante su 43ª reunión ordinaria, celebrada en Suriname el 3 de julio de 2022, nuestros Jefes de Gobierno expresaron sentirse especialmente preocupados por la llegada de armas procedentes de fuera de la región.

En 2020, los líderes de la CARICOM aprobaron la Hoja de Ruta para Implementar las Acciones Prioritarias del Caribe sobre la Proliferación Ilícita de Armas de Fuego y Municiones en Todo el Caribe de Manera Sostenible para 2030. La Agencia de Implementación de la CARICOM para el Crimen y la Seguridad está adoptando varias medidas concretas encaminadas a aplicar la Hoja de Ruta, entre las que destaca la prestación de asistencia técnica y asesoramiento a las autoridades nacionales; el fomento de las capacidades y las actividades de formación; el intercambio de información e inteligencia; el control fronterizo y aduanero; y el apoyo legislativo mediante el desarrollo de leyes modelo, el suministro de instrumentos operativos y la elaboración de marcos regulatorios, de políticas y de normas internacionales, regionales y nacionales.

Deseamos destacar la labor que viene realizando la Agencia de Implementación en la región con el apoyo de Gobiernos y organizaciones asociados, labor que, entre otras cosas, incluye la realización de un estudio exhaustivo y basado en datos, en colaboración con Small Arms Survey (SAS), sobre el tráfico ilícito de armas hacia el Caribe y dentro de la región y sobre los costos socioeconómicos de ese tráfico; la creación de una unidad de inteligencia de la CARICOM para delitos cometidos con armas de fuego que debe ayudar a los Estados miembros de la Comunidad a investigar y enjuiciar ese tipo de delitos, que contará con el apoyo de organismos

del Gobierno de los Estados Unidos, como la Agencia de Alcohol, Tabaco, Armas de Fuego y Explosivos, el Departamento de Seguridad Nacional y la Oficina de Aduanas y Protección Fronteriza; la prestación de asistencia a los Estados miembros de la CARICOM en materia de gestión de armas de fuego y municiones; el establecimiento de importantes alianzas con numerosos organismos internacionales para colaborar en la lucha contra la delincuencia armada, entre los que se incluyen INTERPOL, la Organización Mundial de Aduanas (OMA), la Oficina de las Naciones Unidas contra la Droga y el Delito, el Centro Regional de las Naciones Unidas para la Paz, el Desarme y el Desarrollo en América Latina y el Caribe (UNLIREC), SAS y Mines Advisory Group; la realización de operaciones conjuntas con INTERPOL en todo el Caribe en el ámbito de las armas de fuego del 24 al 30 de septiembre de 2022, que llevaron al decomiso de unas 320 armas, 3.300 cartuchos y un volumen histórico de drogas; la realización de actividades de formación y desarrollo de la capacidad con las instituciones policiales y de seguridad —incluidas las instituciones aduaneras— en colaboración con la OMA; la prestación de apoyo a los Estados miembros en la utilización de la Red Regional Integrada de Información Balística; el mejoramiento y la ampliación del sistema de información anticipada sobre los pasajeros de la CARICOM, que es el único sistema multilateral del mundo que permite a los Estados participantes verificar de manera eficaz en cada uno de sus puertos de entrada a las personas de interés que se encuentran a bordo de una aeronave o de un buque, lo que tiene por objeto garantizar la participación de todos los Estados miembros de la CARICOM y de terceros Estados que estén interesados; el establecimiento de un sistema regional avanzado de información sobre la carga orientado a ayudar a los Estados miembros de la CARICOM que sean participantes a mejorar la selección de la carga; y la elaboración de una ley modelo relativa al Tratado sobre el Comercio de Armas.

El Centro Regional de las Naciones Unidas para la Paz, el Desarme y el Desarrollo en América Latina y el Caribe sigue siendo un asociado importante para la CARICOM. El Centro Regional es el cocustodio, junto con IMPACS, de la implementación de la Hoja de Ruta de Armas de Fuego del Caribe. El UNLIREC llevó a cabo 54 actividades en la región para contribuir a la implementación de la Hoja de Ruta, en las que participaron 600 funcionarios, de los cuales 220 eran mujeres. El Centro también colaboró para elaborar planes de acción nacionales, con el fin de implementar la Hoja de Ruta y supervisar y evaluar los avances en su implementación. Hasta la fecha, diez Estados del Caribe han elaborado sus planes de acción nacionales.

