Naciones Unidas S/PV.9662

Consejo de Seguridad

Septuagésimo noveno año

Provisional

9662ª sesión

Jueves 20 de junio de 2024, a las 10.00 horas
Nueva York

Presidencia:	Sr. Cho Tae-yul/Sr. Hwang	(República de Corea)
Miembros:	Argelia	Sr. Bendjama
	China	Sr. Fu Cong
	Ecuador	Sr. De La Gasca
	Eslovenia	Sr. Žbogar
	Estados Unidos de América	Sra. Thomas-Greenfield
	Federación de Rusia	Sr. Nebenzia
	Francia	Sr. De Rivière
	Guyana	Sr. Persaud
	Japón	Sr. Yamazaki
	Malta	Sra. Frazier
	Mozambique	Sr. Afonso
	Reino Unido de Gran Bretaña e Irlanda del Norte	Dame Barbara Woodward
	Sierra Leona	Sr. Kanu
	Suiza	Sra. Chanda

Orden del día

Mantenimiento de la paz y la seguridad internacionales

Hacer frente a las amenazas cambiantes en el ciberespacio

Carta de fecha 7 de junio de 2024 dirigida a la Presidencia del Consejo de Seguridad por el Representante Permanente de la República de Corea ante las Naciones Unidas (S/2024/446)

Se declara abierta la sesión a las 10.00 horas.

Aprobación del orden del día

Queda aprobado el orden del día.

Mantenimiento de la paz y la seguridad internacionales

Hacer frente a las amenazas cambiantes en el ciberespacio

Carta de fecha 7 de junio de 2024 dirigida a la Presidencia del Consejo de Seguridad por el Representante Permanente de la República de Corea ante las Naciones Unidas (S/2024/446)

El Presidente (*habla en inglés*): Quisiera dar una calurosa bienvenida al Secretario General y a los distinguidos Ministros y demás representantes de alto nivel presentes en el Salón. Su presencia hoy aquí pone de relieve la importancia del tema que abordaremos.

De conformidad con el artículo 37 del Reglamento Provisional del Consejo, invito a participar en esta sesión a los representantes de Albania, la Argentina, Australia, Austria, Bahrein, Bangladesh, Bélgica, el Brasil, Bulgaria, Camboya, Chile, Costa Rica, Croacia, Cuba, Chequia, Egipto, El Salvador, Estonia, Gambia, Georgia, Alemania, Ghana, Grecia, Guatemala, la India, Indonesia, la República Islámica del Irán, Israel, Italia, Kazajstán, Kiribati, Letonia, Liechtenstein, Marruecos, Nepal, Noruega, el Pakistán, Panamá, Filipinas, Polonia, Portugal, Rumanía, la Arabia Saudita, Singapur, España, Türkiye, Ucrania, los Emiratos Árabes Unidos, el Uruguay y Viet Nam.

De conformidad con el artículo 39 del Reglamento Provisional del Consejo, invito a participar en esta sesión a los siguientes exponentes: el Director General de CyberPeace Institute, Sr. Stéphane Duguin, y la Sra. Nnenna Ifeanyi-Ajufo, Profesora de Derecho y Tecnología de la Universidad Leeds Beckett.

De conformidad con el artículo 39 del Reglamento Provisional del Consejo, invito asimismo a participar en esta sesión a la Encargada de Negocios Interina de la Delegación de la Unión Europea ante las Naciones Unidas, Excma. Sra. Hedda Samson; la Representante Especial de INTERPOL ante las Naciones Unidas, Sra. Roraima Ana Andriani; y la Observadora Permanente y Jefa de la Delegación del Comité Internacional de la Cruz Roja ante las Naciones Unidas, Sra. Laetitia Courtois.

El Consejo de Seguridad comenzará ahora el examen del tema que figura en el orden del día.

Deseo señalar a la atención de los miembros del Consejo el documento S/2024/446, que contiene el texto de una carta de fecha 7 de junio de 2024 dirigida a la Presidencia del Consejo de Seguridad por el Representante Permanente de la República de Corea ante las Naciones Unidas, por la que se transmite una nota conceptual sobre el tema objeto de examen.

