Naciones Unidas A/C.1/78/PV.20

Asamblea General
Septuagésimo octavo período de sesiones

Documentos oficiales

Primera Comisión
20ª sesión plenaria
Martes 24 de octubre de 2023, a las 10.00 horas
Nueva York

Presidencia: Sr. Paulauskas . . . . . (Lituania)

Se declara abierta la sesión a las 10.05 horas.

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 Comisión continuará ahora su debate en relación con el grupo temático “Armas convencionales”. Antes de ceder la palabra, quisiera pedir a todas las delegaciones que respeten el límite de tiempo establecido para las declaraciones formuladas durante este segmento temático.

Tiene ahora la palabra el observador de la Santa Sede.

El Arzobispo Caccia (Santa Sede) (*habla en inglés*): Ante todo, mi delegación recuerda que todos los Estados partes en el Tratado sobre la No Proliferación de las Armas Nucleares comparten la obligación de “celebrar negociaciones de buena fe [...] sobre un tratado de desarme general y completo”. Ante la rápida proliferación mundial de armamentos, es aún más imperioso reafirmar ese objetivo.

Lo más preocupante es que en la guerra de Ucrania se ha generalizado el uso de armamento indiscriminado, como minas antipersonal y municiones en racimo. La Santa Sede pide el cese inmediato de la utilización de tales armas, que ponen en peligro a los civiles, especialmente a los niños, y contaminan nuestro hogar común. Como ha destacado el Papa Francisco, no debe permitirse que la preocupación por las implicaciones morales de la guerra nuclear eclipse los problemas éticos cada vez más urgentes que plantea el uso que se está haciendo en la guerra contemporánea de las llamadas armas convencionales, que deberían utilizarse con fines exclusivamente defensivos y no emplearse contra objetivos civiles. De hecho, el rastro de devastación que dejan las armas convencionales exige renovar las medidas destinadas a contener su propagación, aumentar la transparencia sobre las existencias de armas actuales y garantizar que su uso se ajuste en todos los casos al derecho internacional humanitario.

Al perseguir dichos objetivos, la comunidad internacional debe poner siempre en el centro la dignidad inherente del ser humano. En ese sentido, la Santa Sede renueva su apoyo al Programa de Acción para Prevenir, Combatir y Eliminar el Tráfico Ilícito de Armas Pequeñas y Ligeras en Todos Sus Aspectos, en el que los Estados expresaron su determinación de “aumentar el respeto de la vida”, y espera con interés que se siga avanzando en el Programa de cara a la Cuarta Conferencia de las Naciones Unidas para Examinar los Progresos Alcanzados en la Ejecución del Programa de Acción, que se celebrará el año que viene. Del mismo modo, mi delegación respalda el llamamiento del Secretario General a entablar negociaciones para celebrar, de aquí a 2026, un instrumento jurídicamente vinculante que prohíba los sistemas de armas autónomos letales que funcionan sin control ni supervisión humanos. Entre tanto, la Santa Sede insta a todos los Estados a que se abstengan de desarrollar esa clase de armas, que en ningún caso pueden ser sujetos con responsabilidad moral y violan los dictados de la conciencia pública.

Dado que cada vez es más frecuente que los conflictos armados se desarrollen en pueblos y ciudades densamente poblados, el uso de armamento explosivo a menudo resulta indiscriminado y se traduce en bajas inaceptables entre los no combatientes y la destrucción de infraestructuras cruciales para la supervivencia de la población civil. En respuesta a esta situación, la Santa Sede valora positivamente que el pasado mes de noviembre se aprobase en Dublín la Declaración Política sobre las Consecuencias Humanitarias del Empleo de Armas Explosivas en Zonas Pobladas. La Santa Sede agradece al Gobierno de Irlanda su liderazgo en este empeño y espera que, a raíz de la Declaración, en las operaciones militares se pase de un paradigma de daños colaterales a otro de protección intencionada, de manera que se minimice la pérdida de vidas humanas.

Para concluir, permítaseme citar las palabras que el Papa Francisco pronunció ante Consejo de Seguridad en junio:

> "[D]esde un punto de vista económico, la guerra es a menudo más atractiva que la paz, en la medida en que promueve el beneficio. Sin embargo, eso siempre es válido solo para unos pocos y a expensas del bienestar de poblaciones enteras. Por consiguiente, el dinero obtenido con la venta de armas está manchado con sangre inocente. Hace falta más valor para renunciar a los beneficios fáciles en aras del mantenimiento de la paz que para vender armas cada vez más sofisticadas y potentes. Hace falta más valor para tratar de lograr la paz que para hacer la guerra" (*S/PV.9346, pág. 6*).

El Presidente (*habla en inglés*): La Comisión ha escuchado la última intervención de su debate relativo al grupo temático "Armas convencionales".

A continuación, la Comisión iniciará el debate relativo al grupo temático "Otras medidas de desarme y seguridad internacional".

Sr. Sirie (Indonesia) (*habla en inglés*): Me complace intervenir en nombre del Movimiento de Países No Alineados (MNOAL).

El MNOAL destaca los beneficios positivos de las tecnologías de la información y las comunicaciones (TIC) y su contribución al desarrollo, y alienta a los Estados a aplicar las normas, reglas y principios relativos al comportamiento responsable de los Estados al tiempo que impulsan el debate sobre los mecanismos de aplicación, ya que ello ayudará a aumentar la estabilidad y la seguridad en el ciberespacio.

Por otra parte, el MNOAL rechaza en los términos más enérgicos el empleo malintencionado de las nuevas TIC con fines incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales. El MNOAL pide que se intensifiquen las iniciativas para evitar que el ciberespacio se convierta en un escenario de conflicto y velar por que, en cambio, se utilice exclusivamente para fines pacíficos que permitan que las TIC alcancen su pleno potencial para contribuir al desarrollo social y económico.

El MNOAL toma nota de las conclusiones que el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional extrae en sus informes de 2013, 2015 y 2021 sobre la aplicabilidad y la importancia del derecho internacional y, en particular, de la Carta de las Naciones Unidas para mantener la paz y la estabilidad y promover un entorno de las TIC abierto, seguro, estable, accesible y pacífico.

El MNOAL quisiera recordar que 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), establecido en virtud de la resolución 75/240, fue el primer mecanismo inclusivo establecido en el seno de las Naciones Unidas en el que todos los Estados Miembros participan y actúan por consenso.

El MNOAL reitera su determinación de favorecer el buen funcionamiento del grupo de trabajo de composición abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones 2021-2025, establecido en virtud de la resolución 75/240, que en la actualidad es el único mecanismo inclusivo que tiene en cuenta las preocupaciones e intereses de todos los Estados, se basa en el consenso y lleva a cabo su labor en el seno de las Naciones Unidas con la participación activa e igualitaria de todos los Estados. Asimismo, el MNOAL toma nota del proceso de aprobación por consenso del segundo informe anual sobre los progresos realizados del grupo de trabajo (véase A/78/265).

El MNOAL subraya que el desarrollo de todo marco jurídico internacional para abordar las cuestiones relacionadas con el uso de las TIC con repercusiones para la paz y la seguridad internacionales debe tener en cuenta las preocupaciones e intereses de todos los Estados, basarse en el consenso y llevarse a cabo en el seno de las Naciones Unidas con la participación activa e igualitaria de todos los Estados. En ese sentido, el MNOAL es partidario de un mecanismo permanente de una sola

vía, dirigido por los Estados y bajo los auspicios de las Naciones Unidas, que dependa de la Primera Comisión. El MNOAL respalda que se establezca un proceso abierto, inclusivo, transparente, sostenible y flexible que pueda evolucionar para adaptarse a las necesidades de los países en desarrollo y a los cambios en el entorno de las TIC. Además, hace hincapié en que dicho marco jurídico, junto con una plataforma institucional multilateral e inclusiva dedicada a la cooperación internacional con miras a salvaguardar los usos pacíficos de las TIC, contribuiría de forma significativa al aumento de la estabilidad y la seguridad en el ciberespacio mediante la prevención de conflictos, lo que fomentaría la solución de controversias internacionales por medios pacíficos y los usos pacíficos de las TIC. Al mismo tiempo, el MNOAL subraya como posición de principios que ningún elemento de ese marco jurídico debe afectar a los derechos inalienables de los Estados en materia de desarrollo y uso de las TIC con fines pacíficos.

El MNOAL rechaza toda medida unilateral contraria a la Carta de las Naciones Unidas y al derecho internacional que dificulte que las poblaciones de los países afectados alcancen plenamente el desarrollo económico y social y obstaculice su bienestar. El MNOAL condena el uso indebido de las TIC, por ejemplo Internet y los medios sociales, para cometer actos de terrorismo o incitar a ello y recalca la importancia de capacitar a los Estados Miembros y promover medidas de fomento de la confianza destinadas a mejorar la estabilidad y la seguridad en el ciberespacio.

Asimismo, el MNOAL pone de relieve la importancia de que se observen las normas ambientales al preparar y aplicar acuerdos de desarme y limitación de armamentos. Además, reafirma que los foros internacionales de desarme deben tener plenamente en cuenta las normas ambientales pertinentes a la hora de negociar tratados y acuerdos sobre desarme y limitación de armamentos.

El MNOAL acoge con beneplácito que la resolución 77/45 relativa a la relación entre desarme y desarrollo se haya aprobado sin someterla votación y destaca también la importancia de reducir los gastos militares, de conformidad con el principio de la seguridad sin menoscabo al nivel más bajo de armamentos, e insta a todos los Estados a que dediquen los recursos que queden disponibles al hacerlo a encarar los nuevos desafíos a los que se enfrenta la comunidad internacional en los ámbitos del desarrollo, la erradicación de la pobreza y la eliminación de las enfermedades que afligen a la humanidad.

En el marco de este grupo temático, el MNOAL agradecerá el apoyo de todos los Estados a los tres proyectos de resolución que va a presentar “Observancia de las normas ambientales en la elaboración y la aplicación de los acuerdos de desarme y control de armamentos” (A/C.1/78/L.6), “Promoción del multilateralismo en la esfera del desarme y la no proliferación” (A/C.1/78/L.7) y “Relación entre desarme y desarrollo” (A/C.1/78/L.4).

Sr. Chindawongse (Tailandia) (*habla en inglés*): Tengo el honor de formular esta declaración en nombre de la Asociación de Naciones de Asia Sudoriental (ASEAN).

La ASEAN hace suya la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados.

La ASEAN reafirma su compromiso de construir un ciberespacio abierto, seguro, estable, accesible, interoperable, pacífico y resiliente que propicie el progreso económico, una mayor conectividad regional y un mejor nivel de vida para todos. Al mismo tiempo, reconoce la omnipresencia de las ciberamenazas, que se encuentran en constante evolución y tienen carácter transfronterizo. En un contexto de digitalización económica generalizada y proliferación de los dispositivos conectados a Internet en toda la ASEAN, nos hemos vuelto cada vez más vulnerables a actividades maliciosas en el ciberespacio que pueden socavar la paz y la seguridad. En ese sentido, la ASEAN considera que los Estados deben colaborar para dar una respuesta eficaz a las ciberamenazas, fomentar la confianza con miras a minimizar el riesgo de que se incurra en errores de percepción o de cálculo, y aprovechar los beneficios de la tecnología, al tiempo que reconocen que la ciberseguridad es una cuestión transversal que requiere que se coordine la experiencia de múltiples partes interesadas procedentes de diferentes ámbitos.

La ASEAN recalca el papel esencial que despeñan las Naciones Unidas en los debates sobre ciberseguridad. A ese respecto, la ASEAN reafirma su apoyo a la labor del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional 2021-2025, en cuanto que medida de fomento de la confianza y foro en el que alcanzar y recuperar consensos sobre esa cuestión relevante. Por lo tanto, la ASEAN acoge con beneplácito que el segundo informe anual sobre los progresos realizados del Grupo de Trabajo se aprobase por consenso durante su quinto período de sesiones sustantivo, que se celebró en julio de 2023 (véase A/78/265). La ASEAN se enorgullece de la

contribución significativa a los debates internacionales sobre cibernética en las Naciones Unidas que han hecho sus iniciativas, en particular el Directorio de Puntos de Contacto sobre la Seguridad y la Utilización de las Tecnologías de la Información y las Comunicaciones del Foro Regional de la ASEAN y la matriz para el Plan de Acción Regional de la ASEAN sobre la Aplicación de las Normas de Comportamiento Responsable de los Estados en el Ciberespacio. Aguardamos con interés la creación y puesta en funcionamiento de un directorio mundial e intergubernamental de puntos de contacto, así como la elaboración de orientaciones adicionales, incluida una lista de comprobación sobre la aplicación de las normas, como se indica en el informe anual sobre los progresos realizados.

La ASEAN aboga por que el Grupo de Trabajo de Composición Abierta siga siendo la plataforma central para los debates sobre ciberseguridad en las Naciones Unidas hasta el final de su mandato, y espera con interés que se consigan más avances, entre otras cosas, aprovechando el consenso que tanto nos ha costado alcanzar en los dos últimos informes anuales sobre los progresos realizados. La ASEAN señala a la atención de los Estados Miembros la importancia de preservar y mantener el consenso sobre la importante cuestión de la ciberseguridad. Además, deberíamos evitar crear mecanismos paralelos y procesos que se solapen, lo que no haría sino someter a mayor tensión los recursos limitados de las Naciones Unidas y sus Estados Miembros. En ese sentido, la ASEAN cree firmemente que es importante contar con un proceso de una sola vía que se base en las recomendaciones por consenso del grupo de trabajo de composición abierta sobre el diálogo institucional periódico. La ASEAN sigue plenamente decidida a colaborar de forma constructiva con todos los asociados para alcanzar ese objetivo.

En el seno de la ASEAN, la cooperación en materia de ciberseguridad abarca varios pilares y sectores que se guían por su Plan Maestro Digital 2025 y su Estrategia de Cooperación en Ciberseguridad 2021-2025, que fueron aprobados en enero de 2022 por los Ministros competentes en materia digital de los Estados miembros de la Asociación. Ante el reciente aumento de los ataques y amenazas a la ciberseguridad en el mundo y en respuesta a los nuevos avances cibernéticos, dichos Estados miembros han hecho lo posible por poner en práctica medidas de ciberseguridad reforzada con arreglo a la Estrategia 2021-2025. Al mismo tiempo, la ASEAN está trabajando actualmente para llevar a la práctica el Plan de Acción Regional Asiático sobre la aplicación de las normas del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, que se elaboró para que los Estados miembros de la ASEAN detectasen los ámbitos en que necesitan más apoyo para aplicar las normas, entre los que figuran la creación de capacidades y la cooperación internacional.

Para reforzar sus capacidades de respuesta ante incidentes de ciberseguridad, la ASEAN ha acordado crear su Equipo Regional de Respuesta a Emergencias Informáticas para facilitar que los equipos nacionales de respuesta a emergencias informáticas de los Estados miembros de la Asociación intercambien información sobre amenazas y ataques de manera oportuna.

Dado que la ciberseguridad es una cuestión transversal, se creó el Comité Coordinador de Ciberseguridad de la ASEAN para reforzar la colaboración y coordinación regionales en materia de ciberseguridad. El Comité se compone de representantes de los órganos sectoriales pertinentes con el fin de consolidar la coordinación intersectorial en materia de ciberseguridad, sin dejar de respetar los ámbitos de trabajo de dichos órganos.

La ASEAN recalca la importancia de la cooperación internacional y de la creación de capacidades en el ámbito de las TIC para que los Estados, en especial los países en desarrollo, puedan enfrentarse con eficacia a las ciberamenazas y aplicar las 11 normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados en el uso de las TIC. Para ello, la ASEAN inició la ejecución del proyecto Cyber Shield de la ASEAN de 2023 a 2026 para complementar las iniciativas con las que ya contaba la Asociación en materia de creación de capacidades, como el Centro de Excelencia sobre Ciberseguridad de la ASEAN y Singapur, en Singapur, y el Centro de Fomento de la Capacidad en Seguridad Cibernética de la ASEAN y el Japón, en Tailandia, con vistas a respaldar el objetivo común de mejorar las capacidades de la región. La ASEAN aguarda con interés trabajar conjuntamente con las Naciones Unidas en este sentido, especialmente a través de la Alianza Amplia entre la ASEAN y las Naciones Unidas.

Asimismo, la ASEAN colabora con asociados internacionales a fin de mejorar la cooperación internacional en el ámbito de la seguridad de las TIC a través de plataformas como la Reunión de la ASEAN entre Períodos de Sesiones sobre la Seguridad y la Utilización de las Tecnologías de la Información y las Comunicaciones. Además, acoge con beneplácito los progresos que

suponen la apertura del Centro de Excelencia en Ciberseguridad e Información de la Reunión de Ministros de Defensa (ADMM) y el Grupo de Trabajo de Expertos en Ciberseguridad de la Reunión de Ministros de Defensa de la ASEAN-Plus (ADMM-Plus). Entre los logros más destacados de los últimos años figuran la elaboración del Directorio de Puntos de Contacto y Personal Técnico, la compilación de un Glosario de Terminología Cibernética, la realización de un ejercicio de simulación y la creación del portal del Grupo de Trabajo de Expertos en Ciberseguridad de la ADMM-Plus.

Para concluir, la ASEAN reafirma su compromiso de prepararse para el futuro con miras a permitir el progreso económico, mejorar nuestro modo de vida y garantizar la paz y la seguridad para todos. Esperamos contribuir de forma constructiva, junto con los miembros de la comunidad internacional y las partes interesadas pertinentes, a impulsar nuestro objetivo compartido de que el ciberespacio sea pacífico, seguro, interoperable y resiliente.

Sr. Shen Jian (China) (*habla en inglés*): Tengo el honor de formular esta declaración en nombre de Belarús, Burundi, Camboya, el Camerún, Cuba, Dominica, Guinea Ecuatorial, Eritrea, Etiopía, Guinea-Bissau, Gambia, Kazajstán, Kirguistán, la República Democrática Popular Lao, Nicaragua, el Pakistán, Rusia, Somalia, Siria, Vanuatu, Venezuela, Zimbabwe y mi propio país, China.

Con ocasión del segundo aniversario de la aprobación de la resolución 76/234, titulada “Promoción de la cooperación internacional para los usos pacíficos en el contexto de la seguridad internacional”, nosotros, los patrocinadores de la resolución, reiteramos el derecho inalienable de todos los Estados a participar del intercambio más amplio posible de equipo, materiales e información científica y tecnológica para fines pacíficos. En el contexto de una nueva era, teniendo presente la posible repercusión de los avances científicos y tecnológicos en la seguridad mundial, cada vez destaca más la importancia de los usos pacíficos para facilitar el desarrollo económico y social de los Estados Miembros, en particular de los países en desarrollo. Hacemos un llamamiento a la comunidad internacional para que adopte medidas concretas que garanticen la aplicación efectiva de la resolución.