La región también se benefició de una serie de seminarios web y sesiones de capacitación sobre diversas cuestiones, entre ellas mejores prácticas internacionales para investigadores penales, el examen forense de armas de fuego de fabricación privada, la mejora de las técnicas de investigación sobre armas de fuego y la gestión de la información balística.

La CARICOM se suma al llamamiento del Secretario General para que los Estados Miembros y otros asociados presten al Centro apoyo financiero y en especie.

La CARICOM considera que el Tratado sobre el Comercio de Armas, el Programa de Acción para Prevenir, Combatir y Eliminar el Tráfico Ilícito de Armas Pequeñas y Ligeras en Todos Sus Aspectos, los Instrumentos Internacionales de Rastreo y otras resoluciones aplicables de las Naciones Unidas relativas a las armas pequeñas y las armas ligeras son instrumentos fundamentales para prevenir, controlar y eliminar el tráfico ilícito de armas pequeñas y armas ligeras y municiones conexas en todos sus aspectos. La CARICOM alienta a todos los Estados a aplicar plenamente las disposiciones de dichos instrumentos.

Uno de los principales desafíos que encaran los pequeños Estados insulares en desarrollo a la hora de aplicar los instrumentos en materia de armas pequeñas y armas ligeras es la falta de recursos y de capacidad técnica suficientes. Para la aplicación plena y efectiva del Tratado sobre el Comercio de Armas, el Programa de Acción y el Instrumento Internacional de Localización, la cooperación y la asistencia internacionales deben considerarse como una alianza entre Estados en desarrollo, Estados desarrollados y Estados donantes, anclada en la titularidad nacional. Por lo tanto, destacamos la importancia de prestar asistencia incondicional y no discriminatoria a los países en desarrollo que la soliciten para reforzar su capacidad de aplicar de manera efectiva las disposiciones de los instrumentos internacionales de desarme.

Uno de los principales desafíos que encaran los Estados en desarrollo, incluidos los de la CARICOM, a la hora de aplicar el Tratado sobre el Comercio de Armas, el Programa de Acción y el Instrumento Internacional de Localización es la falta de transferencia de tecnología y de intercambio de lecciones relativas a su aplicación. La necesidad de redoblar los esfuerzos para atajar este desequilibrio es fundamental para mejorar el control de

las armas pequeñas y las armas ligeras y reducir la brecha digital tecnológica entre los Estados desarrollados y en desarrollo.

Reconociendo que la ciberseguridad es ahora parte indisoluble de la seguridad regional y que, si no se aborda con urgencia, podría obstaculizar gravemente el desarrollo social y económico de nuestros Estados caribeños, la región ha elaborado un Plan de Acción sobre Ciberseguridad y Ciberdelincuencia de la CARICOM. El Plan pretende abordar las vulnerabilidades en materia de ciberseguridad de cada país caribeño participante y establecer un estándar práctico y armonizado de prácticas, sistemas y conocimientos en materia de ciberseguridad al que cada país caribeño pueda aspirar a corto y mediano plazo. También pretende crear la capacidad y la infraestructura necesarias para poder detectar, investigar y perseguir a tiempo la ciberdelincuencia y sus posibles vínculos con otras formas de actividad delictiva.

Aunque nuestra región dispone de recursos limitados para hacer frente a los diversos y complejos desafíos en materia de seguridad derivados de unas fronteras porosas, unos límites marítimos y terrestres expansivos y una situación geográfica que se encuentra en una zona de tránsito, hemos forjado una serie de alianzas para hacer realidad el desarme regional a través de una serie de medidas prácticas.

El Presidente (*habla en inglés*): Hemos agotado el tiempo que teníamos disponible para esta sesión. La Comisión se reunirá de nuevo mañana por la mañana, cuando escucharemos en primer lugar una exposición informativa a cargo del Presidente del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. A continuación, proseguiremos con el debate con arreglo al grupo temático “Desarme y seguridad regionales”.

Quisiera recordar a los miembros que, al final de su sesión de mañana por la mañana, la Comisión celebrará su tradicional ceremonia de entrega de certificados a los becarios graduados en desarme.

Se levanta la sesión a las 18.05 horas.