Doy ahora la palabra al Secretario General, Excmo. Sr. António Guterres.

El Secretario General (*habla en inglés*): Doy las gracias a la República de Corea por haber convocado este debate de alto nivel sobre una cuestión que nos afecta a todos: la paz y la seguridad en el ciberespacio.

Los avances en las tecnologías digitales se suceden a velocidad de vértigo: desde las tecnologías de la información y la comunicación y la computación en la nube hasta la tecnología de cadenas de bloques, las redes 5G, las tecnologías cuánticas y muchas otras. Los avances digitales están revolucionando las economías y las sociedades. Están uniendo a las personas; diseminando información, noticias, conocimientos y formación simplemente con tocar una pantalla o pulsar las teclas de un ratón; facilitando a los ciudadanos el acceso a los servicios e instituciones gubernamentales; y potenciando las economías, el comercio y la inclusión financiera.

No obstante, la propia calidad de la conectividad instantánea y fluida que aporta los enormes beneficios del ciberespacio también puede dejar a personas, instituciones y países enteros en una situación de grave vulnerabilidad. Y los peligros de convertir en armas las tecnologías digitales aumentan cada año. El ciberespacio ha abierto las puertas de par en par. Cualquiera puede entrar, y muchos lo hacen. La actividad maliciosa en el ciberespacio va en aumento, tanto la que realizan agentes estatales y no estatales como la de auténticos criminales.

Los incidentes graves de ciberseguridad son alarmantemente frecuentes. De la vulneración de servicios públicos esenciales como la sanidad, la banca y las telecomunicaciones; pasando por la actividad ilícita incesante, particularmente la que acometen organizaciones delictivas y los llamados cibermercenarios; a una legión de comerciantes del odio que emponzoñan la autopista de la información con miedo y división; y a la creciente utilización del ciberespacio como un arma más en los conflictos armados en curso, en el marco de la cual los llamados hacktivistas civiles están entrando en la contienda y, en muchos casos, están difuminando la línea que separa a los combatientes de los civiles. Además, la

creciente integración de las herramientas digitales con los sistemas de armas, incluidos los sistemas autónomos, presenta nuevas vulnerabilidades.

Al mismo tiempo, el uso indebido de la tecnología digital es cada vez más sofisticado y sigiloso. Proliferan los programas maliciosos, así como los programas maliciosos de borrado de datos y los troyanos. Las ciberoperaciones habilitadas por la inteligencia artificial están multiplicando la amenaza, y mediante la computación cuántica sería posible desbaratar sistemas enteros debido a su capacidad para desactivar el cifrado. Se están explotando las vulnerabilidades de los programas informáticos, e incluso se venden capacidades de ciberintrusión a través de Internet. Los hackers están atacando activamente las cadenas de suministro de las compañías, lo que acarrea efectos graves, perturbadores y en cascada. El *ransomware* es un grave ejemplo, una amenaza colosal para las instituciones públicas y privadas y la infraestructura crítica de la que dependen las personas. Según algunas estimaciones, los pagos de rescate realizados a consecuencia del *ransomware* alcanzaron un total de 1.100 millones de dólares en 2023.

Sin embargo, más allá de los costos financieros, importan los costos para nuestra paz, seguridad y estabilidad comunes, tanto dentro de los países como entre ellos. Las actividades malintencionadas que socavan las instituciones públicas, los procesos electorales y la integridad en línea erosionan la confianza, atizan las tensiones e incluso siembran la semilla de la violencia y el conflicto.

La tecnología digital brinda una oportunidad increíble para crear un futuro más justo, igualitario, sostenible y pacífico para todos. Sin embargo, los avances deben ir encaminados hacia el bien. En la Nueva Agenda de Paz, la prevención es un elemento central de todas las iniciativas de paz. En la Agenda se exhorta a que se desarrollen marcos sólidos acordes con el derecho internacional, los derechos humanos y la Carta de las Naciones Unidas, y a que todos los Estados centren sus esfuerzos en prevenir la extensión y la escalada de los conflictos en el ciberespacio y a través de él. Como se refleja en la nueva visión sobre el estado de derecho, este debe existir en el ámbito digital del mismo modo que existe en el mundo físico.