Acogemos con beneplácito los compromisos políticos y los esfuerzos concretos de los Estados Miembros en la promoción de la cooperación internacional sobre usos pacíficos, así como los progresos realizados en los marcos multilaterales y a través de canales bilaterales. Al mismo tiempo, persisten las restricciones indebidas a las exportaciones a países en desarrollo de materiales, equipo y tecnología para fines pacíficos. Reafirmamos la importancia de promover la cooperación internacional con fines pacíficos y la necesidad de seguir deliberando sobre este importante tema en el marco de las Naciones Unidas de forma abierta e inclusiva y utilizando los mecanismos y acuerdos internacionales, regionales y bilaterales existentes que proceda con arreglo a la resolución. Exhortamos a todos los Estados Miembros a que continúen los diálogos sobre la promoción de los usos pacíficos y la cooperación internacional pertinente, entre otras cosas detectando las lagunas y los retos, así como ideas y oportunidades para reforzar la cooperación, y estudiando posibles formas de avanzar.

Presentaremos un proyecto de resolución titulado “Promoción de la cooperación internacional para los usos pacíficos en el contexto de la seguridad internacional” a la Asamblea General en su septuagésimo noveno período de sesiones, en 2024. Acogemos con beneplácito la participación activa de todos los Estados en el proceso de seguimiento.

El Presidente (*habla en inglés*): Tiene ahora la palabra el representante de la Unión Europea, en calidad de observadora.

Sr. Karczmarz (Unión Europea) (*habla en inglés*): Tengo el honor de hablar en nombre de la Unión Europea. Se suman a la presente declaración Macedonia del Norte, Montenegro, Serbia, Albania, Ucrania, la República de Moldova y Bosnia y Herzegovina, países candidatos; Georgia, posible país candidato; Islandia y Noruega, países de la Asociación Europea de Libre Comercio y miembros del Espacio Económico Europeo, así como Mónaco y San Marino.

En la última década, la comunidad internacional ha dejado claro que el orden internacional basado en normas también se aplica al comportamiento de los Estados en el ciberespacio. Todos los miembros de la Asamblea General han afirmado en repetidas ocasiones el marco evolutivo de comportamiento responsable de los Estados en el ciberespacio, basado en el reconocimiento de que el derecho internacional es de aplicación en el ciberespacio, la adhesión a normas voluntarias y no vinculantes sobre el comportamiento de los Estados, la creación de capacidades y la mejora de las medidas prácticas de fomento de la confianza para reducir el riesgo de conflicto. El amplio consenso internacional en torno a estos cuatro elementos es el principal logro de la ciberdiplomacia en la última década.

La guerra de agresión ilegal, no provocada e injustificada de Rusia ha puesto en grave riesgo el orden internacional basado en normas, también en el ámbito cibernético. Los ciberataques destructivos contra Ucrania, que a menudo tienen lugar en conjunción con ataques con misiles, no tienen precedentes y afectan de forma indirecta también a los países de la Unión Europea. En el último año, Ucrania no solo ha sido el país que ha sufrido el mayor número de ataques con programas maliciosos de destrucción de datos, sino que también ha logrado evitar muchos de ellos gracias a su extraordinaria ciberdefensa y resiliencia.

El cambio del entorno de amenazas en Europa inducido por la agresión de Rusia contra Ucrania y el aumento y la evolución de otras amenazas procedentes de Estados y actores no estatales han afectado a la forma en que nosotros, como Unión Europea, encaramos las ciberoperaciones maliciosas. Hemos reforzado nuestro compromiso de seguir revisando y mejorando constantemente la ciberresiliencia en el seno de la Unión Europea y de desarrollar nuevas estrategias sobre la mejor manera de hacer frente a las ciberamenazas que representan todos los agentes maliciosos.

Aunque reconocemos que los Estados son los principales responsables de velar por la paz y la seguridad internacionales, hay otras partes interesadas que desempeñan un papel esencial. 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), creado en virtud de la resolución 75/240, constituye una oportunidad para que la comunidad internacional lleve a cabo un intercambio de opiniones abierto, inclusivo y transparente sobre cómo pueden utilizar los Estados las tecnologías de la información y las comunicaciones de manera responsable y coherente con el derecho internacional.

Acogemos con beneplácito el consenso alcanzado en 2023 sobre el informe anual del Grupo de Trabajo sobre los progresos realizados (véase A/78/265) y subrayamos la necesidad de que la comunidad internacional continúe avanzando en la senda del refuerzo de la seguridad y la estabilidad en el ciberespacio. Aunque el informe anual sobre los progresos realizados podría haber ido más lejos, en él se reseñan múltiples decisiones y los próximos pasos que pueden estudiarse como vías concretas y factibles para avanzar en el refuerzo del marco de las Naciones Unidas de comportamiento responsable de los Estados y del derecho internacional.

Aún queda mucho por hacer, sobre todo en lo que respecta al apoyo a la aplicación práctica de los resultados de esos debates. La Unión Europea y sus Estados miembros aguardan con interés seguir colaborando con los Estados y otras partes interesadas para impulsar esas iniciativas, en particular mediante un diálogo inclusivo sobre la elaboración de un programa de acción de las Naciones Unidas que se base en los resultados consensuados de los sucesivos grupos de expertos gubernamentales y grupos de trabajo de composición abierta de las Naciones Unidas, así como en la labor del actual grupo de trabajo de composición abierta y en el informe del Secretario General.

El amplio apoyo que recibió la resolución 77/37 en el período de sesiones de la Primera Comisión del año pasado, en el que contó con 157 votos a favor y el patrocinio de un grupo interregional de 74 países, reafirmó el compromiso de los Estados de aplicar el marco normativo acordado mediante un mecanismo permanente, inclusivo y orientado a la acción. Asimismo, demuestra claramente que la gran mayoría de los Estados tiene la aspiración común de promover la paz, la seguridad y la estabilidad en el ciberespacio a través de una plataforma permanente y cooperativa que fomente el intercambio de conocimientos y mejores prácticas, evite la duplicación de medidas y respalde las iniciativas nacionales y regionales de aplicación. Más de 40 Estados, de todos los grupos regionales, han compartido sus comunicaciones por escrito y el Secretario General ha emitido un informe (A/76/77) en el que trata asuntos muy útiles y ofrece recomendaciones para seguir manteniendo un debate inclusivo sobre el programa de acción.

Como se exponía en la resolución 77/37 del año pasado, esta propuesta tiene por objeto proporcionar a los Estados la flexibilidad necesaria para dar respuesta a cuestiones en las que se pueden aprovechar los debates políticos, el intercambio de información y la aplicación práctica. El impulso procederá de los Estados y, además, se intentará mejorar la participación de múltiples partes interesadas, gracias a consultas periódicas con aquellas que resulten pertinentes, como el sector privado, el mundo académico y la sociedad civil, con el fin de estudiar y obtener sus perspectivas específicas. Muchas partes interesadas no estatales ya están impulsando iniciativas con el objetivo de fomentar la confianza entre los Estados y los actores no estatales, y, al incluir a estos últimos, se lograrán resultados más significativos y se contribuirá a la transparencia, la credibilidad y la sostenibilidad de la aplicación del marco.

Sobre todo, cabe señalar que, si se creara una plataforma permanente, los debates de la comunidad internacional podrían concentrarse en cuestiones fondo y en

mejorar la cooperación y la confianza entre los Estados, en lugar de versar de manera recurrente sobre futuros procesos. No debemos desaprovechar esta oportunidad de impulsar nuestra labor en un entorno estable, y la Unión Europea y sus Estados miembros apoyan plenamente la resolución correspondiente presentada a la Asamblea General con este fin. Para mantener un proceso de una sola vía en las Naciones Unidas, necesitamos que, cuando el Grupo de Trabajo de Composición Abierta 2021-2025 termine su labor, se cree un mecanismo permanente de alcance, estructura y contenido basados en los debates mantenidos en el seno del Grupo de Trabajo en 2024 y 2025.

Dado que las amenazas a la ciberseguridad internacional no dejan de aumentar, es más importante que nunca estrechar nuestra cibercolaboración con los asociados internacionales y promover una interpretación compartida de cómo se aplica el derecho internacional y cómo seguir poniendo en práctica el marco de las Naciones Unidas de comportamiento responsable de los Estados. Por ello, la Unión Europea apoya el proyecto de resolución A/C.1/78/L.60, presentado por Francia, con el fin de establecer un mecanismo bajo los auspicios de las Naciones Unidas en cuanto que marco flexible en el que los Estados Miembros de las Naciones Unidas puedan mantener debates prácticos sobre la mejor estrategia para que el ciberespacio sea seguro para todos. Solo podremos ser eficaces al garantizar un ciberespacio abierto, estable y seguro de si colaboramos, mejoramos la coordinación y la complementariedad, acabamos con los comportamientos estancos y creamos métodos nuevos e innovadores para hacer frente a los comportamientos cibernéticos maliciosos. Este objetivo es una de las principales aspiraciones de la Unión Europea.

Sr. Lagardien (Sudáfrica) (*habla en inglés*): Sudáfrica hace suya la declaración formulada en nombre del Movimiento de Países No Alineados.

Sudáfrica acoge con beneplácito la aprobación por consenso del segundo informe sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Este proceso ha sido importante para fomentar la confianza mutua y promover la cooperación pacífica entre los Estados. En cuanto al gran número de amenazas a las que se enfrentan los Estados, Sudáfrica considera que, para afrontar aquellas que se dirigen contra las infraestructuras de las tecnologías de la información y las comunicaciones (TIC), se necesitan medidas de cooperación.

Hemos participado de buena fe en el grupo de trabajo de composición abierta para garantizar que el diálogo entre los Estados tenga lugar bajo los auspicios de las Naciones Unidas, que es un foro universal y multilateral en el que se promueve el arreglo pacífico de controversias. Sudáfrica considera que el mantenimiento de la paz y la seguridad internacionales en el ciberespacio es una responsabilidad colectiva. Creemos que los Estados deben utilizar la versión actual de las 11 reglas, normas y principios de comportamiento responsable de los Estados en el ciberespacio, mientras estudiamos un posible marco de cooperación más amplio.

El segundo informe anual sobre los progresos realizados nos ofrece dos medidas globales de fomento de la confianza: la labor constante de entablar un diálogo institucional periódico y el directorio de puntos de contacto. Además, consideramos que el grupo de trabajo de composición abierta y sus resultados consensuados constituyen en sí mismos una medida de fomento de la confianza, y encomiamos al Presidente del grupo de trabajo, el Embajador Burhan Gafoor, y a su equipo por sus esfuerzos para garantizar que logremos resultados tangibles y que el proceso siga orientado a la acción. Los debates sobre los distintos formatos de intercambio de puntos de vista entre los Estados acerca de las amenazas potenciales y emergentes nos han demostrado que la comunidad internacional puede colaborar de manera constructiva en momentos políticos difíciles. En ese sentido, Sudáfrica respalda las propuestas de crear un repositorio de amenazas y un portal mundial de cooperación en materia de ciberseguridad. Confiamos en que en los futuros períodos de sesiones del grupo de trabajo de composición abierta puedan seguir desarrollándose estas ideas.

Aunque sería beneficioso incluir en el proceso intergubernamental sesiones informativas de expertos procedentes de organizaciones regionales y subregionales, empresas, organizaciones no gubernamentales y el mundo académico, teniendo debidamente en cuenta una representación geográfica equitativa, consideramos que el Presidente del grupo de trabajo de composición abierta ha hecho uso de sus facultades de convocatoria para invitar a diversas partes interesadas a compartir sus puntos de vista sobre la implementación de la seguridad de las TIC. Así pues, el grupo de trabajo de composición abierta ha podido incorporar a sus trabajos el mayor número posible de puntos de vista diversos.

Como país en desarrollo, Sudáfrica se ha beneficiado del intercambio de puntos de vista entre los Estados sobre el grupo de trabajo de composición abierta y apoyamos al Presidente y el calendario que ha propuesto

con el fin de facilitar el proceso para acordar el futuro de nuestros debates como comunidad internacional. Sudáfrica cree que es vital que protejamos los procesos existentes de ese tipo, pues han dado buenos resultados en tiempos difíciles.

Sr. Alqaisi (Jordania) (*habla en árabe*): Para empezar, quisiera reiterar, en nombre del Grupo de los Estados Árabes, la necesidad de poner fin a la guerra y a la brutal agresión israelí contra la Franja de Gaza. El Grupo condena esa agresión con total contundencia. Debe garantizarse tanto el acceso seguro y sostenible a la ayuda humanitaria y médica esencial como el fin de los desplazamientos forzosos de palestinos.

En cuanto a nuestro debate temático de hoy, el Grupo de los Estados Árabes se adhiere a la declaración formulada en nombre del Movimiento de Países No Alineados.

Con respecto a otras medidas de desarme, el Grupo de los Estados Árabes recalca que las soluciones acordadas en un marco multilateral de conformidad con la Carta de las Naciones Unidas constituyen la única vía sostenible para resolver las cuestiones relacionadas con el desarme y la seguridad internacional. El Grupo hace un llamamiento a todos los Estados Miembros para que reiteren y cumplan los compromisos individuales y colectivos que han contraído en el marco multilateral internacional. Asimismo, hace hincapié en que confía en el papel fundamental de las Naciones Unidas en los ámbitos del desarme y la no proliferación.

El Grupo de los Estados Árabes expresa su preocupación por el aumento de las tensiones y del gasto militar a escala mundial, pues gran parte de esos recursos podrían destinarse a fomentar el desarrollo sostenible y erradicar la pobreza en el mundo, en particular en los países en desarrollo, incluidos los Estados árabes. El Grupo reafirma la importancia de dar seguimiento al programa de trabajo aprobado en la Conferencia Internacional sobre la Relación entre Desarme y Desarrollo de 1987, así como a los efectos del aumento del gasto militar para la consecución de los Objetivos de Desarrollo Sostenible, de conformidad con la Agenda 2030 para el Desarrollo Sostenible.

La posesión y modernización constantes de los arsenales nucleares constituyen una grave amenaza para la paz y la seguridad internacionales y para el desarrollo sostenible. Por ello, el Grupo de los Estados Árabes subraya la necesidad de que los foros internacionales de desarme tengan en cuenta las normas pertinentes al negociar tratados y convenciones sobre desarme y control de armamentos. Todos los Estados deben contribuir a garantizar el pleno cumplimiento de las normas medioambientales al aplicar dichos tratados y convenciones.

En lo que respecta a la ciberseguridad, el Grupo de los Estados Árabes expresa su preocupación por que las tecnologías de la información y las comunicaciones (TIC) se utilicen cada vez más en actividades destructivas que amenazan la paz y la seguridad internacionales, en particular las perpetradas por organizaciones terroristas y delictivas. El Grupo subraya la necesidad de que las Naciones Unidas sigan elaborando normas vinculantes que regulen el comportamiento responsable de los Estados en ese ámbito vital y se ajusten a su rápida evolución. Asimismo, es necesario seguir cooperando a escala internacional y mantener el papel central de las Naciones Unidas en esa labor.

El Grupo de los Estados Árabes subraya la importancia de intensificar la cooperación internacional para promover la seguridad de las TIC. De este modo aumentarían las capacidades de los Estados para contrarrestar los ataques de sabotaje, que se destacan en muchos informes publicados por diversos grupos de expertos gubernamentales y grupos de trabajo de composición abierta. El Grupo desea garantizar que las Naciones Unidas desempeñen un papel central en la promoción de las normas internacionales relativas a la seguridad de las TIC y mantener la cooperación con las Naciones Unidas en este ámbito, que repercute en todas las instalaciones vitales de diversos Estados y cada vez tiene mayor protagonismo en actividades de sabotaje que amenazan la seguridad internacional.

En conclusión, el Grupo de los Estados Árabes resalta su disposición a participar activamente 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). El Grupo de los Estados Árabes acoge con beneplácito la aprobación por consenso del segundo informe anual sobre los progresos realizados del grupo de trabajo de composición abierta (véase A/78/265) y espera con interés la celebración de debates centrados en las distintas propuestas pertinentes para ayudar a los países en desarrollo a contrarrestar el incremento de las amenazas derivadas del uso de las TIC.

Sr. Sirie (Indonesia) (*habla en inglés*): Indonesia hace suyas las declaraciones formuladas en nombre del Movimiento de Países No Alineados y de la Asociación de Naciones de Asia Sudoriental. A ese respecto, quisiera añadir algunos comentarios en nombre de mi país.

Mi primera observación se refiere a la importancia de reforzar las medidas de cooperación en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones (TIC). La tecnología suele describirse como un arma de doble filo, al ser una valiosa herramienta que también plantea importantes riesgos. Sin embargo, a medida que estamos más interconectados, los ciberataques se perfilan como una amenaza fundamental para la infraestructura digital, al causar interrupciones de los servicios, robos de datos y fraude. A ese respecto, Indonesia subraya la necesidad de adoptar medidas para que todos los Estados Miembros cooperen con el fin de garantizar un ciberespacio seguro y estable.

Indonesia reafirma su apoyo a 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 (2021-2025), incluido su énfasis en la creación de capacidades y el fomento de la confianza. De este modo se ayudará a los países a mejorar sus capacidades en materia de ciberseguridad. Por su parte, Indonesia acaba de poner en marcha su Estrategia Nacional de Ciberseguridad, concretamente en julio. La estrategia facilitará la labor de nuestro recién creado Organismo Nacional de Ciberseguridad y reforzará el marco jurídico para salvaguardar a los usuarios informáticos, las infraestructuras nacionales críticas y el ciberespacio a través de la legislación, como ilustran la Ley de Privacidad de Datos de 2022 y la Ley de Información y Transacciones Electrónicas de 2008. Indonesia espera con interés continuar el debate sobre el fomento de la creación de capacidades en materia de ciberseguridad en el seno del Grupo de Trabajo de Composición Abierta.

Mi segunda observación se refiere al fortalecimiento de los marcos y normas multilaterales sobre el uso de las TIC. En el actual panorama de la seguridad internacional, la cooperación basada en el consenso parece estar decayendo. No debemos dejar que eso ocurra en el ámbito de la seguridad de las TIC. Esa tendencia permitiría que los actores maliciosos perturbasen la seguridad del ciberespacio, lo que amenazaría la paz y la estabilidad internacionales. Por lo tanto, dado la situación precaria de nuestro entorno internacional, Indonesia aplaude el esfuerzo realizado por los Estados Miembros al aprobar por consenso el segundo informe anual sobre los progresos realizados (véase A/78/265). Gracias a su enfoque inclusivo y gradual, el Grupo de Trabajo de Composición Abierta ha logrado convertirse en una plataforma que facilita la cooperación, la transparencia y las medidas de fomento de la confianza en materia de seguridad de las TIC. Asimismo, Indonesia acoge con beneplácito y espera con interés la implementación del directorio de puntos de contacto, que es uno de los resultados concretos y tangibles obtenidos por el Grupo de Trabajo. Por lo tanto, es esencial que mantengamos la inviolabilidad del Grupo de Trabajo como marco inclusivo para gestionar los ciberriesgos, lo que fomenta la buena gobernanza y las buenas prácticas en los ámbitos del ciberespacio.