También acojo con satisfacción la determinación de la Asamblea General de actuar en ese ámbito. En ella se incluye el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. Los Estados se están basando en el marco normativo respaldado universalmente para el comportamiento responsable de los Estados en el ciberespacio, y están estudiando activamente la aplicabilidad del derecho internacional a las actividades de los Estados en ese ámbito. Además, bajo los auspicios de la Asamblea General, los Estados Miembros están trabajando para alcanzar en los próximos meses un consenso sobre un nuevo tratado contra la ciberdelincuencia, que debería intensificar la cooperación y, a la vez, proteger los derechos humanos en línea. Pero dados los vínculos claros y crecientes entre el ciberespacio y la paz y la seguridad mundiales, el Consejo también puede desempeñar un papel crucial integrando las consideraciones cibernéticas en su flujo de trabajo actual y sus resoluciones.

Esta es solo la segunda vez que el Consejo de Seguridad celebra una sesión oficial sobre este asunto. Sin embargo, muchas de las cuestiones que se examinan en torno a esta mesa se ven afectadas por el ciberespacio y están vinculadas a este, tales como la protección de los civiles en los conflictos armados, las operaciones de paz, la lucha contra el terrorismo y las operaciones humanitarias. La integración del tema del ciberespacio en las deliberaciones del Consejo sería útil para sentar las bases que permitan dar respuestas más eficaces a esta problemática tan importante.

(*continúa en francés*)

Para garantizar la paz y la seguridad en el mundo físico, necesitamos nuevos enfoques de la paz y la seguridad en el mundo digital. La Cumbre del Futuro prevista para septiembre será una oportunidad vital para mejorar la cooperación en torno a los desafíos mundiales esenciales y revitalizar el sistema multilateral. El Pacto que surgirá de la Cumbre representa una oportunidad especial para apoyar el mantenimiento de la paz y la seguridad internacionales en el ciberespacio. Entre otras prioridades, el capítulo 2 del Pacto pretende reafirmar el consenso mundial sobre la protección de la infraestructura crítica frente a las prácticas digitales perjudiciales y reforzar la rendición de cuentas de cada persona en relación con la tecnología basada en datos, entre ellas la inteligencia artificial. Mientras tanto, mi Órgano Asesor de Alto Nivel sobre Inteligencia Artificial está ultimando su informe sobre la manera en que podemos controlar la IA en favor de la humanidad, abordando al mismo tiempo sus riesgos e incertidumbre. Estoy deseoso de trabajar con el Consejo, la Asamblea General y todos los Estados Miembros para garantizar que la tecnología se emplee como es debido: para trabajar por el progreso y la seguridad de todas las personas y del planeta que compartimos.

El Presidente (*habla en inglés*): Doy las gracias al Secretario General por su exposición informativa.

Tiene ahora la palabra el Sr. Duguin.

Sr. Duguin (*habla en inglés*): Es un honor dirigirme hoy al Consejo de Seguridad para tratar un asunto de vital importancia: cómo hacer frente a la evolución de las amenazas en el ciberespacio. Como Director General de CyberPeace Institute, una organización no gubernamental independiente y neutral con sede en Suiza, hablo por experiencia, ya que nuestro instituto ofrece servicios gratuitos de ciberseguridad a los más vulnerables, es decir, a organizaciones sin fines de lucro; vigila a los agentes generadores de amenazas; detecta y analiza amenazas; y aboga por el respeto de las leyes y normas en el ciberespacio.

Al analizar la evolución de la amenaza, me gustaría tratar el efecto acumulativo de las disrupciones graves en el panorama de riesgos, que en conjunto tienen un efecto directo en el mantenimiento de la paz y la seguridad internacionales. Abordaré varios temas: la proliferación de agentes generadores de amenazas y los ataques cada vez más frecuentes contra la infraestructura crítica; el estado actual de la amenaza, sobre todo a raíz de la convergencia de ciberataques y desinformación, y el uso de ciberataques para eludir las sanciones internacionales; y la evolución de la amenaza de aquí en adelante, en vista del riesgo singular que supone la inteligencia artificial (IA) para la ciberseguridad. Estos cambios suponen grandes desafíos para la paz y la seguridad internacionales, sobre todo porque dificultan la atribución, es decir, el proceso de identificación del autor o la fuente de un ciberataque o una operación.

Empezaré por la proliferación de agentes generadores de amenazas. Desde 2022, cuando la Federación de Rusia invadió Ucrania, CyberPeace Institute viene documentando una proliferación de agentes generadores de amenazas alineados con ambas partes beligerantes. La guerra ya no es territorio exclusivo de los Estados. Diversos actores no estatales —grupos delictivos, colectivos de hacktivistas que tienen motivaciones geopolíticas y otros civiles— participan en ciberataques y operaciones en el contexto de los conflictos armados. Persiguen cuatro objetivos: destruir la infraestructura, perturbar el funcionamiento normal de los servicios esenciales, sincronizar la desinformación y los ciberataques, y robar datos para utilizarlos como arma mediante la infiltración y el espionaje. En ese contexto, en CyberPeace Institute hemos rastreado más de 3.000 campañas de ciberataques lanzadas por 127 agentes generadores de amenazas, que afectan a 56 países y atacan 24 sectores de la infraestructura crítica. El daño causado por esos ciberataques se ha hecho sentir mucho más allá de las fronteras de los países en conflicto, ya que cerca del 70 % de todos los ciberataques afectan a organizaciones de países no beligerantes. Esas cifras están disponibles públicamente en nuestra plataforma llamada “Ciberataques en tiempos de conflicto”. La proliferación de ataques que he descrito plantea un interrogante sobre la reducción de las tensiones en el contexto de un posible cese de hostilidades. En esas circunstancias, ¿cómo se puede controlar a esos 127 agentes generadores de amenazas u obligarlos a poner fin a sus actividades maliciosas?

Esa proliferación repercute directamente en la seguridad de la infraestructura crítica. Quisiera presentar dos ejemplos. En febrero de 2022, un ciberataque con un programa malicioso borrador llamado AcidRain arremetió contra el acceso a Internet de banda ancha por satélite en Ucrania. El impacto se dejó sentir más allá de las fronteras de Ucrania. Se vio afectado el funcionamiento de turbinas eólicas en toda Europa, una importante empresa energética alemana perdió acceso a la vigilancia a distancia de más de 5.800 turbinas de ese tipo, y miles de abonados a servicios de Internet por satélite en Alemania, Francia, Hungría, Grecia, Italia y Polonia se vieron perjudicados. Estas repercusiones no solo se sienten en tiempos de conflicto armado. Durante la pandemia de enfermedad por coronavirus (COVID-19), CyberPeace Institute observó 500 ciberataques contra establecimientos de salud durante los dos años que duró la pandemia. Esos 500 ciberataques no son ni siquiera la punta del iceberg: representan un pequeño cubo de hielo en la punta del iceberg. Solamente esos 500 ataques perturbaron la atención médica en 43 países, dieron lugar al robo de datos de 20 millones de pacientes y supusieron una disrupción acumulativa de cinco años en el acceso a la asistencia médica. Eso equivale a una acumulación de cinco años de desvíos de ambulancias, cancelaciones de citas y acceso reducido de los pacientes a la atención médica.