Cuando nos encontramos en el ecuador del mandato del Grupo de Trabajo de Composición Abierta, deseo secundar las declaraciones formuladas por otras delegaciones sobre una propuesta de proyecto de resolución relativa al futuro mecanismo destinado a deliberar sobre la seguridad de las TIC. Es importante que sigamos respetando los elementos comunes del futuro mecanismo, tal y como se acordó por consenso en el segundo informe anual sobre los progresos realizados. Debemos evitar presentar proyectos de resolución concurrentes sobre el mismo tema, lo que conduciría a la fragmentación de la labor de la Primera Comisión, ya que daría lugar a procesos paralelos que socavarían el trabajo del Grupo de Trabajo. En vez de eso, debemos seguir valiéndonos del Grupo de Trabajo para debatir una cooperación constante, de modo que los países intercambien mejores prácticas y capacidades con el fin de hacer frente de manera eficaz a los retos que plantea la ciberseguridad, reducir la brecha digital y facilitar un progreso económico y social sin trabas.

Sr. Hegazy (Egipto) (*habla en inglés*): Para empezar, permítanme expresar nuestra enérgica condena de los constantes ataques contra palestinos en Gaza. Volvemos a pedir un alto el fuego urgente e incondicional, y repetimos nuestro llamamiento a Israel para que ponga fin de inmediato a sus intentos de forzar a más de un millón de civiles en el sur de Gaza a desplazarse y permita el acceso sin trabas de la asistencia humanitaria para aliviar el sufrimiento humano actual del pueblo palestino.

Egipto hace suyas las declaraciones formuladas en nombre del Movimiento de Países No Alineados y el Grupo de los Estados Árabes, y desea hacer las siguientes observaciones.

Egipto reitera que los instrumentos no discriminatorios, multilaterales y jurídicamente vinculantes son las herramientas más eficaces para lograr un progreso sostenible en los ámbitos del desarme y la seguridad internacional. Habida cuenta de los rápidos avances científicos y tecnológicos que se están registrando en distintos ámbitos estratégicos, que son esferas que repercuten de manera directa en la seguridad internacional y carecen

de normas acordadas internacionalmente para impedir que se conviertan en el escenario de carreras armamentistas y conflictos armados, la determinación constante de todos los Estados de acatar los compromisos previamente acordados y de respetar el derecho internacional es una condición necesaria para mantener la paz y la seguridad internacionales y evitar el caos, y para garantizar con fiabilidad que las tecnologías pertinentes persisten y contribuyen al desarrollo y al bienestar.

Entre los ejemplos destacados se encuentran el ciberespacio, el espacio ultraterrestre y la organización de las aplicaciones de la inteligencia artificial, también en lo que respecta al ámbito de las armas autónomas letales. Es evidente que la falta de progresos a la hora de hacer frente a las diversas amenazas a la seguridad que surgen en tales campos no se debe a que la comunidad internacional no tenga los conocimientos técnicos necesarios, sino a que algunos Estados no abandonan la creencia errónea de que se puede mantener una hegemonía absoluta en esos ámbitos. De ahí su oposición a toda iniciativa encaminada a establecer regímenes jurídicos de carácter multilateral y equitativo que prohíban el uso de esas tecnologías con fines maliciosos o militares, lo que desembocará en una carrera armamentista imposible de ganar.

Acogemos con beneplácito el venturoso fin del segundo ciclo anual del 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 la aprobación de su segundo informe anual sobre los progresos realizados (véase A/78/265) y el documento de elementos sobre la puesta en funcionamiento del directorio mundial de puntos de contacto, así como otras recomendaciones orientadas al futuro que podrían allanar el camino hacia debates centrados en las cuestiones y propuestas pendientes en el ámbito de la labor del Grupo de Trabajo.

Se presentaron al Grupo de Trabajo de Composición Abierta muchas ideas creativas y propuestas constructivas, incluido un diálogo institucional periódico bajo los auspicios de las Naciones Unidas, como un posible programa de acción de las Naciones Unidas sobre el uso de las TIC en el contexto de la seguridad internacional que Egipto ha iniciado junto con Francia desde 2020 y desarrollado con el apoyo de un grupo interregional de Estados con el objetivo de complementar la labor del Grupo de Trabajo cuando concluya su mandato después de 2025.

En este contexto, Egipto ha presentado su posición nacional sobre el futuro proceso de diálogo institucional periódico en la página web del Grupo de Trabajo de Composición Abierta. Compartimos el punto de vista de que cualquier proceso futuro sobre ese tema debe contener un pilar específico sobre la aplicación del marco acordado y la capacitación de los países en desarrollo en ese sentido. Debería tratarse de un mecanismo flexible, orientado a la acción, de una sola vía, permanente y basado en el consenso bajo los auspicios de las Naciones Unidas, tal y como se prevé en el párrafo 55 del segundo informe anual consensuado sobre los progresos realizados del Grupo de Trabajo de Composición Abierta. Debería identificar las posibles lagunas del marco existente mediante la implementación de resultados consensuados, reforzar la cooperación y la asistencia internacionales y seguir desarrollando el marco existente de normas, reglas y principios, además de obligaciones vinculantes.

En ese contexto, acogemos con beneplácito que la idea de centrarse en la aplicación del marco acordado existente y en seguir desarrollándolo cuente cada vez con más apoyo. Además, creemos que debemos seguir respaldando al actual grupo de trabajo de composición abierta para que concluya con éxito sus actividades y dedicando nuestros esfuerzos a alcanzar una base común para crear el futuro mecanismo, aprovechando la labor del Grupo de Trabajo. En ese sentido, alentamos a todas las delegaciones a que no se adelanten a las negociaciones en curso ni impongan prematuramente el establecimiento de vías paralelas no solo en lo que respecta al grupo temático 5, sino también en todos los demás. Esa tendencia no haría sino desembocar en mayores divisiones y estancamientos.

Sra. Gómez Sardinas (Cuba): Apoyamos la intervención del representante de Indonesia en nombre del Movimiento de Países No Alineados. Nos sumamos a la intervención del representante de China relativa a la cooperación internacional con fines pacíficos en el contexto de la seguridad internacional.

Reiteramos el compromiso de Cuba con el desarme general y completo que permita alcanzar un mundo libre de armas de destrucción en masa 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 cumplimiento de la Agenda 2030 para el Desarrollo Sostenible y sus Objetivos de 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 que prohíban la militarización del espacio ultraterrestre y del ciberespacio y las armas letales autónomas.

El Sr. Lagardien (Sudáfrica), Vicepresidente, ocupa la Presidencia.

Respaldamos la continuidad de 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 (2021-2025), mecanismo que permite a los Estados Miembros discutir este tema de forma transparente, inclusiva y en igualdad de condiciones. Como muestra de nuestro compromiso con este foro, favorecimos la aprobación por consenso de su segundo informe anual sobre los progresos (véase A/78/265), aunque teníamos mayores expectativas, en especial para avanzar en el desarrollo de normas adicionales para el comportamiento responsable de los Estados en materia de seguridad en el uso de las tecnologías de la información y las comunicaciones (TIC). No deben prejuzgarse los resultados de las discusiones sobre el futuro mecanismo de diálogo institucional periódico, ni privilegiar la propuesta del programa de acción por encima de otras iniciativas nacionales.

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, de forma declarada o encubierta, para 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.

Rechazamos los métodos de guerra no convencional que el Gobierno de los Estados Unidos continúa aplicando contra Cuba y los millonarios recursos que destina a ese fin. Condenamos el empleo de las nuevas tecnologías de la información y otras plataformas digitales para intentar desestabilizar a nuestro país, difundir noticias falsas y promover un cambio de régimen. 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, en particular el desarme nuclear, es necesario y posible. Cuba continuará promoviendo la adopción de medidas eficaces que nos permitan alcanzar ese noble fin.

Sr. Pieris (Sri Lanka) (*habla en inglés*): Sri Lanka se adhiere a la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados. Deseo formular la siguiente declaración en nombre de mi país.

La tercera década del siglo XXI se caracteriza, en esencia, por los rápidos avances y revoluciones de las tecnologías de la información y las comunicaciones (TIC). No cabe duda de que nos encontramos en un momento trascendental de la era digital y en un mundo que está aprovechando los beneficios de las TIC, que, hoy por hoy, están más intrínsecamente interrelacionadas con nuestra vida cotidiana que nunca. El espacio virtual que habitamos a diario da fe del papel vital que han llegado a desempeñar las TIC para todos, desde los Estados hasta las personas. Al haberse extendido a todas las esferas de las actividades humanas, las TIC se han convertido en un facilitador de todos esos ámbitos.

En mi país, en mayo se puso en marcha un programa llamado DIGIECON Sri Lanka 2023-2030, que pone de relieve la gran sinergia entre las TIC y el progreso económico de Sri Lanka y la firme determinación de transformar Sri Lanka en un país inclusivo desde el punto de vista digital. El programa, que comprende un plan maestro digital y un marco de política regulatoria, junto con una serie de eventos anuales, tiene por objeto propulsar la economía de Sri Lanka hacia una economía digital inclusiva mediante el aprovechamiento de soluciones avanzadas basadas en la tecnología.

Al mismo tiempo que anuncia esas fronteras y a pesar de todas sus características positivas, el ciberespacio, al igual que otros tipos de tecnologías transformadoras, también da cobijo a diversos actores que se entregan a actividades delictivas y terroristas, así como a quienes, por su propio interés, propagan el odio, la intolerancia y la incitación a la violencia, especialmente en los medios sociales. En los últimos tiempos se han observado niveles de vulnerabilidad sin precedentes en lo que se

refiere a los ciberataques y otras actividades maliciosas dirigidas contra los servicios de las TIC, de manera que se perturba la vida de millones de personas con solo pulsar unos botones.

Por consiguiente, Sri Lanka apoya las deliberaciones multilaterales que tienen lugar en el marco del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Se trata del único mecanismo inclusivo que se lleva a cabo en el seno de las Naciones Unidas con la participación activa e igualitaria de todos los Estados. Acogemos con beneplácito la aprobación de su segundo informe anual sobre los progresos realizados (véase A/78/265) y la creación del directorio mundial e intergubernamental de puntos de contacto, y aguardamos con interés sus futuras deliberaciones. Asimismo, estamos siguiendo con interés los debates en curso del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos.

Recalcamos que esas tecnologías deben usarse con arreglo a los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional y, 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, arreglo pacífico de controversias, respeto de los derechos humanos y adhesión al principio reconocidos de coexistencia pacífica entre los Estados. Por lo tanto, los Estados afectados son los principales responsables de promulgar leyes y adoptar medidas para prevenir las actividades ilegales y delictivas dirigidas contra particulares, la industria o los organismos gubernamentales, aunque muchos países en desarrollo, incluido el mío, se enfrentan a limitaciones de capacidad.

La creatividad del ser humano es bien conocida, como también lo su capacidad para autodestruirse utilizando esa creatividad y persiguiendo su interés propio a corto plazo, ya sea mediante el uso malicioso de las tecnologías disponibles o la invención de otras nuevas, como la inteligencia artificial o los sistemas armamentísticos autónomos letales. No podemos permitirnos desventuras que pongan en peligro nuestra misma existencia.

Sra. Lipana (Filipinas) (*habla en inglés*): Filipinas hace suyas las declaraciones formuladas por el representante de Tailandia, en nombre de la Asociación de Naciones de Asia Sudoriental, y el representante de Indonesia, en nombre del Movimiento de Países No Alineados (MNOAL). Permítaseme hacer las observaciones siguientes a título nacional.

Apoyamos firmemente el proyecto de resolución A/C.1/78/L.4 del MNOAL, relativo a la relación entre desarme y desarrollo, en el que se hace hincapié en la importancia de armonizar el desarme con los objetivos globales de desarrollo. El proyecto de resolución pide que se reduzca el gasto militar y se reasignen los recursos al desarrollo económico y social, de manera que se reduzca la disparidad entre las naciones desarrolladas y las naciones en desarrollo. En él se subraya la relación simbiótica que existe entre el desarme y el desarrollo y el papel que desempeña la seguridad en la consecución de la paz y la prosperidad.

Filipinas respalda plenamente el proyecto de resolución A/C.1/78/L.6 del MNOAL, relativo a las normas medioambientales y el desarme, en el que se pone de relieve el vínculo crucial entre la protección del medio ambiente y la seguridad mundial, lo que fomenta un desarme responsable centrado en la preservación del medio ambiente. Filipinas se suma al MNOAL para destacar la importancia del multilateralismo en las iniciativas de desarme y no proliferación y resalta la capacidad de las negociaciones transparentes y la cooperación entre los Estados para preservar la paz y la seguridad mundiales.

En cuanto a la seguridad y la utilización de las tecnologías de la información y las comunicaciones (TIC), Filipinas apoya plenamente 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). Destacamos que las TIC tienen efectos positivos en el desarrollo y que es necesario que los Estados se comporten de manera responsable para garantizar la estabilidad y la seguridad en el ciberespacio. Filipinas deplora el uso malicioso de las TIC que vulnera el derecho internacional y pide que se adopten medidas colectivas para salvaguardar el ciberespacio y promover su uso pacífico.

Respaldamos el segundo informe anual sobre los progresos realizados del Grupo de Trabajo de Composición Abierta (véase A/78/265). El Grupo de Trabajo, que funciona por consenso y abarca a todos los miembros, ha logrado producir resultados orientados a la acción para fomentar la confianza entre las naciones en materia de ciberseguridad. Filipinas apoya plenamente los buenos resultados que ha obtenido hasta la fecha como mecanismo vigente que tiene en cuenta las preocupaciones y los intereses en materia de ciberseguridad de

todos los Estados Miembros de las Naciones Unidas. Somos partidarios de crear un mecanismo permanente de una sola vía, dirigido por los Estados y bajo los auspicios de las Naciones Unidas, que dependa de la Primera Comisión. El mecanismo debe ser abierto, inclusivo, transparente, sostenible y flexible para adaptarse a las necesidades cambiantes de los países en desarrollo en el dinámico entorno de las TIC. Esperamos que todos podamos contribuir a que reine la armonía entre nuestras iniciativas dirigidas a conseguir ese objetivo y en nuestras deliberaciones actuales y futuras sobre cuestiones de ciberseguridad.

Como hemos venido escuchando a lo largo de las consultas informales, no es útil que haya proyectos de resolución concurrentes, que lo que hacen es fomentar la división. En ese sentido, con la intención de tender puentes, hemos contraído y mantenemos el compromiso de ayudar a encontrar puntos de encuentro, y Filipinas seguirá colaborando con los proponentes y las delegaciones interesadas para trabajar en un futuro mecanismo que pueda gozar del mayor apoyo posible.

En cuanto a las armas autónomas letales, Filipinas respalda plenamente el proyecto de resolución A/C.1/78/L.56 sobre el asunto. Encomiamos a la comunidad internacional por reconocer la urgente necesidad de afrontar los retos que plantean los sistemas de armas autónomos, que suscitan preocupaciones humanitarias, jurídicas, tecnológicas, éticas y de seguridad. Al encarar el rápido desarrollo de esas tecnologías, es crucial defender el derecho internacional y mantener las exigencias más elevadas de la humanidad. La inclusividad del proyecto de resolución, que tiene en cuenta diversas perspectivas, garantiza un enfoque integral para afrontar esta cuestión fundamental. Al encargar a la Secretaría que elabore un informe exhaustivo en el que se examinen los avances tecnológicos y se cuente con la participación de diversas partes interesadas, se demuestra que la comunidad internacional tiene el compromiso de defender el derecho internacional y salvaguardar la paz y la seguridad. Filipinas cree que el proyecto de resolución catalizará las medidas multilaterales colectivas destinadas a hacer frente a los retos que plantean los sistemas armamentísticos autónomos letales. Confiamos en continúen los debates y los avances sobre este asunto en el marco de la Convención sobre Ciertas Armas Convencionales.

En conclusión, Filipinas se mantiene firme en su empeño de construir un futuro de seguridad, desarrollo y uso responsable de la tecnología. Nos comprometemos a apoyar sin fisuras los principios de desarme y desarrollo sostenible y abrazamos el poder del multilateralismo. Además, hacemos hincapié en la necesidad de salvaguardar el ámbito digital, garantizar el uso pacífico de las TIC y mantener la seguridad del ciberespacio.

Por último, defendemos las iniciativas internacionales destinadas a afrontar los retos éticos y de seguridad que plantean las armas autónomas letales. Juntos, podemos dar respuesta a esas complejas cuestiones en cumplimiento del derecho internacional y las exigencias más elevadas de la humanidad.

Sr. Sivamohan (Malasia) (*habla en inglés*): Malasia se adhiere a las declaraciones formuladas por el representante de Indonesia, en nombre del Movimiento de Países No Alineados, y el representante de Tailandia, en nombre de la Asociación de Naciones de Asia Sudoriental (ASEAN).

La dependencia sin precedentes de las tecnologías de la información y las comunicaciones (TIC) que caracteriza a la sociedad global requiere que se preste una atención constante a las cuestiones de seguridad, que trascienden las fronteras nacionales, al tiempo que el creciente uso de las TIC ha brindado nuevas oportunidades para impulsar objetivos compartidos. Deben afrontarse con eficacia los riesgos y retos que plantea el uso malicioso de las TIC. En ese sentido, Malasia encomia 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 (2021-2025). Acogemos con beneplácito que en julio se aprobase el segundo informe anual sobre los progresos realizados del Grupo de Trabajo (véase A/78/265), que proporciona una base sólida para el trabajo de este último en el próximo año.

Nos complace que los Estados Miembros hayan alcanzado un acuerdo sobre los elementos para la elaboración y la puesta en práctica de un directorio mundial e intergubernamental de puntos de contacto. Además, Malasia espera con interés los debates adicionales del Grupo de Trabajo de Composición Abierta sobre, entre otros asuntos, las amenazas que plantean las TIC a las infraestructuras críticas y a las infraestructuras críticas de información, la integración sistemática de principios acordados de creación de capacidades en materia de TIC y la aplicación del derecho internacional en el uso de las TIC.

Malasia mantiene su compromiso de participar activamente en la labor del Grupo de Trabajo de Composición Abierta, que ha demostrado ser un valioso foro para que todos los Estados Miembros debatan sobre cuestiones de seguridad de las TIC teniendo en cuenta

las contribuciones de las partes interesadas pertinentes. La integridad, eficacia y credibilidad del Grupo de Trabajo deben mantenerse incluso mientras estudiamos posibles formatos de diálogo institucional periódico de cara a la etapa posterior a 2025.

Resulta tranquilizador observar que, como se refleja en el segundo informe anual sobre los progresos realizados del Grupo de Trabajo de Composición Abierta, los Estados Miembros han acordado, en principio, los elementos comunes en los que se basaría un futuro mecanismo de diálogo institucional periódico. Entre esos elementos figuran los siguientes:

> "Un mecanismo permanente de una sola vía, dirigido por los Estados y bajo los auspicios de las Naciones Unidas, que dependería de la Primera Comisión de la Asamblea General de las Naciones Unidas" (*A/78/265, anexo, párr. 55 a)*).

Además, los Estados Miembros:

> "Reconocieron la importancia del principio de consenso, tanto en lo que respecta al establecimiento del futuro mecanismo en sí como a sus procesos de toma de decisiones" (*ibid., párr. 56*).

A ese respecto, Malasia reitera que deberían evitarse las vías multilaterales paralelas en ámbitos clave del desarme y la seguridad internacional. Se trata de una cuestión que preocupa especialmente a las delegaciones más pequeñas de los países en desarrollo, dadas sus limitaciones en lo que concierne a recursos financieros y humanos.

En un contexto de renovadas tensiones entre las principales Potencias en el que impera la falta de confianza, el Grupo de Trabajo de Composición Abierta ha obtenido resultados tangibles de forma gradual y consensuada, lo que demuestra la buena fe con la que todas las delegaciones han participado en el proceso. A pesar de que hay opiniones divergentes sobre cuestiones específicas de su ámbito, está claro que el Grupo de Trabajo constituye en sí mismo una medida vital de fomento de la confianza. Mientras estudiamos diversas propuestas sobre cómo proceder en el futuro, sigamos trabajando de forma constructiva para garantizar que el Grupo de Trabajo alcance todo su potencial, de conformidad con su mandato. Mi delegación espera fervientemente que, hasta el final de su mandato, el Grupo de Trabajo siga siendo una plataforma de una sola vía, abierta e inclusiva que pueda responder con flexibilidad a las necesidades de los Estados Miembros ante la rápida evolución del ámbito de la seguridad de las TIC.

Sr. In Den Bosch (Reino de los Países Bajos) (*habla en inglés*): Además de la declaración formulada en nombre de la Unión Europea, quisiera hacer las siguientes observaciones a título nacional.

Las tecnologías de la información y las comunicaciones (TIC) son importantes impulsoras del desarrollo sostenible y pueden tener una influencia positiva en la vida de las personas. Sin embargo, el riesgo de que actores estatales y no estatales utilicen estas tecnologías de forma indebida aumenta a la par que nuestra dependencia de ellas. Por lo tanto, es crucial no solo que defendamos las reglas y normas aplicables al uso de las TIC por parte de los Estados, sino que las reforcemos. Debemos aprovechar el potencial de las tecnologías digitales para el desarrollo económico y social, al mismo tiempo que garantizamos la seguridad y el bienestar de las sociedades y las personas.

Para hacer frente a esos retos, los Estados han creado un marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional. No es un logro desdeñable. El marco ha sido el resultado de ingentes negociaciones e iniciativas para fomentar la confianza entre los Estados y, por tanto, cuenta con el respaldo de todos los Miembros de las Naciones Unidas. El informe anual de 2023 sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) añade otra capa importante a ese marco al reafirmar la aplicabilidad del derecho internacional al ciberespacio y realizar avances concretos en la creación de un directorio de puntos de contacto. El informe brinda recomendaciones concretas sobre la aplicación de las normas de comportamiento responsable de los Estados, afianza la necesidad de adoptar una perspectiva de género al hacer frente a las amenazas que plantean las TIC y fomenta una creación de capacidades que responda a las cuestiones de género. En ese sentido, los Países Bajos seguirán apoyando la participación de las mujeres en el Grupo de Trabajo mediante las becas Women in Cyber.

Acogemos con beneplácito la labor expuesta en el informe, incluida la profundización en interpretaciones comunes de la forma de aplicar los principios específicos del derecho internacional en el ciberespacio. Asimismo, seguimos apoyando las actividades del Grupo de Trabajo de Composición Abierta sobre la creación de capacidades destinada a impulsar la aplicación del marco consensuado. Con vistas a consolidar los avances ya logrados en el informe anual sobre los progresos

realizados del Grupo de Trabajo, los Países Bajos esperan que el proyecto de documento de posición de Singapur para respaldar el informe se apruebe sin votación.

Los Países Bajos apoyan la iniciativa del programa de acción de crear un mecanismo permanente, inclusivo y orientado a la acción cuando termine la labor del actual grupo de trabajo de composición abierta en 2025. El programa de acción debe impulsar iniciativas que persigan dos objetivos: en primer lugar, mantener el progreso y el desarrollo del marco normativo de comportamiento responsable de los Estados sobre la base del consenso, y, en segundo lugar, fomentar la cooperación internacional para promover la aplicación de ese marco evolutivo. Estos dos objetivos también se mencionan en la conclusión del informe del Secretario General sobre el programa de acción (A/78/76), que acoge con beneplácito las propuestas orientadas a la acción que favorezcan la aplicación del marco normativo y respalden las capacidades de los Estados en ese sentido.

En su contribución al informe del Secretario General sobre el programa de acción, los Países Bajos propusieron un mecanismo basado en las necesidades que facilitase la creación de capacidades en el marco del programa de acción y aprovechase las iniciativas ya existentes dentro y fuera del sistema de las Naciones Unidas. La propuesta no es aún definitiva, y seguiremos trabajando en ella con otros Estados Miembros.

En cuanto al impulso de la iniciativa del programa de acción, los Países Bajos apoyan firmemente el proyecto de resolución A/C.1/78/L.60, presentado por Francia, que establece un calendario y unos objetivos claros con vistas a crear un futuro mecanismo de diálogo institucional periódico para 2026. Además, incentiva a seguir desarrollando el mecanismo en el seno del actual grupo de trabajo de composición abierta y adopta un enfoque equilibrado sobre la posibilidad de que se requieran otras obligaciones jurídicamente vinculantes en el futuro.

En conclusión, los Países Bajos esperan con interés continuar la labor del Grupo de Trabajo de Composición Abierta y lograr avances tangibles hacia un ciberespacio más abierto, libre, seguro, interoperable y pacífico.

Sr. Fausto González (México): México concede una importancia especial al enfoque del uso responsable y pacífico del ciberespacio. En una era digital en la que la mayoría de las actividades humanas están interconectadas a través del ciberespacio, es esencial reconocer que el comportamiento irresponsable en esta esfera puede llevar a ciberataques, a tensiones geopolíticas e incluso a conflictos.

Es por ello por lo que México reitera la urgencia de asegurar un ciberespacio que sea abierto, libre, estable, seguro, accesible y resiliente para todos. Desde nuestra óptica, la aplicabilidad del derecho internacional, incluido el derecho internacional humanitario, en el ciberespacio es innegable. Estamos firmemente comprometidos con la implementación rigurosa de normas y principios que establezcan el comportamiento responsable de los Estados en este dominio. En esta búsqueda, vemos la necesidad de equilibrar las preocupaciones de ciberseguridad con la protección de los derechos humanos y el fomento del desarrollo a través de las tecnologías de la información.

Para los países en desarrollo, la regulación del ciberespacio no es simplemente una cuestión de seguridad, sino un prerrequisito para el desarrollo sostenible en su sentido más amplio. Es una herramienta que, si se utiliza y regula adecuadamente, es capaz de impulsar la innovación, garantizar el acceso equitativo a la información, fortalecer nuestra economía digital y cerrar las brechas de desigualdad que existen en el mundo.

Una preocupación latente y que compartimos con muchos Estados es la posibilidad de una carrera de capacidades ofensivas en el ciberespacio. Es alarmante pensar que las naciones o incluso entidades privadas puedan dirigirse hacia el desarrollo de capacidades ofensivas avanzadas que resulten en acciones potencialmente desestabilizadoras. Ante esto, México aboga por un compromiso colectivo para evitar que el ciberespacio se convierta en un nuevo escenario de rivalidades.

El Presidente vuelve a ocupar la Presidencia.

Bajo esta visión, reiteramos nuestra confianza en el multilateralismo. Consideramos que las Naciones Unidas, y en especial 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), representan el foro ideal para seguir abordando de manera integral los desafíos que el ciberespacio y las tecnologías de la información presentan en el contexto de la seguridad internacional. Resaltamos los significativos avances en las deliberaciones de dicho grupo, de manera particular en la aprobación de dos informes anuales de progresos y en el establecimiento y operación del directorio mundial de puntos de contacto, incluidas otras medidas de fomento de la cooperación y la confianza en el ciberespacio. Es especialmente importante que el grupo de trabajo siga promoviendo la construcción de entendimientos bajo el privilegio del diálogo y evite la división de esfuerzos en detrimento de todos nuestros países.

Finalizo haciendo un llamado a mantener discusiones productivas y constructivas que nos lleven hacia un mecanismo de diálogo permanente sobre ciberseguridad. Este mecanismo debe ser inclusivo y permitir la participación de todos los actores relevantes, así como la cooperación internacional y la creación de capacidades con base en las diversas necesidades regionales y subregionales. El diálogo para el desarrollo de un mecanismo institucional permanente sobre ciberseguridad, que considere la creación de capacidades e incluya las normas del derecho internacional, las reglas y los principios para el comportamiento responsable de los Estados y las medidas de fomento de la confianza, deben continuar entre las prioridades del grupo de trabajo. México aboga por que las próximas sesiones sustantivas del grupo de trabajo logren nuevamente consolidar más recomendaciones encaminadas a garantizar un ciberespacio pacífico y justo para todos.

Sra. Lukabyo (Australia) (*habla en inglés*): Todos nos beneficiamos de un ciberespacio abierto, seguro, estable, accesible y pacífico. Nunca ha sido tan evidente la importancia de que el ciberespacio se base en normas, que es lo único puede proporcionar la estabilidad y la independencia necesarias para que todos los países determinen su propio futuro digital y su desarrollo económico.

Sin embargo, nunca antes el ciberespacio había sido tan disputado. Este año siguen produciéndose casos inaceptables de ciberactividad maliciosa en nuestra propia región indopacífica y en otros lugares, como el ataque de Rusia a la infraestructura energética de Ucrania. Las cuestiones cibernéticas se han convertido en asuntos estratégicos de política exterior que preocupan con urgencia a todos los países. Todos tenemos la responsabilidad de trabajar de consuno y con la industria, la sociedad civil y la comunidad técnica para gestionar los complejos retos de la seguridad internacional en el ciberespacio y de centrar nuestros esfuerzos en promover la paz y evitar los conflictos.

Australia mantiene su firme compromiso de colaborar para hacer frente a esos retos, en particular a través de las Naciones Unidas, que cuentan con una sólida trayectoria de fomento de la cooperación internacional para comprender las amenazas incipientes y reducir los riesgos para la paz y la seguridad internacionales.

Reafirmamos una vez más nuestro compromiso de actuar de conformidad con el marco de las Naciones Unidas de comportamiento responsable de los Estados en el ciberespacio, confeccionado y acordado mediante los informes de consenso de los grupos de expertos gubernamentales y los grupos de trabajo de composición abierta de las Naciones Unidas. Australia seguirá compartiendo públicamente la manera en que aplica, interpreta y acata lo establecido en el marco. La transparencia favorece la rendición de cuentas, la previsibilidad y la estabilidad, por lo que alentamos a todos los Estados a que apliquen de forma significativa y cumplan fielmente sus compromisos de conformidad con el marco.

Australia se congratula del alto nivel de participación de mujeres representantes y de colaboración con las partes interesadas que se ha registrado recientemente en el quinto período de sesiones del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Asimismo, acoge con beneplácito el informe anual sobre los progresos realizados del Grupo de Trabajo (véase A/78/265) y su reafirmación inequívoca del marco. Alentamos a todos los Estados a que participen de forma significativa en los próximos pasos recomendados por el informe, en particular los relativos a que los Estados continúen participando en debates centrados en cómo aplicar el derecho internacional en el ciberespacio.

Australia concede gran importancia a que se obtengan resultados consensuados sobre cuestiones cibernéticas en las Naciones Unidas, habida cuenta de que esas cuestiones son demasiado importantes para abordarlas de forma separada en múltiples frentes. Australia lleva mucho tiempo defendiendo la creación de un mecanismo permanente de las Naciones Unidas que impulse el comportamiento responsable de los Estados en el ciberespacio y sea inclusivo, transparente, democrático y esté basado en el consenso.

Acogemos con beneplácito la iniciativa de Francia de liderar el proyecto de resolución A/C.1/78/L.60, relativo a la creación de un programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones, que nos prepara de forma significativa para hacer frente a las amenazas emergentes a la seguridad internacional. Australia subraya que cualquier nuevo mecanismo permanente no competiría con lo que ha habido antes. La modalidad y la estructura de los debates sobre cibernética en las Naciones Unidas han evolucionado considerablemente desde los tiempos del primer Grupo de Expertos Gubernamentales de 2004, que estaba formado por 15 expertos de los Estados que trabajaban a puerta cerrada, hasta la creación *ad hoc*, en 2018, de los grupos de trabajo de composición abierta,

en los que pueden participar los 193 Estados Miembros de las Naciones Unidas. El programa de acción, que parte de la base de lo que se había hecho antes, representa el siguiente paso en estos debates y garantiza que en el futuro se conceda a estas cuestiones la atención e importancia que merecen.

Además, debemos colaborar para garantizar el desarrollo, el despliegue y el uso responsables de la inteligencia artificial (IA) en el ámbito militar. La aplicación militar de la IA genera tanto nuevas oportunidades como riesgos potenciales. Australia seguirá participando activamente en esta nueva agenda internacional, por ejemplo en la Cumbre sobre Inteligencia Artificial Responsable en el Ámbito Militar, que se celebrará el año que viene en la República de Corea. Encomiamos a los Estados Unidos por su liderazgo en la Declaración Política sobre el Uso Militar Responsable y la Autonomía de la Inteligencia Artificial. Australia seguirá colaborando con diligencia con todos los Estados Miembros para llegar a un consenso sobre cuestiones cibernéticas y de IA que se base en el respeto del derecho internacional y las normas de comportamiento responsable de los Estados.

Sr. Vidal Mercado (Chile): Chile suscribe la intervención realizada por el representante de Indonesia en nombre del Movimiento de Países No Alineados.

Consideramos que el uso malicioso de las tecnologías de la información y las comunicaciones (TIC) puede afectar no solamente el desarrollo y el bienestar de los Estados, y sus niveles de digitalización, resiliencia, e infraestructura, sino que también representan una amenaza a la seguridad internacional. De la misma forma, los ciberataques y las actividades maliciosas en el ciberespacio pueden impactar con mayor gravedad a determinados grupos y entidades, como son las personas vulnerables, las personas mayores, y las mujeres y las niñas. Por lo anterior, es fundamental que la comunidad internacional siga trabajando para generar los consensos necesarios que garanticen un ciberespacio libre, abierto, accesible, estable, seguro y pacífico. 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 responsable de los Estados en el ciberespacio, incluyendo el derecho internacional humanitario, el derecho internacional de los derechos humanos, y la implementación de las 11 normas voluntarias y no vinculantes de las Naciones Unidas.

Reconocemos los avances y logros 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, particularmente en el ámbito de la creación y desarrollo de capacidades, y el establecimiento de medidas de fomento de la confianza, destacando en este sentido el establecimiento de un directorio mundial de las Naciones Unidas para puntos de contacto nacionales. De la misma forma, destacamos el 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. Es fundamental poder avanzar en mejorar nuestras capacidades, y poder generar instancias de cooperación e intercambio de información, promoviendo en ese sentido el trabajo con todas las partes interesadas, como el sector privado, la sociedad civil, el sector académico y la comunidad técnica, entre otros. Destacamos también la importancia de la aproximación regional y del trabajo con organismos regionales en cuanto a la implementación del marco de trabajo del grupo de trabajo de composición abierta.

No cabe duda de que el desarme, la no proliferación y el control de armamentos pueden repercutir positivamente en el bienestar humano, la igualdad, la justicia y sobre todo el desarrollo de este mundo, en particular de los países menos adelantados, los pequeños Estados insulares en desarrollo y los países en desarrollo sin litoral. Pues, el elevado gasto militar claramente podría tener un fin más noble. Es fundamental promover una mayor representación de los países menos adelantados en los foros multilaterales que se refieren al desarme y la seguridad internacional.

Finalmente, nos permitimos hacer un llamado para que todos los miembros respalden los tres proyectos de resolución presentados por el Movimiento de Países No Alineados sobre este grupo temático y los demás. También destacamos la resolución A/C.1/78/L.19, sobre la juventud, el desarme y la no proliferación. Creemos que es necesario incentivar la toma de conciencia en la juventud sobre estas materias, que son apremiantes, para tener el día de mañana líderes y tomadores de decisiones informados y educados sobre una materia tan sensible para vivir en paz y así en un mundo mejor. De igual manera, agradecemos a la sociedad civil, las instituciones educativas y las organizaciones no gubernamentales que se esmeran por aportar información sobre el desarme y la seguridad internacional.

Sra. Hanlumyuang (Tailandia) (*habla en inglés*): Tailandia hace suyas las declaraciones formuladas en nombre del Movimiento de Países No Alineados y de la Asociación de Naciones de Asia Sudoriental (ASEAN).

La ciberseguridad es uno de los asuntos más importantes en el mundo interconectado actual. El uso indebido de las tecnologías de la información y las comunicaciones (TIC) se ha convertido en una amenaza cada vez más grave para la paz y la seguridad internacionales, así como para la humanidad. Es imperioso que nos esforcemos por promover que el ciberespacio sea un entorno abierto, seguro, estable, accesible, compatible, pacífico y resiliente. Para lograrlo, Tailandia desea reiterar cuatro cuestiones importantes.

En primer lugar, Tailandia reafirma la importancia de un ciberespacio basado en normas para prevenir actos maliciosos y conflictos en el ciberespacio. Reiteramos la posición que mantenemos desde hace tiempo de que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable en el contexto de las TIC. Como complemento del Derecho internacional, las 11 normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados en el ciberespacio constituyen una base muy sólida para fomentar la confianza entre los Estados. Es esencial que los Estados sigan forjándose una interpretación de cómo se aplica el Derecho internacional en el contexto de las TIC y detectando dónde existen lagunas. Los Estados deben colaborar para elaborar orientaciones adicionales, incluida una lista de comprobación sobre la aplicación de las normas.