Otro aspecto de la evolución de la amenaza es el uso de ciberataques para eludir sanciones internacionales y financiar actividades ilegales. Por ejemplo, varios agentes de la sociedad civil, organizaciones de ciberseguridad y Estados han analizado las actividades de dos presuntos grupos delictivos, Kimsuky y Lazarus Group, cuyas tácticas, herramientas, procesos e intenciones se han atribuido a la República Popular Democrática de Corea. Esos grupos delictivos coordinan ciberataques globales de todo tipo, que a veces utilizan *ransomware* o se dirigen contra la cadena de suministro, bolsas de

criptomonedas o instituciones financieras. Además de generar daños directos o primarios significativos, esos ataques son un vector para eludir las sanciones internacionales. Según estimaciones recientes, Lazarus Group y Kimsuky han ganado más de 3.000 millones de dólares con ese tipo de ataques. Esa escalada crea un daño ingente. El ataque WannaCry de mayo de 2017, que afectó a más de un cuarto de millón de computadoras en más de 150 países en menos de 24 horas, causó importantes trastornos y tuvo un impacto generalizado en los sectores sanitario, financiero y del transporte.

Para concluir sobre la evolución de las amenazas, resulta importante prever nuevos riesgos, como los que suponen la informática cuántica para la criptografía, que ya se ha mencionado, y la IA generativa para los modelos delictivos. Desde la llegada de la IA generativa y los grandes modelos lingüísticos, los actores maliciosos vienen utilizando la IA simplemente para aumentar su capacidad. Hoy en día, la IA se utiliza para ampliar los procesos existentes en lo que se conoce como cadena de ciberataque, que es el proceso estándar por el que debe pasar cualquier atacante para perpetrar un ciberataque. El uso de la IA ahorra tiempo en el reconocimiento de objetivos, automatiza las búsquedas de los puntos vulnerables y aumenta la capacidad de producción del phishing, por ejemplo. Ese es solo el primer paso, pues ya hay grupos que están experimentando con el uso de IA generativa para automatizar diferentes partes de los ciberataques. Eso supone un riesgo inaceptable. Si esos experimentos resultan exitosos, se podría alcanzar un nivel tan alto de automatización en toda la cadena de ciberataque que un actor malicioso podría desatar, de forma voluntaria o accidental, un ciberataque autónomo.

Dada la convergencia de varias disrupciones acumulativas —la proliferación de amenazas, el nuevo *modus operandi* específico para atacar la infraestructura crítica o eludir las sanciones y los sucesos futuros vinculados a la nueva tecnología de IA—, resulta difícil responder con una estrategia coherente. Aun así, se pueden tomar varias medidas, y con esto concluyo.

Podemos llevar a la práctica las leyes, las normas y las sanciones, sobre todo mediante la documentación transparente de las violaciones y un enfoque orientado al futuro para prevenir el uso malintencionado del ciberespacio, incluido el uso indebido de la IA o la informática cuántica.

Es importante denunciar a los autores, aplicar sanciones y tomar medidas apropiadas y adecuadas. No puede haber distensión sin atribución, ya que es crucial para fundamentar la toma de decisiones sobre las medidas que deben adoptarse y las defensas que deben determinarse. La atribución puede tener un efecto disuasorio, ya que exigir rendición de cuentas a los autores puede permitir respuestas jurídicas y diplomáticas y reforzar la formulación de políticas.

Por último, es indispensable poder medir de forma exhaustiva y cuantificable los daños causados por los ciberataques. CyberPeace Institute está elaborando una metodología de este tipo para medir los daños ocasionados por los ciberataques porque, hasta ahora, se han descrito con demasiada frecuencia en cuanto a la pérdida de dinero o de capacidad, mientras que el daño a la población humana y las construcciones sociales también es importante.

Estos aspectos son cruciales para mantener la paz y la seguridad internacionales.

El Presidente (*habla en inglés*): Agradezco al Sr. Duguin por su exposición informativa.

Tiene ahora la palabra la Sra. Ifeanyi-Ajufo.

Sra. Ifeanyi-Ajufo (*habla en inglés*): Me siento privilegiada por haber sido invitada a intervenir en este foro sobre el mantenimiento de la paz y la seguridad internacionales y la respuesta a las amenazas cambiantes en el ciberespacio, en particular al aportar una perspectiva regional y analizar la situación en África.