En segundo lugar, se necesitan diálogos institucionales periódicos abiertos, inclusivos y transparentes como plataforma para debatir las cuestiones mencionadas. Los diálogos también podrían servir para compartir las mejores prácticas y potenciar las iniciativas de creación de capacidades. El actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) sigue constituyendo un marco crucial para este tipo de debate. Agradecemos al Embajador Burhan Gafoor de Singapur su labor excepcional como Presidente, gracias a la cual se logró la aprobación por consenso del segundo informe anual sobre los progresos realizados (véase A/78/265). Tailandia acoge con beneplácito la propuesta de creación de un futuro mecanismo para promover un diálogo institucional periódico sobre esa cuestión, en particular el programa de acción. Apoyamos un mecanismo permanente de una sola vía, dirigido por los Estados y bajo los auspicios de las Naciones Unidas.

En tercer lugar, Tailandia subraya el papel vital que desempeñan las medidas de fomento de la confianza para promover que los Estados se fíen unos de otros en el ciberespacio a todos los niveles. Tailandia acoge con beneplácito el resultado concreto del Grupo de Trabajo de Composición Abierta relativo a la creación y puesta en funcionamiento de un directorio mundial e intergubernamental de puntos de contacto, que podría facilitar las comunicaciones seguras y directas entre los Estados para contribuir a prevenir y abordar los incidentes graves relacionados con las TIC y rebajar las tensiones en situaciones de crisis. Es igualmente importante reforzar las medidas de fomento de la confianza a través de actividades regionales. Entre las iniciativas y mecanismos relacionados con este tipo de medidas desarrollados por la ASEAN figuran su Estrategia de Cooperación en Ciberseguridad 2021-2025, su Comité Coordinador de Ciberseguridad y la reunión entre períodos de sesiones de su Foro Regional sobre la Seguridad y la Utilización de las Tecnologías de la Información y las Comunicaciones.

Por último, Tailandia reconoce que se precisan programas de creación de capacidades para ayudar a los Estados a mejorar su ciberresiliencia y a aplicar las normas y el derecho internacional. Alentamos a aquellos Estados que estén en condiciones de hacerlo a que sigan apoyando estos programas, que deben ser sostenibles, políticamente neutrales y transparentes y estar impulsados por la demanda. En ese sentido, nos gustaría dar las gracias al Japón mantener desde 2018 su apoyo al Centro de Fomento de la Capacidad en Seguridad Cibernética de la ASEAN y el Japón, con sede en Bangkok.

En conclusión, Tailandia tiene el compromiso de colaborar activamente con todas las partes para tratar de tender puentes entre puntos de vista divergentes con el fin de construir un entorno de las TIC más seguro y estable.

Sr. Saadi (Iraq) (*habla en árabe*): En primer lugar, la delegación del Iraq desea hacer suyas las declaraciones formuladas por el representante de Jordania, en nombre del Grupo de los Estados Árabes, y el representante de Indonesia, en nombre del Movimiento de Países No Alineados.

La delegación del Iraq se suma a los llamamientos a la entidad israelí para que ponga fin al brutal bombardeo de civiles desarmados que está llevando a cabo en la Franja de Gaza. Insistimos en la necesidad de un alto el fuego y de que se preste asistencia humanitaria para poner fin al sufrimiento humanitario de la población de la Franja y a su desplazamiento forzoso sistemático.

Como respuesta a la posesión, refuerzo y crecimiento continuos de los arsenales militares y al aumento de las tensiones internacionales y regionales, se está intensificando la carrera armamentista y el gasto militar mundial, lo que, en conjunto, plantea graves amenazas para la paz y la seguridad internacionales y regionales. Por ello,

todos debemos adoptar medidas urgentes y efectivas para reducir esas amenazas y promover la paz y la seguridad internacionales y regionales con el fin de alcanzar los Objetivos de Desarrollo Sostenible de aquí a 2030.

La delegación del Iraq recalca que la promoción de la universalidad de las convenciones y los tratados de desarme, incluidos los relativos al desarme de las armas de destrucción masiva, especialmente las armas nucleares, es la única garantía de que no se utilizarán dichas armas y no se amenazará con su uso y de que se evitarán sus desastrosas repercusiones. Esas armas son letales y destructivas tanto para los seres humanos como para el medio ambiente. Las soluciones acordadas en el seno de las Naciones Unidas en un marco multilateral constituyen la única garantía sostenible para afrontar las cuestiones relacionadas con el desarme y la seguridad internacional. Por lo tanto, es necesario reiterar y cumplir los compromisos individuales y colectivos contraídos en un contexto multilateral internacional. Asimismo, es importante que las Naciones Unidas desempeñen un papel fundamental en el ámbito del desarme y la no proliferación.

La delegación del Iraq expresa su creciente preocupación por el aumento de las tensiones internacionales y regionales en el entorno de la seguridad internacional, que ha contribuido al incremento del uso de las tecnologías de la información y las comunicaciones (TIC) en actividades que amenazan la paz y la seguridad regionales e internacionales. A ese respecto, el Iraq acoge con beneplácito la aprobación del segundo informe anual sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), establecido en virtud de la resolución 75/240, y celebra también la excepcional labor desempeñada por el Presidente del Grupo de Trabajo, el Embajador Burhan Gafoor. Estamos dispuestos a respaldarle plenamente y a hacer todo lo posible para garantizar el éxito de futuros períodos de sesiones, de manera que se aprueben recomendaciones que den apoyo a todos los Estados, especialmente a los países en desarrollo, y les ayuden a hacer frente a los retos y riesgos derivados del uso de las TIC, además de a las crecientes amenazas que existen en ese ámbito. De este modo se contribuirá a la construcción de un ciberespacio seguro y accesible para todos.

Sr. Ahmed (Pakistán) (*habla en inglés*): Estamos a punto de dar un paso monumental en la historia de la tecnología humana, presagiado por el advenimiento de la inteligencia artificial (IA), cuyo salto inevitable de los algoritmos al armamento continúa sin que se hayan creado salvaguardias adecuadas que rijan su diseño, desarrollo y despliegue. Además, nos encontramos en la antesala de una nueva carrera armamentista, en la que los algoritmos estarán al mando. A medida que la IA llega al campo de batalla, es razonable preguntarse si los seres humanos seguirán controlándola y al frente del interruptor para apagarla, y hasta qué punto.

Si los seres humanos no llevan las riendas, esos nuevos medios y capacidades militares que ha posibilitado la tecnología pueden aumentar los riesgos nucleares, incrementar la probabilidad de errores de cálculo y accidentes y provocar respuestas asimétricas, lo que reduciría el umbral del uso de la fuerza y los conflictos armados. En tiempos de crisis, un umbral bajo de uso de la fuerza sería muy desestabilizador. Además, esas nuevas herramientas pueden reconfigurar la dinámica de los conflictos, alterar las estrategias de disuasión, intensificar las carreras armamentistas, introducir patrones de escalada imprevistos y plantear nuevos riesgos en un entorno de seguridad internacional que ya es complejo.

Aunque algunos Estados destacan los beneficios que se derivan del uso de la IA en el campo de batalla, es igualmente importante subrayar los abrumadores riesgos y las consecuencias potencialmente catastróficas. El momento en que aún es posible adoptar medidas y salvaguardias se va pasando rápidamente a medida que nos preparamos para una irrupción tecnológica. Si no se hace frente a esos graves riesgos para la paz y la seguridad, los Estados afectados por las actuales asimetrías no tendrían más remedio que defenderse utilizando las capacidades de que disponen. Resulta alentador que aumente el número de iniciativas regionales y esfuerzos multilaterales destinados a dar respuesta a las aprensiones que suscitan las capacidades militares de la IA. Asimismo, agradecemos el llamamiento del Secretario General en favor de la gobernanza de la IA.

La respuesta de los mecanismos multilaterales ha sido más bien modesta e insuficiente. Las deliberaciones de la Convención sobre Ciertas Armas Convencionales (CCAC) se han centrado principalmente en la aplicación del derecho internacional humanitario y solo pretenden encarar los sistemas de armas autónomos letales (SAAL). No se centran ni en el tema más amplio del desarrollo de la IA en lo que respecta a todas sus aplicaciones militares, incluida su integración en los ámbitos ya existentes, ni en sus repercusiones para la seguridad y la estabilidad a escala mundial y regional.

En la Primera Comisión, un grupo de países ha presentado por primera vez un nuevo proyecto de resolución (A/C.1/78/L.56) sobre SAAL. Creemos que los

debates sobre SAAL deberían continuar en los grupos de expertos gubernamentales de la CCAC con el objetivo de elaborar normas internacionales mediante un nuevo protocolo. Al mismo tiempo, otros organismos de desarme pueden y deben desempeñar un papel complementario con el fin de encarar la cuestión más amplia de la IA en aplicaciones militares de una forma que favorezca las sinergias positivas y evite la duplicación.

La magnitud de los retos que plantea el uso de la IA con fines militares, en particular en sistemas de armas, exige una respuesta multilateral polifacética y holística. En consecuencia, este año, el Pakistán ha presentado en la Conferencia de Desarme un documento de trabajo con propuestas para incluir un punto en el orden del día con vistas a que se delibere sobre las implicaciones de la IA militar para la seguridad y la estabilidad.

El uso con fines militares de las tecnologías de la información y las comunicaciones (TIC) y del ciberespacio plantea amenazas muy graves para la paz, la seguridad y la estabilidad, tanto a escala internacional como regional. Las singulares diferencias entre el ámbito físico y el cibernético, así como la magnitud y el alcance de la aplicabilidad del derecho internacional vigente y su interpretación, exigen mayor prontitud en la consideración, elaboración y desarrollo de normas y reglas acordes que rijan la utilización del ciberespacio. Las deliberaciones en curso 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) tienen el potencial de alcanzar entendimientos comunes que pueden constituir la base para nuevos esfuerzos normativos encaminados a evitar que el ciberespacio se convierta en otro ámbito de conflicto.

Asimismo, nos complace formar parte de la declaración conjunta formulada por el representante de China sobre la promoción de la cooperación internacional para los usos pacíficos en el contexto de la seguridad internacional. Debe garantizarse el derecho de todos los Estados a hacer un uso pacífico de la ciencia y la tecnología con arreglo a sus obligaciones internacionales, sin discriminación y sin restricciones indebidas. Las iniciativas destinadas a regular el material y la tecnología de doble uso deben impulsarse en el marco de las Naciones Unidas y en entornos multilaterales inclusivos.

Sr. Moriko (Côte d'Ivoire) (*habla en francés*): Mi delegación hace suya la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados, y desea hacer las siguientes observaciones a título nacional.

A pesar de que son relativamente recientes, las amenazas a la seguridad vinculadas a las tecnologías digitales se encuentran entre las más complejas y alarmantes. De hecho, los autores estatales y no estatales cada vez utilizan más el ciberespacio con fines hostiles y las formas en que lo hacen evolucionan rápidamente, lo que a veces tiene graves repercusiones en todos los aspectos de la vida humana. Se trata de un fenómeno sin límites espaciales, de modo que pone en serio peligro la paz y la estabilidad mundiales y deberían buscarse soluciones con diligencia.

Dado que el desafío traspasa las fronteras, la respuesta solo será eficaces de verdad si tiene lugar también en un marco internacional y multilateral. Entre otras cosas, debería centrarse en la protección de las infraestructuras críticas y de las infraestructuras críticas de información, que son objeto de cada vez más ataques complejos que causan importantes perturbaciones y daños financieros e incluso ponen en peligro la vida de las personas. Debe prestarse especial atención a fomentar las iniciativas regionales destinadas a facilitar el intercambio de experiencias y buenas prácticas, como el Cyber Africa Forum, que se celebró el 24 y 25 de abril en Côte d'Ivoire y versó sobre la protección de las infraestructuras críticas frente a las ciberamenazas.

Además, es importante intentar evitar que el ciberespacio se utilice para la propaganda, la planificación y la logística terroristas, en particular mediante una aplicación más eficaz del Llamamiento a la Acción de Christchurch, concebido con el fin de eliminar los contenidos terroristas y extremistas violentos en línea y firmado por mi país en septiembre de 2019.

Asimismo, es esencial reforzar el marco de comportamiento responsable de los Estados, creado bajo los auspicios de las Naciones Unidas, mediante un compromiso más firme de incrementar la reflexión en el seno del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Los avances en las deliberaciones en el Grupo son motivo de legítimo optimismo para mi delegación, que este año ha vuelto a sumarse al consenso en torno al segundo informe anual sobre los progresos realizados (véase A/78/265), que se basa en un enfoque dinámico y tangible, también en lo que respecta a los próximos pasos.

En particular, mi delegación celebra la creación de un directorio mundial e intergubernamental de puntos de contacto, cuyo objetivo es intensificar la interacción y la cooperación de los Estados para aumentar la

transparencia y la previsibilidad, lo que contribuirá a preservar la paz y la seguridad internacionales. Además, mi país acoge con beneplácito los debates en curso sobre los requisitos y modalidades para crear un programa de acción destinado a promover un comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. Côte d'Ivoire apoya firmemente el programa de acción, que, sobre la base de la labor del Grupo de Trabajo, constituiría un mecanismo permanente inclusivo y orientado a la acción para responder a la necesidad de que las iniciativas de la comunidad internacional se adapten constantemente a retos de seguridad en constante evolución.

Mi país apoya sobre todo el concepto de un enfoque renovado sobre la creación de capacidades para los Estados, especialmente para los más vulnerables. No cabe duda de que este enfoque tendría efectos beneficiosos en la capacidad de los Estados para responder a los ciberincidentes y es esencial para facilitar que todos los Estados puedan aplicar el marco de comportamiento responsable con vistas a consolidar su alcance y a construir un entorno digital pacífico, fiable y resiliente. Por eso, el año pasado y de nuevo este año, mi delegación ha patrocinado el proyecto de resolución que promueve ese mecanismo e insta a que los debates sobre la creación de este se traduzcan en un resultado positivo.

Sra. González López (El Salvador): Las tecnologías de la información y las comunicaciones (TIC) son herramientas fundamentales en el mundo actual, pero su uso inconsistente con la normativa del comportamiento responsable de los Estados en el ciberespacio, así como su contravención al derecho internacional, particularmente la Carta de las Naciones Unidas, representan desafíos graves para nuestra seguridad internacional.

El Salvador es plenamente consciente del aumento en el uso de medios cibernéticos para amenazar infraestructuras críticas, infraestructuras críticas de información y cadenas de suministros globales. Estas amenazas requieren una discusión seria sobre la normativa del comportamiento responsable, el derecho internacional en el ciberespacio y medidas que fomenten la confianza, la capacidad y el diálogo institucional. Estos debates tienen lugar en el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, en el cual mi país participa de manera constructiva. Creemos que este grupo desempeña una labor crucial para establecer entendimientos comunes y encontrar convergencias en los temas del ciberespacio.

A pesar de los avances que El Salvador ha logrado en materia cibernética y digital, respaldamos conceptualmente el avance futuro de estas discusiones con un formato permanente e inclusivo bajo los auspicios de las Naciones Unidas. Por ello, hemos presentado opiniones nacionales y hemos participado en consultas que aporten elementos sobre el alcance, la estructura y el contenido de un futuro programa de acción sobre el comportamiento responsable de los Estados en el ciberespacio.

Durante este período de sesiones, la Primera Comisión ha escuchado un número creciente de Estados referirse a las implicaciones en la seguridad internacional de las tecnologías emergentes, en particular la inteligencia artificial (IA). Mi país ha sido enfático en los foros pertinentes acerca de los riesgos asociados, por ejemplo, con la inteligencia artificial generativa y el aprendizaje automático. Aunque vemos importantes oportunidades para mejorar nuestros sistemas de ciberseguridad mediante el uso de la IA, hacemos un llamado a adoptar un enfoque de IA para ciberseguridad y no ciberseguridad para IA.

Instamos a regular y promover el uso de la IA basado en riesgos y a emprender discusiones profundas sobre modelos de gobernanza para esta tecnología, así como a continuar analizando las posibles amenazas y desafíos con implicaciones para la seguridad internacional. Además, es relevante destacar que el uso de la IA en el campo de la seguridad va más allá de los sistemas de armas autónomas, abarcando una nueva dimensión centrada en la automatización y no solo en la autonomía. Llamamos a considerar la IA de manera integral, ya que, dada la naturaleza de esta tecnología, sus aplicaciones y usos afectan todos los aspectos de la vida humana, incluso aquellos que no están directamente relacionados con la seguridad. Esta dependencia tecnológica se profundiza rápidamente y requiere discusiones sustantivas.

El Salvador ha abordado en esta Primera Comisión el enfoque transversal de género como una herramienta crucial para comprender las diferentes experiencias de mujeres y hombres en los asuntos de seguridad, y el ciberespacio no es la excepción. Es innegable que la violencia de género puede agravarse con el uso de las TIC. Es por ello que instamos a seguir debatiendo este tema con el objetivo de crear entornos en línea más seguros y de reducir la brecha digital, especialmente la de género.

Finalmente, El Salvador concede gran importancia a la participación de múltiples actores en estos procesos. Los desafíos en el ciberespacio requieren una colaboración activa de la sociedad civil, organizaciones no

gubernamentales, organismos regionales, sector académico e industria. Por lo tanto, exhortamos a continuar trabajando con los valiosos aportes de estos actores precisamente en nuestras deliberaciones.

Sr. Muhith (Bangladesh) (*habla en inglés*): Bangladesh hace suya la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados. Permítaseme exponer nuestra posición nacional.

Resulta innegable que la rápida transformación del panorama de la seguridad mundial, impulsada por la rápida evolución de las tecnologías, subraya la necesidad de adoptar diversas medidas de desarme que no se circunscriban a los marcos convencionales. El rápido avance de la tecnología, especialmente en los campos de la inteligencia artificial (IA), los sistemas de armas autónomos, la biotecnología y las cibercapacidades, ha revolucionado no solo nuestra vida cotidiana, sino también el panorama de la seguridad mundial. Esas innovaciones han desbloqueado un potencial ilimitado para el progreso humano y el crecimiento económico. Sin embargo, también han traído consigo nuevos tipos de riesgo, que exigen soluciones de desarme innovadoras.

Bangladesh expresa su profunda preocupación por el desarrollo de las capacidades militares de IA y la aparición de tecnologías cuánticas, en particular las relacionadas con los sistemas de armas, que han puesto de manifiesto las deficiencias de los marcos de gobernanza existentes. Tenemos la responsabilidad primordial de utilizar la IA en favor de la paz, no del conflicto. Por lo tanto, recalcamos la urgente necesidad de marcos integrales eficaces para regular la IA y las tecnologías emergentes de manera que se garantice su uso responsable, eficaz y ético.