En cualquier debate sobre la paz y la seguridad en el ciberespacio, es necesario medir la seguridad del ciberespacio a través de las realidades y las perspectivas regionales existentes. Debemos reconocer que la realización efectiva de la ciberseguridad choca a menudo con las realidades de los Estados en desarrollo, en especial los de la región africana, que permanecen al final de la brecha digital y carecen de la capacidad, las competencias y las infraestructuras necesarias para garantizar de manera eficaz la paz y la seguridad a los niveles previstos. Por lo tanto, al tiempo que reconocemos nuestros puntos en común en materia de ciberseguridad, también debemos reconocer las diferencias y los desafíos entre regiones y analizar las ciberamenazas en el contexto de las realidades específicas de cada país y región.

Las dimensiones de paz y seguridad del ámbito cibernético han llegado a ser una agenda fundamental para muchas regiones. Por ejemplo, en noviembre de 2022, por primera vez, el Consejo de Paz y Seguridad de la Unión Africana abordó la cuestión de la paz y la seguridad en el ciberespacio desde la perspectiva de su regulación en el marco de las normas del derecho

internacional. Posteriormente, la Unión Africana adoptó la ciberseguridad como programa emblemático de la Agenda 2063 de la Unión Africana y como tema transversal de la Estrategia de Transformación Digital de la Unión Africana para África (2020-2030). Es importante destacar que la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, que proporciona un marco normativo unificado para mitigar las ciberamenazas y proteger la infraestructura de las tecnologías de la información y las comunicaciones (TIC), entró en vigor en junio de 2023. En enero de este año, la Unión Africana también adoptó una posición común africana sobre la aplicación del derecho internacional al uso de las TIC en el ciberespacio. Debo añadir que la posición africana es el primer documento de posición sobre la aplicación del derecho internacional en el ciberespacio, que incluye una sección sobre la creación de capacidades. África es también la primera región que adopta una posición común regional.

También debemos reconocer que existen diversos desafíos para que las regiones puedan mantener la paz, la seguridad y la estabilidad en el ciberespacio. Desde el año pasado, por ejemplo, se han perpetrado ciberataques contra la sede de la Comisión de la Unión Africana, que comprometieron el funcionamiento de los sistemas de correo electrónico. La Autoridad de Comunicaciones de Kenya anunció que, solo en 2023, Kenya registró 860 millones de ciberataques, pues se llevaron a cabo ataques sofisticados dirigidos a la infraestructura de información crítica del país. Solo en julio de 2023, Kenya sufrió un ciberataque de gran repercusión en la importantísima plataforma eCitizen, que incapacitó el acceso a más de 5.000 servicios gubernamentales de ministerios, Gobiernos de condados y organismos. Un grupo que se hace llamar Anonymous Sudan declaró ser responsable de esos ciberataques en Kenya y otras partes de África. Hace unos meses, los ciberataques organizados obligaron al Gobierno de Malawi a suspender la expedición de pasaportes, tras un ciberataque a la red informática del Servicio de Inmigración, que se consideró una violación grave de la seguridad nacional.

Esto plantea cuestiones importantes, como las difusas líneas de la responsabilidad de los actores estatales y no estatales y la dinámica de cómo estas ciberamenazas emergentes añaden fisuras a los conflictos ya existentes. Vemos cómo las actividades de los grupos terroristas y extremistas organizados se ven favorecidas por los conflictos en regiones como África. Vemos cómo las actividades delictivas en el ciberespacio no solo exacerban las amenazas existentes y los desafíos a la paz y la seguridad internacionales en la región, sino también cómo los Estados vulneran los derechos humanos internacionales, so pretexto de la ciberseguridad al cerrar el acceso a Internet, en especial en el contexto de los conflictos armados. Estas acciones no solo vulneran los derechos a la comunicación y la libertad de información de los ciudadanos, sino que también han impedido una acción humanitaria eficaz durante los conflictos en lugares como África y, por supuesto, en otros lugares. También vemos cómo la desinformación y la información errónea cibernéticas se utilizan cada vez más como herramientas para echar por tierra la paz y la seguridad en algunas partes de la región. Esto se ve agravado por el despliegue de la inteligencia artificial en tales circunstancias.