Estamos firmemente convencidos de que el ciberespacio tiene que considerarse un bien público mundial del que deben beneficiarse todos, en todas partes, sin discriminación alguna. Para poder aprovechar los enormes beneficios de las tecnologías digitales, la comunidad internacional debe favorecer un entorno de las tecnologías de las información y las comunicaciones (TIC) que sea seguro, abierto y digno de confianza y se sustente en la aplicabilidad del derecho internacional al ciberespacio, normas bien definidas de comportamiento responsable de los Estados, medidas sólidas de fomento de la confianza y la creación coordinada de capacidades. Nuestra única esperanza de crear un entorno de las TIC libre, seguro, estable, accesible y pacífico pasa por el multilateralismo, y hacemos hincapié en que las Naciones Unidas deben desempeñar un papel de liderazgo en el desarrollo de normas cibernéticas internacionales.

En ese sentido, Bangladesh considera que 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 un mecanismo fundamental e inclusivo en el marco de las Naciones Unidas. Reafirmamos nuestra contribución constructiva al éxito del Grupo de Trabajo y acogemos con beneplácito la aprobación por consenso de sus dos informes anuales consecutivos sobre los progresos realizados. En consonancia con el segundo informe anual sobre los progresos realizados (véase A/78/265), apoyamos la creación de un mecanismo permanente de una sola vía, dirigido por los Estados y en el seno de las Naciones Unidas. Asimismo, respaldamos el establecimiento de un proceso abierto, inclusivo, transparente, sostenible y flexible que pueda satisfacer de manera eficaz las necesidades cambiantes de los países en desarrollo en el panorama dinámico de las TIC.

A falta de una estructura normativa que goce de aceptación mundial, consideramos que los principios de la Carta de las Naciones Unidas y del derecho internacional pertinente deberían aplicarse al ciberespacio en lo que respecta al mantenimiento de 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, como la reciente Ley de Ciberseguridad de 2023, 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 en el espacio ultraterrestre debería ser objeto de más investigaciones y análisis fundamentados. La educación es fundamental para fomentar la comprensión de las consecuencias humanitarias y económicas de las armas. Bangladesh destaca la importancia de la educación para el desarme y la no proliferación. Agradecemos la valiosa labor que lleva a cabo el Instituto de las Naciones Unidas de Investigación sobre el Desarme y hacemos hincapié en la necesidad de destinar más recursos predecibles a apoyarlo en la ampliación y gestión de su base de conocimientos en beneficio de todos los Estados Miembros.

En conclusión, debemos situar a las personas en el centro de nuestras iniciativas de desarme y velar por que este salve vidas ahora y en el futuro. Continuemos colaborando para que el mundo sea un lugar más seguro.

Sr. Eustathiou de los Santos (Uruguay): El Uruguay comparte la preocupación de varios Estados Miembros en lo que respecta al incremento de las actividades maliciosas vinculadas a las tecnologías de la información y las comunicaciones (TIC), particularmente aquellas que afectan la vulnerabilidad de los sectores vinculados a la infraestructura crítica, sanitaria, de seguridad y defensa. Estas actividades malintencionadas son un problema real y creciente, que requiere de una mayor cooperación entre los Estados y entre los sectores públicos y privados para proteger su integridad, funcionamiento y disponibilidad.

En el Uruguay, estamos avanzando en fortalecer el Centro Nacional de Respuesta a Incidentes de Seguridad Informática, multiplicando su capacidad de respuesta y monitoreo de forma de minimizar los tiempos de detección y respuesta a incidentes, reduciendo riesgos y generando ahorros significativos para el país. Para hacer frente a estas amenazas reales y potenciales, el Uruguay considera fundamental que sigamos promoviendo gestiones tendientes a incrementar la cooperación y la generación de capacidades tomando en cuenta las diferencias que existen en cada país para hacer frente a los usos malintencionados de las TIC. Creemos que el objetivo central de la creación de capacidades es garantizar una participación segura, efectiva y significativa de todos los Estados en el ciberespacio para beneficiarse de las oportunidades de desarrollo sostenible que de ello se derivan. En ese sentido, los mecanismos de cooperación como la tradicional Norte-Sur, Sur-Sur y triangular, generarán acciones específicas de asistencia técnica para el desarrollo de capacidades, incluyendo aquellas orientadas a la aplicación de las 11 normas de comportamiento responsable de los Estados en el ciberespacio.

El Uruguay reafirma la relevancia de contar con un intercambio de buenas prácticas nacionales en materia de prevención de amenazas digitales. Tal como mi país lo ha hecho con varios países de nuestra región a través de nuestra Agencia de Gobierno Electrónico y Sociedad de la Información. También reconocemos el papel fundamental de las Naciones Unidas en la elaboración de medidas de fomento de la confianza y el apoyo a su implementación a nivel mundial, tal como ha sido resaltado en anteriores informes del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (A/76/135) y del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) (véase A/78/265).

Los desarrollos tecnológicos deben estar acompañados de una institucionalidad sólida, un marco de reconocimiento de los derechos humanos y construcción de entornos seguros y de confianza jurídica. Como sociedad se comparten obligaciones, pero además derechos y oportunidades. La aplicación conjunta de un marco normativo debe llevarse a cabo de forma coordinada, teniendo en cuenta las opiniones de los Miembros, basadas en un enfoque del ciberespacio centrado en el ser humano.

En ese sentido, nuestro país se ha planteado una agenda integral y continua, que hemos denominado Agenda Uruguay Digital, en la que analizamos el marco regulatorio, promoviendo su conocimiento y adopción, en colaboración con todos los actores involucrados. Para nosotros, la transformación digital viene de la mano de la seguridad jurídica, por eso promovemos las adaptaciones normativas necesarias para acompasar los avances tecnológicos, priorizando las mejoras en los procedimientos administrativos, los mecanismos para el intercambio de información entre entidades públicas y privadas, y la gestión de emprendimientos en el ámbito digital.

Mi delegación considera que, a la hora de adaptar los marcos regulatorios, debemos enfatizar en los aspectos de accesibilidad, derechos de autor, derechos del consumidor, defensa de la competencia, protección de datos, seguridad, transparencia y ciberdelitos, promoviendo además la adhesión a estándares y convenciones internacionales en esos temas.

Sra. Muigai (Kenya) (*habla en inglés*): Kenya hace suyas las declaraciones formuladas por los representantes de Nigeria e Indonesia en nombre del Grupo de los Estados de África y del Movimiento de Países No Alineados, respectivamente. Deseo añadir las siguientes observaciones a título nacional.

Damos las gracias al Representante Permanente de Singapur, Presidente del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), por la exposición informativa que presentará próximamente. Encomiamos los notables avances logrados por el Grupo de Trabajo de Composición Abierta bajo su liderazgo y confiamos en que se seguirán obteniendo resultados tangibles en este ámbito crucial.

En la era digital en la que vivimos, la influencia omnipresente de la tecnología configura nuestra sociedad global cada vez más interconectada. De hecho, el rápido avance de la era digital está redefiniendo en consecuencia nuestra percepción de la seguridad y nuestra forma de vida, incluido el desarrollo de la diplomacia. Lograr el difícil equilibrio entre la innovación y la prevención de las intenciones maliciosas es una labor crucial, aunque hercúlea. Es más, exige un esfuerzo colectivo mundial en el que se adopte un enfoque multilateral.

En ese sentido, nuestra principal tarea está clara: definir las reglas, normas y principios de comportamiento responsable entre los Estados a los efectos de nuestra seguridad y el uso de las tecnologías de la información y las comunicaciones. Ante los rápidos avances tecnológicos, se necesita urgentemente un entorno de rendición de cuentas en el que se mantenga la ciberseguridad y se fomente la colaboración digital mundial de forma responsable. Al emprender esa tarea global, debemos tener en cuenta las iniciativas de los Estados que han introducido innovaciones significativas y han sido pioneros en los avances de la seguridad digital. Alentamos a esos Estados a que sean magnánimos al compartir la información pertinente y las mejores prácticas para ayudar a otros países a desarrollar sus propias infraestructuras de ciberseguridad.

Asimismo, las Naciones Unidas deben ser proactivas en su apoyo a las naciones para que mejoren sus capacidades digitales y afronten las repercusiones de la revolución digital, incluido el uso indebido de la inteligencia artificial, los macrodatos y los medios sociales. A ese respecto, debe impulsarse y reforzarse la cooperación y la coordinación en materia de creación de capacidades recurriendo a los organismos y organizaciones especializados existentes de múltiples partes interesadas, como el Foro Mundial de Competencia Cibernética. Además, es de vital importancia no dejar de estudiar ni de tratar de entender la incesante evolución del panorama de las ciberamenazas. Si disponemos de información sobre las amenazas existentes y potenciales en el ámbito de la seguridad de la información, podemos invertir en medidas preventivas y anticipatorias mediante la cooperación, la colaboración y la coordinación.

En su afán por proteger su espacio digital, Kenya ha adoptado diversas medidas, como la creación del Equipo Nacional de Respuesta a Incidentes Informáticos de Kenya, la implantación de una infraestructura nacional de clave pública y la reciente puesta en marcha del Comité Nacional de Coordinación en Materia de Delitos Informáticos y Cibernéticos, integrado por los ministerios y organismos pertinentes y dotado de una secretaría completa que vela por la aplicación efectiva de las decisiones.

En conclusión, la delegación de Kenya hace hincapié en que el diálogo institucional periódico, tal como se describe a grandes rasgos en nuestro mandato, es primordial para garantizar no solo que se escuche la voz de todas las naciones, sino también que aprendamos, actuemos y crezcamos juntos colectivamente. Sea nuestro objetivo común construir un espacio digital inclusivo y seguro para las generaciones actuales y futuras.

Sr. Gusmão de Sousa (Timor-Leste) (*habla en inglés*): Como Estado en desarrollo, Timor-Leste tiene en común con muchos otros Estados los beneficios y las amenazas que representan las tecnologías de la información y las comunicaciones (TIC) para los procesos de construcción nacional y desarrollo del país. Ello incluye el mantenimiento de la paz y la seguridad, basado en el respeto de la soberanía nacional de todos los Miembros y en virtud de normas sobre el uso pacífico de las TIC, tal y como se establece en la Carta de las Naciones Unidas.

La reciente pandemia de enfermedad por coronavirus nos ha mostrado la importancia de contar con recursos sólidos en el ámbito de la seguridad de las TIC. Debemos prestar especial atención a las necesidades de los países en desarrollo en lo que respecta a la aplicación de las normas vigentes y a su ampliación. El creciente desarrollo de las TIC, junto con las amenazas incipientes en el ciberespacio, causarán daños que pueden perjudicar nuestras vidas. Al ser un Estado pequeño, Timor-Leste cree que esta plataforma multilateral desempeña un importante papel, ya que ha proporcionado un mejor espacio para entablar un diálogo entre todos con el fin de salvar las divisiones entre países y velar por que todos puedan beneficiarse de las ventajas que nos aportarán las TIC.

Como país nuevo que se embarca en el proceso de digitalización de la nación, Timor-Leste sigue preocupado por la creciente amenaza de ciberataques contra las infraestructuras críticas y las infraestructuras críticas de información. Los Estados en desarrollo continúan enfrentándose a diferentes retos al responder a las ciberamenazas. En consecuencia, Timor-Leste considera que la coordinación y la cooperación y el intercambio de buenas prácticas a través de plataformas bilaterales, regionales y multilaterales respaldarán y reforzarán las estructuras nacionales. A ese respecto, desde nuestro punto de vista, el anterior Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta se complementaron en su labor y constituyeron

plataformas dinámicas para reforzar la cooperación y colaborar en materia de ciberseguridad.

Asimismo, aprovechamos esta oportunidad para encomiar a Singapur por dirigir las actividades del actual 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 deseamos destacar el papel central que ha desempeñado en el debate sobre las TIC y la paz y la seguridad internacionales bajo los auspicios de las Naciones Unidas. Acogemos con beneplácito la aprobación del informe anual de 2023 sobre los progresos realizados (véase A/78/265) y creación del directorio mundial de puntos de contacto, habida cuenta de que en la actualidad estamos estableciendo nuestros procedimientos internos relativos a ese proceso.

En cuanto a los futuros mecanismos de diálogo institucional periódico, Timor-Leste acoge con beneplácito la propuesta de elaboración de un futuro programa de acción sobre ciberseguridad, ya que creemos que puede ser un marco inclusivo, abierto, transparente y eficaz bajo los auspicios de las Naciones Unidas. No obstante, deseamos subrayar que el Grupo de Trabajo de Composición Abierta sigue siendo el foro adecuado para idear el programa de acción e implantarlo, pues se trata de un mecanismo inclusivo que refleja los intereses de todos los Estados. Asimismo, consideramos que, para que todos acepten el programa de acción, este debería centrarse en medidas de fomento de la confianza, especialmente en el caso de los países en desarrollo en lo que respecta a la satisfacción de sus necesidades, por ejemplo de creación de capacidades, con el fin de facultar a todos y reforzar la aplicación de las normas establecidas, también mediante la subsanación de las lagunas jurídicas en la aplicabilidad del derecho internacional al ciberespacio. En consecuencia, para prepararnos, celebramos que se sigan debatiendo las propuestas, incluidos los detalles concretos, como cuestiones organizativas.

Deseamos destacar la necesidad de fortalecer la cooperación multilateral para seguir el ritmo del panorama de la seguridad en rápida evolución, incluidos los acontecimientos en el ciberespacio. Estamos de acuerdo en que las medidas de fomento de la confianza son herramientas cruciales para propiciar que los Estados se fíen unos de otros y para prevenir los conflictos. A ese respecto, reafirmamos nuestro apoyo a los mecanismos de desarme y hacemos hincapié en la participación igualitaria de las mujeres en ellos.

Además, quisiéramos hacer nuestra la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados y destacar la importancia de garantizar que el uso de la información, las comunicaciones y la tecnología se ajuste plenamente a los propósitos y principios de la Carta de las Naciones Unidas y al derecho internacional. Timor-Leste concede gran importancia a la preservación del régimen jurídico internacional relativo al desarme y al control de armamentos. Su aplicabilidad al ciberespacio es importante para mantener la paz y la estabilidad. Dado que nuestro Gobierno está invirtiendo notablemente en el proceso de digitalización, en la actualidad estamos estableciendo el marco, la estrategia y la política necesarios en el ámbito del ciberespacio. En esa línea, pedimos la cooperación de todos en nuestras iniciativas, especialmente en el proceso de creación de capacidades.

Por último, consideramos que la colaboración con los sectores pertinentes, como el sector privado, ayudará a los Estados, especialmente a los países en desarrollo, a comprender la naturaleza de las amenazas y a cooperar y enfrentarse a ellas adecuadamente, lo que enriquecerá ese proceso.

Sra. Rodríguez Mancia (Guatemala): Nos encontramos ante una coyuntura internacional caracterizada por amenazas a la paz, así como frecuentes actos que atentan contra la seguridad mundial y flagelos que afectan a los sectores más vulnerables de nuestra sociedad. Aunado a esto, el desarrollo de las tecnologías de la información y las comunicaciones (TIC) crece a pasos agigantados, llamando a la atención la necesidad de profundizar en el conocimiento y fortalecimiento de las capacidades nacionales y de la cooperación en materia de ciberseguridad. El ciberespacio se ha convertido en un lugar de dominio central e indispensable para la actividad global, por lo que, por su naturaleza civil y de doble uso, ha sido utilizado por grupos criminales y terroristas en más de una ocasión. Es por ello que su protección mediante un comportamiento estatal responsable es fundamental para garantizar el mantenimiento de la paz y la seguridad internacionales.

Es sumamente preocupante que varios Estados estén desarrollando capacidades de TIC con fines militares, lo que ha provocado que el uso de estas tecnologías en futuros conflictos entre Estados sea cada vez más probable. Estas actividades representan una complejidad de condiciones que requieren de la participación y cooperación de todos los sectores de nuestros países para desarrollar los marcos técnicos y legales que fortalezcan la ciberseguridad, tanto a nivel nacional como global. Por esta razón, mi país cree plenamente en la necesidad de continuar impulsando la creación de capacidades

como una parte esencial para la cooperación de los Estados y la promoción de medidas de fomento de la confianza en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones. Guatemala reitera la importancia de contar con una plena transparencia y apoya las actividades de intercambio de información y difusión de mejores prácticas, tanto a nivel subregional como regional e internacional.

Mi delegación destaca que la aplicabilidad del derecho internacional al comportamiento de los Estados en el ciberespacio, las normas voluntarias no vinculantes de comportamiento de los Estados aplicables en tiempos de paz y la aplicación de medidas de fomento de la confianza siguen siendo cruciales. Además, después de ser testigo de las brechas existentes entre los países en materia de ciberseguridad y defensa, mi país otorga especial interés a los esfuerzos de creación de capacidad para encontrar un espacio más equitativo que ayude a mantener un balance en el contexto de la seguridad internacional.

Guatemala cuenta actualmente con una estrategia nacional de seguridad cibernética, cuyo principal objetivo es fortalecer las capacidades del país, creando el ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y el ejercicio de los derechos de las personas en el ciberespacio. Además de eso, en este último año Guatemala ha tenido un importante avance en el proceso de desarrollo de la ley de ciberseguridad. Mi país tiene el honor de ser país observador del Convenio del Consejo de Europa sobre la Ciberdelincuencia, que busca abordar los delitos informáticos y en Internet mediante la armonización de las leyes entre las naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre naciones.

Por lo anterior, vemos con positivismo el segundo informe anual sobre los progresos (véase A/78/265) del 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 resaltamos la importancia de la presentación del proyecto de resolución A/C.1/78/L.60 para establecer el programa de acción que busca fortalecer y avanzar en la creación de un mecanismo orientado al comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional, el cual ha sido apoyado por Guatemala. En esa línea, tomamos nota de las recomendaciones del Secretario General en la Nueva Agenda de Paz, que propone el establecimiento de un mecanismo multilateral independiente de rendición de cuentas sobre el uso malintencionado del ciberespacio por parte de los Estados.

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

Sr. Varem (Estonia) (*habla en inglés*): Estonia hace suya la declaración formulada por el observador de la Unión Europea. Además, nos gustaría destacar las siguientes cuestiones a título nacional.

Estonia concede una enorme importancia a prevenir y gestionar las amenazas a la paz y la seguridad internacionales, incluidas las derivadas del uso malicioso del ciberespacio. Las amenazas asociadas al uso de las tecnologías de la información y las comunicaciones (TIC) evolucionan y se intensifican, lo que pone de relieve la creciente preocupación por la seguridad nacional e internacional. Los ciberincidentes maliciosos pueden tener efectos devastadores para las metas de desarrollo económico y social y en las infraestructuras críticas, así como consecuencias directas en la estabilidad internacional.

En particular, la invasión ilegal y no provocada de Ucrania por parte de Rusia ha puesto de manifiesto que las ciberoperaciones se utilizan para respaldar objetivos militares y se han convertido en parte de las operaciones militares. Durante la agresión rusa, las autoridades gubernamentales, las infraestructuras críticas, los gobiernos locales, el sector de la seguridad y la defensa y las empresas privadas ucranianos han sido blanco de ataques en el ciberespacio. Además, se ha demostrado que las ciberoperaciones maliciosas tienen efectos indirectos peligrosos, lo que evidencia el carácter transfronterizo de las ciberamenazas.

Estonia condena enérgicamente estas ciberoperaciones maliciosas. Queremos destacar 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. Los Estados Miembros de las Naciones Unidas deben unir sus fuerzas para consolidar el orden internacional basado en normas y respetarlo también en el ciberespacio. Recordamos que cualquier uso de las TIC por los Estados de forma incompatible con las obligaciones que contrajeron en el marco de comportamiento responsable de los Estados menoscaba la paz y la seguridad internacionales, la confianza y la estabilidad entre los Estados Miembros.

Estonia valora muy positivamente 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 (2021-2025) y acoge con beneplácito el acuerdo alcanzado en julio con respecto al informe anual sobre los progresos realizados (véase A/78/265). A pesar de la difícil situación geopolítica, el informe de consenso subraya el creciente interés de los Estados Miembros de las Naciones Unidas por profundizar en los debates sobre el marco de comportamiento responsable de los Estados. Estonia considera que las deliberaciones sobre amenazas, normas, derecho internacional, creación de capacidades y futuro diálogo institucional han sido muy útiles para aclarar las perspectivas nacionales y regionales y también para fraguar los compromisos mundiales en materia de ciberestabilidad.

Los Estados Miembros de las Naciones Unidas han pedido en reiteradas ocasiones un mecanismo permanente de las Naciones Unidas sobre cuestiones cibernéticas en el contexto de la seguridad internacional. Estonia sigue apoyando la creación de un programa de acción inclusivo, de una sola vía y orientado a la acción una vez concluya la labor del actual grupo de trabajo de composición abierta en 2025, de acuerdo con lo expuesto en la resolución 77/37. Agradecemos que las próximas sesiones del Grupo de Trabajo de Composición Abierta vayan a proporcionar más ocasiones para configurar el programa de acción de forma colectiva.

Por último, nos gustaría reiterar la importancia de aprovechar los conocimientos especializados adquiridos por la comunidad de las distintas partes interesadas. Valoramos que las sesiones del Grupo de Trabajo de Composición Abierta ofrezcan oportunidades de contar con la participación significativa, periódica y sustancial del sector privado, la sociedad civil y el mundo académico. Estonia invita a los Estados y a otras partes interesadas a seguir participando en intercambios constructivos con el fin de compartir, escuchar y trabajar en pro de una mayor ciberresiliencia mundial.

Sra. Nam (Nueva Zelandia) (*habla en inglés*): Mi país está decidido a promover una conducta estatal responsable en un ciberespacio libre, abierto, pacífico y seguro. Los avances tecnológicos en el ciberespacio tienen el potencial de hacer del mundo un lugar más seguro y pueden contribuir al desarrollo sostenible, la prosperidad y el crecimiento económico. Sin embargo, el ciberespacio también se ha convertido cada vez más en un vector de amenazas nuevas y emergentes incompatibles con la paz y la seguridad internacionales, entre las que se encuentran el despliegue de programas maliciosos secuestradores, el ataque a infraestructuras críticas y el uso malicioso de la ciberactividad, que cada vez es más frecuente en el contexto de los conflictos armados.

Nueva Zelandia concede importancia a colaborar para hacer frente a esos retos y promover un comportamiento responsable de los Estados en línea. En ese sentido, acogemos con beneplácito el consenso alcanzado sobre el segundo informe anual sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) en su quinto período de sesiones sustantivo, celebrado en julio.

Nueva Zelandia señala, como ya lo ha hecho y lo han hecho muchos otros en ocasiones anteriores, que el ciberespacio no es un espacio sin ley y que el derecho internacional se aplica tanto en internet como en el mundo real. Nueva Zelandia se ha sentido alentada al ver que los Estados siguen compartiendo sus perspectivas nacionales sobre la aplicación del derecho internacional, incluida su opinión sobre la aplicabilidad del derecho internacional humanitario y el derecho internacional de los derechos humanos. Insistimos una vez más en nuestra posición de que la totalidad de la Carta de las Naciones Unidas es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el ciberespacio, y que los Estados pueden y deben esperar tener que rendir cuentas por su ciberactividad maliciosa contraria a la Carta y al derecho internacional.

Acogemos con beneplácito la propuesta de un programa de acción de las Naciones Unidas 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. Seguimos avanzando mucho en el marco del Grupo de Trabajo de Composición Abierta y nuestros debates han puesto de manifiesto muchas cuestiones que es necesario afrontar colectivamente. Desde nuestro punto de vista, cuando concluya la labor del actual grupo de trabajo, se necesitará un mecanismo permanente, inclusivo, flexible y adaptable de diálogo institucional periódico para continuar aplicando el marco de comportamiento responsable de los Estados y seguir facilitando el trabajo sobre diversas cuestiones, sobre la base de los resultados obtenidos por los sucesivos grupos de expertos gubernamentales y grupos de trabajo de composición abierta.

Acogemos con beneplácito y apoyamos el proyecto de resolución A/C.1/78/L.60, presentado por Francia, que proporciona una vía clara y transparente para que todos los Estados Miembros estudien la definición del

alcance, la estructura, el contenido y las modalidades del futuro mecanismo de una forma que complemente la labor del actual grupo de trabajo.

Por último, también insistimos en la importancia de la participación de múltiples partes interesadas, como la industria, el mundo académico y la sociedad civil, a la hora de hacer frente a los numerosos retos que plantea el ciberespacio. Los Gobiernos no pueden superar esos retos solos. Las partes interesadas no gubernamentales continúan aportando una perspectiva esencial y unos valiosos conocimientos técnicos a los debates internacionales sobre ciberseguridad, y seguimos celebrando y fomentando el diálogo con todas las partes interesadas pertinentes.

Sr. Ogasawara (Japón) (*habla en inglés*): Estamos siendo testigos de una creciente amenaza en el ciberespacio debido al aumento del número de incidentes relacionados con el uso malicioso de las tecnologías de la información y las comunicaciones (TIC), como los ataques con programas maliciosos, las ciberoperaciones contra infraestructuras críticas y el robo de criptomonedas. No hay fronteras en el ciberespacio. Por eso, la cooperación internacional es una necesidad ineludible para todos nosotros.

En ese contexto, el Japón concede gran importancia 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) en cuanto que plataforma inclusiva bajo los auspicios de las Naciones Unidas. Encomiamos el liderazgo del Presidente singapurense y de su equipo y acogemos con beneplácito la aprobación del segundo informe anual sobre los progresos realizados (véase A/78/265), que tuvo lugar en julio, así como los avances sustanciales que hemos logrado colectivamente, como la creación del directorio mundial de puntos de contacto.

Debemos promover el estado de derecho en el ciberespacio. El ámbito cibernético no es un espacio sin ley. El derecho internacional, incluida la Carta de las Naciones Unidas y el derecho internacional humanitario, es de aplicación en el ciberespacio. Dada la rapidez con la que cambia el entorno de las TIC, nuestra prioridad debería ser seguir entablando debates concretos sobre la forma en que se aplica el derecho internacional vigente. Esperamos con interés debates más concretos y sustanciales sobre este importante tema, también en las reuniones entre períodos de sesiones del Grupo de Trabajo de Composición Abierta.

La creación de capacidades es otro ámbito prioritario. El Japón ha colaborado estrechamente con la Asociación de Naciones de Asia Sudoriental, el Banco Mundial y otros asociados internacionales para potenciar las iniciativas regionales y mundiales de creación de capacidades en el campo de las TIC. La mesa redonda mundial sobre creación de capacidades en materia de seguridad de las TIC, prevista para mayo de 2024, brindará una excelente oportunidad para que todos los Estados Miembros intercambien opiniones sobre medidas prácticas de creación de capacidades y contará con una amplia participación de las partes interesadas pertinentes.

En cuanto al diálogo institucional periódico, agradecemos a los principales patrocinadores interregionales que hayan presentado el proyecto de resolución A/C.1/78/L.60, relativo al programa de acción propuesto por Francia. El Japón opina que esta propuesta de programa de acción flexible, inclusivo y de una sola vía puede garantizar una transición fluida a un nuevo mecanismo permanente orientado a la acción después de 2025, en el que podamos seguir desarrollando los logros del Grupo de Trabajo de Composición Abierta. Esperamos sinceramente que el proyecto de resolución, resultado de nuestros esfuerzos colectivos, sea aprobado con un amplio apoyo de los Estados Miembros.

Al ser único país que ha sufrido el uso de bombas atómicas durante una guerra, el Japón concede una importancia primordial a nuestras iniciativas en materia de desarme y a la educación para la no proliferación. En la Décima Conferencia de las Partes encargada del Examen del Tratado sobre la Prohibición de las Armas Nucleares, celebrada en agosto del año pasado, el Primer Ministro Kishida Fumio anunció la creación del Fondo de Líderes Juveniles en favor de un mundo sin armas nucleares, una de nuestras iniciativas enmarcadas en el Plan de Acción de Hiroshima que presentó en la Conferencia. El principal objetivo del programa es que futuros líderes procedentes tanto de Estados poseedores de armas nucleares como de Estados no poseedores visiten el Japón para conocer de primera mano la realidad del uso de las armas nucleares. Asimismo, pretende crear una red mundial de diversas cohortes internacionales de futuros líderes y otros actores clave de los Gobiernos, la sociedad civil, la educación, el mundo académico, los medios de comunicación, la industria y otros sectores.

Las tragedias de Hiroshima y Nagasaki no deben repetirse. La concienciación sobre las experiencias vividas en ambas ciudades tras el uso de armas nucleares debe ser el sustrato de nuestras iniciativas colectivas para construir un mundo sin este tipo de armas. El Japón considera que es su deber transmitir esas experiencias a las generaciones futuras y a través de las fronteras.

Sr. Van der Haegen (Suiza) (*habla en francés*): Las ciberoperaciones maliciosas llevadas a cabo por actores estatales y no estatales no han dejado de aumentar en los últimos años, tanto en tiempos de paz como en conflictos armados. La guerra contra Ucrania es un ejemplo de esa evolución, pero no el único. Está aumentando exponencialmente el número de ciberataques perpetrados por actores criminales contra empresas o particulares, contra infraestructuras críticas o directamente contra Estados, como demostró el ataque a Costa Rica. Esos retos solo pueden afrontarse respetando el marco acordado de comportamiento responsable de los Estados en el ciberespacio, que se ha confirmado y reafirmado en los informes de consenso de los grupos de expertos gubernamentales y los grupos de trabajo de composición abierta y ha recibido el respaldo de todos los Estados en la Asamblea General.

Suiza acoge con beneplácito la aprobación del segundo informe anual sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), pues constituye una base sólida para la futura labor del Grupo. En particular, celebramos la oportunidad de proseguir el debate sobre la aplicabilidad del derecho internacional, incluido el derecho internacional humanitario, en el ciberespacio. Además, acogemos con satisfacción que se haya hecho gran hincapié en la protección de las infraestructuras críticas y las infraestructuras críticas de información frente a las amenazas que plantean las TIC y que se haya recomendado la celebración de nuevos debates centrados en ese tema. Los últimos ciberincidentes y la situación geopolítica actual han demostrado que es de suma importancia proteger las infraestructuras críticas, en particular los establecimientos médicos y de salud. En ese contexto, Suiza opina que el Grupo de Trabajo debería centrarse en mejorar la comprensión, promoción y aplicación de las 11 normas voluntarias vigentes antes de formular otras nuevas.

Damos las gracias al Presidente del Grupo de Trabajo de Composición Abierta por presentar el proyecto de decisión A/C.1/78/L.13, que pone de relieve la aprobación del informe anual sobre los progresos realizados y el calendario de sesiones. Suiza apoya plenamente el proyecto de decisión y el enfoque procedimental y práctico. Asimismo, debemos recalcar que Suiza abriga importantes reservas sobre el proyecto de resolución A/C.1/78/L.11, presentado por la Federación de Rusia en relación con esa cuestión, ya que parece redundante y duplicaría el texto presentado por el Presidente del Grupo de Trabajo. Dicho proyecto también presenta problemas de fondo, en particular porque no se basa en una redacción consensuada, adopta un enfoque selectivo, no hace referencia al marco consensuado e intenta adaptar el mandato del Grupo de Trabajo, todo lo cual podría poner en tela de juicio los importantes avances logrados hasta la fecha en el grupo de trabajo actual. Dadas las circunstancias, Suiza no estaría en condiciones de apoyar el proyecto.

Suiza respalda los debates en curso en torno a la creación de un programa de acción de las Naciones Unidas sobre ciberseguridad en el seno del Grupo de Trabajo de Composición Abierta. Creemos que el programa de acción es la mejor opción para el nuevo diálogo institucional periódico una vez que el grupo de trabajo actual haya finalizado su labor en 2025. Por eso copatrocinamos el proyecto de resolución A/C.1/78/L.60, que ha sido presentado por Francia, Colombia, el Senegal y los Estados Unidos y contribuirá a impulsar esos debates.

Antes de concluir, me gustaría destacar los numerosos retos a los que nos enfrentamos debido al rápido avance del progreso tecnológico. Las repercusiones de la inteligencia artificial, así como de otros ámbitos de la ciencia y la tecnología, incluidas las ciencias de la vida, ocupan un lugar destacado en este período de sesiones de la Primera Comisión. De cara al futuro, estos avances deberían convertirse en una de las cuestiones en las que se centre la atención de la Comisión y deberíamos asegurarnos de que esta última apruebe una resolución que conecte las distintas vertientes del control de armamentos y el desarme con las tecnologías emergentes y examine las complejas sinergias de la ciencia y la tecnología y sus consecuencias para la paz y la seguridad internacionales.

Sra. Page (Reino Unido) (*habla en inglés*): El Reino Unido tiene el compromiso de promover un ciberespacio libre, abierto, pacífico y seguro que refuerce la seguridad colectiva y apoye el desarrollo mundial. Para ello es preciso que todos los Estados mantengan y cumplan los compromisos ya acordados en el seno de las Naciones Unidas, a saber, el marco de comportamiento responsable de los Estados en el ciberespacio y la aplicabilidad del derecho internacional vigente al ciberespacio, incluida la Carta de las Naciones Unidas en su totalidad.

A pesar de esos acuerdos, algunos Estados siguen actuando de forma irresponsable. Rusia ha utilizado ciberoperaciones como parte de una dilatada campaña de actividades hostiles y desestabilizadoras contra Ucrania. Esos ataques tienen repercusiones en el mundo real. Nos preocupa profundamente que el proyecto de

resolución presentado por Rusia intente reinterpretar estos acuerdos consensuados únicamente en pos de su propio interés y que, al hacerlo, socave el marco que hemos construido aquí juntos de forma colectiva.

Los patrones de ciberactividad maliciosa siguen evolucionando. Ha aumentado el número de ataques dirigidos contra las instituciones, procesos y valores democráticos del Reino Unido. Responderemos con contundencia a los actos hostiles contra nuestras infraestructuras nacionales críticas, entre otras cosas mediante el refuerzo de nuestras defensas a través de nuestro Equipo de Tareas de Defensa de la Democracia y las nuevas potestades previstas en la Ley de Seguridad Nacional.

Los efectos de los programas maliciosos secuestradores en las infraestructuras nacionales críticas pueden socavar la paz y la seguridad internacionales, por lo que acogemos con beneplácito las referencias a esta cuestión en el segundo informe anual sobre los progresos realizados (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Este año, el Reino Unido, en coordinación con asociados internacionales, sancionó a 18 ciberagentes dedicados a los programas maliciosos secuestradores. Seguiremos imponiendo costos a quienes nos perjudiquen y asegurándonos de que los actores maliciosos rinden cuentas.

Además, el Reino Unido está especialmente preocupado por el uso irresponsable de las cibercapacidades avanzadas disponibles en el mercado. Ese mercado en expansión abarca una amplia variedad de productos y servicios, entre los que se encuentran los programas espía comerciales. Dentro de un marco jurídico nacional e internacional que salvaguarde los derechos humanos, los servicios policiales pueden hacer un uso responsable de las herramientas cibernéticas comerciales para prevenir delitos graves y el terrorismo. Sin embargo, su uso indebido puede socavar los derechos humanos y amenazar nuestra seguridad colectiva y la estabilidad del ciberespacio. Se trata de un reto complejo que requiere la colaboración de diversos sectores. El Reino Unido y Francia están colaborando estrechamente para desarrollar una respuesta en la que participen múltiples partes interesadas y esperamos seguir cooperando con todos los Miembros en este sentido.

El Reino Unido reconoce la labor del Grupo de Trabajo de Composición Abierta, incluido el cuidadoso equilibrio alcanzado en su informe anual consensuado. Tenemos el compromiso de desempeñar el papel que nos corresponde al adoptar un comportamiento responsable en el ciberespacio y apoyar a otros para que lo hagan, lo que incluye destinar 32 millones de libras esterlinas a financiar actividades de creación de capacidades este año y participar en un debate constructivo para que los Estados lleguen a un mayor entendimiento sobre cómo se aplica al ciberespacio el derecho internacional, incluido el derecho internacional humanitario.

El Reino Unido apoya el proyecto de resolución A/C.1/78/L.60, presentado por Francia, con vistas a que, cuando concluya la labor Grupo de Trabajo de Composición Abierta en 2025, se cree un mecanismo permanente, orientado a la acción e inclusivo que se base en resultados consensuados, incluidos los alcanzados en el seno del Grupo de Trabajo. Tal mecanismo daría continuidad a los debates de los Estados sobre tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional y permitiría aplicar y seguir desarrollando el marco de las Naciones Unidas de comportamiento responsable en el ciberespacio.

Por último, quisiera referirme a los regímenes multilaterales de control de las exportaciones, 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. Nos preocupan los esfuerzos constantes de algunos Estados por socavar y desacreditar esos regímenes cruciales.

Sr. Ghorbanpour Najafabadi (República Islámica del Irán) (*habla en inglés*): La República Islámica del Irán expresa sus sinceras condolencias y su firme solidaridad a la imperecedera nación de Palestina. Condenamos enérgicamente las terribles atrocidades que ha cometido el régimen israelí en Gaza recientemente, que, hasta la fecha, han causado la muerte de más de 5.000 personas, de las cuales más del 60 % son mujeres y niños. El derramamiento de sangre y los bombardeos indiscriminados deben cesar de inmediato y la asistencia humanitaria debe prestarse sin trabas.

Mi delegación se adhiere a la declaración formulada por el representante de Indonesia en nombre del Movimiento de Países No Alineados.

En un contexto en el que los ciberataques están aumentando de forma significativa, en concreto, hasta en un 50 % en 2022, según se ha notificado, la República Islámica del Irán reitera enfáticamente su postura inamovible sobre la utilización del ciberespacio y el entorno de las tecnologías de la información y las comunicaciones. Estamos convencidos de que estos activos de inestimable valor, que pueden asimilarse a un patrimonio

común de la humanidad, deben aprovecharse exclusivamente con fines pacíficos, y es indispensable que los Estados colaboren y respeten escrupulosamente el derecho internacional pertinente.

En consonancia con ese punto de vista de principios, el Irán ha tomado parte activa en negociaciones intergubernamentales bajo los auspicios de las Naciones Unidas. Participamos guiados por nuestra firme determinación de salvaguardar los derechos de todas las partes afectadas. De conformidad con la resolución fundacional 75/240, el principio rector de la metodología que sigue 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) en sus actividades es el consenso, loque implica respetar las perspectivas de todos y cada uno de los Estados Miembros. Debe mantenerse y fomentarse la esencia del consenso, dado que es la base de las deliberaciones del Grupo.

La aprobación del segundo informe anual del Grupo de Trabajo de Composición Abierta (véase A/78/265), acompañado de un conjunto completo de declaraciones que aclaran las posiciones de los Estados Miembros, incluido el Irán, nos indica que los avances posteriores y el éxito final del Grupo de Trabajo dependen sobre todo de que se alcance un consenso sustantivo. Como hemos subrayado anteriormente, no debe darse por sentado que los Estados Miembros participarán voluntariamente en el consenso o decidirán no obstaculizarlo. Por consiguiente, nos corresponde examinar e integrar con diligencia los puntos de vista y las contribuciones de todos los Estados Miembros en los resultados del Grupo de Trabajo.

En ese sentido, es esencial que revisemos los documentos anteriores del Grupo de Trabajo de Composición Abierta, incluido el resumen de la Presidencia y el informe anual de 2021 sobre los progresos realizados (véase A/77/275), en los que se señalaron en gran medida las cuestiones pendientes. Esos documentos deben servir de base para entablar unas negociaciones constructivas y acercar puntos de vista divergentes. Deseamos hacer hincapié en que, si aspiramos a que el Grupo de Trabajo sea eficaz como medida de fomento de la confianza, debemos prestar atención a las preocupaciones e intereses de todos los Estados Miembros. De lo contrario, se debilitará la confianza esencial de la que goza el Grupo de Trabajo y que tiene un valor incalculable para su misión.

A la luz de la evolución de las situaciones, es crucial reconocer que ciertos Estados, en especial los Estados Unidos, no solo han acometido la militarización del ciberespacio, sino que también han llevado a cabo múltiples ciberataques. En particular, el régimen israelí ha lanzado una serie de ciberataques contra el Irán, entre los que destaca el tristemente célebre Stuxnet. Condenamos sin reservas esas acciones e imploramos a la comunidad internacional que haga que sus autores rindan cuentas. Es lamentable que recientemente se haya implicado al Irán de forma falsa y sin fundamento en un supuesto ciberataque. Rechazamos categóricamente las afirmaciones infundadas que se basan en mentiras y advertimos sobre sus riesgos.

Sr. Getahun (Etiopía) (*habla en inglés*): Mi delegación se adhiere a las declaraciones formuladas en nombre del Movimiento de Países No Alineados y del Grupo de los Estados de África.

Las tecnologías de la información y las comunicaciones (TIC) hacen contribuciones enormes y bien reconocidas a la paz, el crecimiento y el desarrollo es enorme y reconocida. Para que esas contribuciones tengan repercusiones positivas y duraderas, es absolutamente imprescindible defender los principios de comportamiento responsable de los Estados en cuanto al uso de las TIC solo con fines pacíficos. Las TIC cada vez se usan más en la industria, pero también están aumentando las amenazas derivadas de su empleo con fines delictivos. Consideramos que esto va en detrimento de nuestras iniciativas colectivas dirigidas a utilizar esas tecnologías para garantizar la paz y la estabilidad y lograr nuestras estrategias, por lo que debemos dar una respuesta oportuna y rápida a la situación.

Etiopía colabora con otros para favorecer 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 (2021-2025), que es el único mecanismo inclusivo en la actualidad. Para que pueda llevar a cabo su mandato con éxito, es fundamental la participación igualitaria de todos los Estados en resultados consensuados. A este respecto, Etiopía es de la opinión de que el mejor enfoque es un proceso dirigido por los Estados que dependa de la Primera Comisión. En una línea similar, consideramos que las plataformas regionales también son importantes para alcanzar el consenso necesario. Por lo tanto, compartimos el punto de vista de que la evolución del uso del ciberespacio en el contexto de la seguridad internacional podría debatirse mediante un planteamiento inductivo que parta de los niveles subregional y continental hasta llegar al nivel mundial, lo que contribuiría a fomentar la confianza de todos.

Hacemos hincapié en que los países en desarrollo necesitan programas de creación de capacidades sobre cuestiones técnicas, jurídicas y relativas a las

TIC que resulten pertinentes para el uso pacífico del ciberespacio. En ese sentido, es fundamental que el sistema de las Naciones Unidas y las organizaciones regionales desempeñen un papel clave para prestar apoyo a la creación de capacidades con el fin de que los países en desarrollo puedan mejorar sus capacidades a todos los niveles y beneficiarse del uso de las TIC para alcanzar sus objetivos de desarrollo. Este apoyo a la creación de capacidades también es decisivo para las medidas de fomento de la confianza, con miras a reforzar la estabilidad y la seguridad del ciberespacio.

Etiopía está haciendo todo lo posible para usar las capacidades de las TIC con el fin de potenciar cambios económicos y sociales rápidos y construir una sociedad más próspera. Hemos formulado políticas y legislación con el objetivo de promover y aprovechar la utilización de las TIC y hemos avanzado en la construcción institucional para valernos del potencial de las TIC y cumplir nuestros objetivos de desarrollo. Etiopía tiene el compromiso de contribuir a la puesta en práctica de la agenda del pacto digital global y de beneficiarse de ella para reforzar la cooperación digital mediante un proceso abierto e inclusivo. Apoyamos plenamente la promoción de soluciones digitales mediante el acceso y el uso de bienes públicos digitales para alcanzar los Objetivos de Desarrollo Sostenible e intentar reducir la brecha digital.

Al tratar de desarrollar la industria de las TIC y resolver con eficacia los problemas de carácter cibernético, nos hemos topado con varios retos, como la falta de recursos financieros y un bajo nivel de competencias digitales y competencias para incorporar bienes públicos digitales. Por tanto, en nuestro empeño por utilizar las TIC de forma eficaz y sostenible para hacer frente a nuestros polifacéticos retos de desarrollo, pedimos a la comunidad internacional un apoyo impulsado por la demanda que nos permita hacer frente a los obstáculos que afectan al uso de las TIC.

En conclusión, Etiopía recalca la importancia de garantizar la paz, la seguridad y la estabilidad del entorno de las TIC, y reitera su firme determinación de colaborar con todos para lograr ese objetivo.

Sr. Berard Cadieux (Canadá) (*habla en inglés*): El Canadá desea abordar dos cuestiones relacionadas con la paz y la seguridad internacionales: el comportamiento responsable de los Estados en el ciberespacio y la importancia de que la aplicación de una perspectiva de género a las cuestiones de desarme sea la norma y no una excepción.

El Canadá acoge con beneplácito el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC), elaborado en virtud del informe de consenso (véase A/76/135) 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 en el seno del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), así como en sus informes anuales de 2022 y 2023 sobre los progresos realizados (véanse A/77/275 y A/78/265, respectivamente).

El marco es crucial para la paz y la seguridad y para alcanzar un entendimiento sobre cómo deben comportarse los Estados en el ciberespacio. Por ello, nos preocupa que el cuestionamiento de la solidez del marco por parte de un pequeño número de Estados, incluidos algunos que desempeñaron un papel clave en su formulación. Recordamos que en virtud de los informes del Grupo de Expertos Gubernamentales de 2015 (véase A/70/174) y 2021, la comunidad internacional acordó por consenso un conjunto de amplias normas voluntarias sobre el comportamiento responsable de los Estados en el ciberespacio, y los Estados también convinieron en que el derecho internacional es de aplicación en el ciberespacio. Esas normas y el derecho internacional son medios adecuados para orientar a los Estados sobre lo que pueden y no pueden hacer en el ciberespacio. Acogemos con beneplácito los debates en curso en el Grupo de Trabajo de Composición Abierta sobre la implementación de normas y sobre cómo se aplica el derecho internacional.

Las medidas prácticas de fomento de la confianza y la creación de capacidades son otros dos elementos clave del marco de comportamiento responsable de los Estados en el ciberespacio. Desde 2015, el Canadá ha destinado más de 30 millones de dólares a proyectos de creación de cibercapacidades en todo el mundo y colabora con diversas organizaciones para promover una Internet abierta y segura. Reconocemos que es necesario seguir trabajando y esperamos con interés profundizar en nuestro debate en los próximos años.

(*continúa en francés*)

El Canadá opina que es preciso que los miembros de las Naciones Unidas creen un foro permanente para fomentar debates pragmáticos y orientados a la acción cuando concluya el actual mandato del Grupo de Trabajo de Composición Abierta. Por ello, el Canadá copatrocina la propuesta de programa de acción en la presente sesión de la Primera Comisión. El programa de acción es el mejor foro para realizar avances concretos en la

aplicación del marco normativo acordado, por ejemplo mediante el apoyo a actividades específicas de creación de capacidades. Además, proporcionará un foro inclusivo en el que todos los Estados Miembros puedan centrarse en esas y todas las demás cuestiones relacionadas con la ciberseguridad, al tiempo que se benefician de los conocimientos técnicos del sector privado, la sociedad civil y el mundo académico.

En aras de la inclusividad, el Canadá reafirma que, para velar por una Internet abierta, es necesario invertir en equidad de género y comprender las consecuencias que presentan los problemas de ciberseguridad en función del género. Reconocemos la labor realizada por el Grupo de Trabajo de Composición Abierta para poner de relieve las diversas contribuciones de las mujeres, la publicación de documentación en el portal del Grupo de Trabajo y el actual programa de becas Women in Cyber. Esperamos con interés aprovechar ese programa en las futuras iniciativas de las Naciones Unidas relacionadas con el ciberespacio.

Las perspectivas de género no solo son vitales en el ciberespacio, sino que también son clave para nuestra labor en todos los mecanismos de desarme. La incorporación de este tipo de perspectiva facilita la creación de iniciativas eficaces y duraderas que ayudan a hacer frente a las amenazas para la seguridad más acuciantes en el mundo. Para ello, una posible estrategia es recopilar y compartir datos sobre los efectos de las armas desglosados por edad y género. El Canadá se siente alentado por la mejora de la representación de género en los foros de las Naciones Unidas, incluida esta Comisión. Sin embargo, el desequilibrio de género sigue existiendo, de manera que faltan voces y perspectivas esenciales en los debates y se trata de voces y perspectivas necesarias para elaborar políticas y programas eficaces de no proliferación y desarme.

En conclusión, cerrar la brecha de género es un requisito previo para crear un mundo más inclusivo, pacífico y próspero. Por consiguiente, el Canadá mantiene su firme determinación de colaborar con todas las partes interesadas para fomentar que se tengan en cuenta las consideraciones de género en todos los aspectos de la seguridad internacional.

Sr. Shen Jian (China) (*habla en chino*): El panorama internacional actual en lo que respecta al ciberespacio es complicado, presenta una situación grave y se caracteriza por la formación de bloques, la militarización y la fragmentación. Este año se cumple el 25º aniversario del inicio del proceso de seguridad de la información en las Naciones Unidas. Desde los grupos de expertos gubernamentales hasta llegar al 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, la seguridad de la información en las Naciones Unidas partió de cero y amplió su escala, de manera que se han conseguido logros significativos, entre los que se encuentran la confirmación de los principios de la soberanía en el ciberespacio y el mantenimiento de la paz en el ciberespacio; la elaboración de 11 normas de comportamiento responsable de los Estados en el ciberespacio; el cumplimiento y la aplicación del marco de comportamiento responsable de los Estados; y el recién creado directorio mundial e intergubernamental de puntos de contacto. Estos logros que tanto costó conseguir han desempeñado un papel importante en el mantenimiento de la paz y la estabilidad en el ciberespacio.

Las experiencias positivas de los últimos 25 años han demostrado que la única manera de afrontar los retos y alcanzar el desarrollo conjunto y la prosperidad común es defender la paz, la cooperación y la inclusión, al tiempo que se rechaza el conflicto, la confrontación y la exclusividad. Mantener la naturaleza pacífica del ciberespacio es nuestra única opción. Deberíamos situar la paz y la cooperación en el centro de nuestras políticas y demostrar nuestra voluntad de promover la paz y el desarrollo mediante la cooperación, rechazar los ciberconflictos y la ciberguerra, y facilitar que el ciberespacio sea un lugar lleno de oportunidades digitales en lugar de un nuevo campo de batalla para la rivalidad entre grandes Potencias.

La gobernanza mundial del ciberespacio requiere que todos los países participen de manera igualitaria y adopten decisiones conjuntas. Tenemos que defender firmemente que las Naciones Unidas sean un elemento central en materia de seguridad de la información, respetar la autoridad del Grupo de Trabajo de Composición Abierta como único proceso dedicado a la seguridad de la información bajo los auspicios de las Naciones Unidas, y aunar esfuerzos para alcanzar acuerdos a largo plazo sobre el futuro marco institucional de la seguridad de la información.

En la era digital, tenemos que tomar la iniciativa para hacer frente a los nuevos retos que plantea la seguridad de la información y afanarnos por resolver los problemas reales y urgentes que afectan a todos los países. El segundo informe anual sobre los progresos realizados del Grupo de Trabajo de Composición Abierta reconoce que

> “[t]eniendo en cuenta el crecimiento y la agregación de datos asociados a las tecnologías nuevas y emergentes, los Estados también señalaron la creciente importancia de la protección y la seguridad de los datos” (*A/78/265, anexo, párr. 17*).

China ha propuesto una iniciativa global sobre la seguridad de los datos que ofrece una solución eficaz a la seguridad de los datos a escala mundial y podría servir de base para nuestros futuros debates. Frente a los riesgos y desafíos que plantea el ciberespacio, China desea colaborar con todas las partes, mantener la solidaridad y la cooperación y realizar actividades conjuntas para edificar una comunidad con un futuro compartido en el ciberespacio.

La inteligencia artificial (IA) es un nuevo ámbito del desarrollo humano que ha creado enormes oportunidades para el desarrollo socioeconómico y al que también acompañan riesgos y retos imprevisibles. La gobernanza de la IA, una tarea común a la que se enfrentan todos los países del mundo, afecta al futuro de la humanidad. China acaba de poner en marcha la Iniciativa Mundial de Gobernanza de la IA, a través de la cual pide a todos los países que mejoren los intercambios y la cooperación y colaboren para prevenir los riesgos. Deberíamos desarrollar marcos de gobernanza sobre la base de un amplio consenso, para que las tecnologías de IA sean más seguras, fiables, controlables y equitativas. China ya había publicado también documentos de posición sobre la regulación de las aplicaciones militares de la IA y la consolidación de la gobernanza ética de la IA.

China aboga por un enfoque centrado en las personas y por conceptos como la IA para el bien, y prioriza el desarrollo y la ética. Consideramos que la IA debe desarrollarse siempre de forma beneficiosa para la civilización humana. Debemos trabajar juntos para prevenir el uso malicioso y el abuso de las tecnologías de IA por parte de terroristas, extremistas y grupos delictivos organizados transnacionales, y luchar contra ellos. Todos los países, especialmente los grandes, deben adoptar una actitud prudente y responsable ante la investigación, el desarrollo y la aplicación de las tecnologías de IA en el ámbito militar y abstenerse de pretender conseguir ventajas militares absolutas y de socavar el equilibrio estratégico y la estabilidad mundiales.

China aboga por la aplicación de una regulación por niveles y categorías con el fin de garantizar que los sistemas de armas pertinentes estén siempre bajo control humano. Habida cuenta del doble uso que caracteriza a la tecnología de la IA, al reforzar la regulación y la gobernanza, debemos garantizar los derechos de todos los países a los usos pacíficos. China se opone a trazar líneas ideológicas o formar grupos exclusivos para dificultar que otros países desarrollen la IA. También nos oponemos a que se erijan barreras y se interrumpa la cadena mundial de suministro de IA mediante monopolios tecnológicos y medidas coercitivas unilaterales.

China apoya activamente los debates para crear una institución internacional que gobierne la IA en el marco de las Naciones Unidas y coordine los esfuerzos para abordar las principales cuestiones relativas al desarrollo, la seguridad y la gobernanza internacionales de la IA.

Sr. Christoglou (Grecia) (*habla en inglés*): Grecia hace suya la declaración formulada por el observador de la Unión Europea y desea añadir algunas observaciones a título nacional.

En los últimos años, se han intensificado los comportamientos maliciosos en el ciberespacio, entre los que se encuentra un drástico aumento de los ciberataques dirigidos contra las infraestructuras críticas, las cadenas de suministro y la propiedad intelectual, así como un incremento de los ataques con programas maliciosos secuestradores contra empresas, organizaciones y ciudadanos. Además, los ciberataques han evolucionado en su faceta de instrumento en los conflictos armados hasta convertirse en una de las amenazas más importantes de nuestro tiempo para la paz y la seguridad. Ante esta situación, Grecia apoya firmemente la labor llevada a cabo en las Naciones Unidas, que se ha centrado especialmente en la aplicación de la legislación nacional en el ciberespacio y ha permitido establecer tanto normas de comportamiento responsable como medidas de fomento de la confianza. Aprovechar esa labor contribuye a impulsar la paz y la estabilidad en el ciberespacio y beneficia a todos los países.

Grecia también acoge con beneplácito el informe anual de 2023 (véase A/78/265) del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), en particular la recomendación en la que se pide a los Estados que debatan sobre el alcance, la estructura y el contenido de un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio. Estamos convencidos de que la creación de un mecanismo permanente, inclusivo y orientado a la acción proporcionaría una base sólida para dar continuidad a los dos aspectos más importantes de nuestra labor: la aplicación y el ulterior desarrollo del marco de comportamiento responsable de los Estados en el ciberespacio.

Grecia tiene la firme determinación de proseguir los debates en las Naciones Unidas sobre cuestiones de ciberseguridad, y reafirmamos nuestra voluntad de hacer una contribución positiva encaminada a lograr avances constructivos, como demuestra nuestra participación activa en el reciente proceso del Grupo de Trabajo de Composición Abierta desde su inicio.

Se levanta la sesión a las 12.55 horas.