Sin embargo, consideramos que el Consejo de Seguridad puede marcar una diferencia inmensa para reforzar la paz y la seguridad en el ciberespacio, sobre todo desde una perspectiva regional. De hecho, las fuentes de desigualdad existentes requieren interacciones complejas para definir un mandato sobre la paz y la seguridad en el ciberespacio del Consejo de Seguridad. Estas disparidades en las infraestructuras de ciberseguridad y en las capacidades digitales constituyen un desafío fundamental, al que se suman los persistentes conflictos políticos en regiones como África. También parece haber desconocimiento de las obligaciones relacionadas con la no intervención, la diligencia debida y la solución pacífica de las controversias en el contexto del ciberespacio.

Mientras el Consejo de Seguridad determina su mandato para mantener la paz y la seguridad en el ciberespacio, es importante considerar medidas de colaboración que puedan aprovecharse con eficacia para contrarrestar las amenazas existentes y crear capacidades. Es preciso establecer y reforzar la capacidad a escala regional. Sin embargo, debemos señalar que no es solo una cuestión de capacidad jurídica, técnica y operacional, sino también de realidades sociales, económicas y políticas. Habida cuenta de los diversos niveles de madurez en materia de ciberseguridad y los contextos locales, se requiere un refuerzo estratégico de las capacidades regionales. Deben tenerse en cuenta las realidades específicas de las distintas regiones, ya que las carencias de capacidad no tienen por qué ser las mismas en todas ellas. Los intentos de desarrollar y transferir cibercapacidades entre regiones deben enfocarse con determinación, pero también deben elaborarse estrategias basadas en mecanismos definidos de rendición de cuentas.

En regiones como África, los ámbitos prioritarios donde es necesario reforzar las capacidades para hacer frente a las amenazas cibernéticas son la gobernanza, la

elaboración de políticas, las herramientas técnicas y las infraestructuras, así como la investigación. Es necesario desarrollar capacidades para la protección de infraestructuras críticas. Es importante garantizar la creación de equipos de respuesta a incidentes de ciberseguridad a nivel regional allí donde aún no existan, y ordenar el establecimiento de puntos de contacto regionales las 24 horas durante los siete días de la semana. También es importante implantar y aplicar mecanismos de colaboración regional e internacional entre esos equipos.

Para promover la confianza y la seguridad en el ámbito cibernético, es preciso centrarse en la aplicación de las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio en todas las regiones. Se han planteado muchas preguntas sobre el carácter voluntario de las normas y la necesidad de contar con enfoques más responsables para mantener la paz y la seguridad en el ciberespacio, por ejemplo, disponer de directrices claramente definidas sobre el uso de la fuerza, los ataques armados y la legítima defensa en el ciberespacio. Una vez más, la creación y el apoyo de foros para elaborar medidas de fomento de la confianza disminuirán la desconfianza entre los Estados Miembros y contribuirán a la solución pacífica de las controversias en el ámbito cibernético.

Asimismo, es importante que el Consejo de Seguridad establezca mecanismos que permitan comprender el panorama de las ciberamenazas en las distintas regiones. Ello permitirá tomar decisiones informadas sobre la regulación de la seguridad y la estabilidad. Ello puede implicar también la creación de un grupo de trabajo sobre la paz y la seguridad en el ciberespacio, en primer lugar para estudiar recomendaciones sobre los conflictos y el fomento de la paz y la estabilidad en el ciberespacio. La creación de centros de ciberseguridad regional funcionales para mejorar la cooperación transfronteriza y el intercambio de información ayudará también a lograr esos objetivos. Además, se debe prestar atención al fortalecimiento de capacidades para elaborar y aplicar estrategias de ciberseguridad regionales y nacionales amplias, así como a la promoción de una cultura del liderazgo en materia de ciberseguridad.

Las organizaciones regionales tienen un papel crucial en la formulación de políticas y la colaboración con los Estados de cada región para lograr resultados en materia de paz y seguridad. Por ello, la actual cooperación entre las Naciones Unidas y las organizaciones regionales y subregionales en el mantenimiento de la paz y la seguridad internacionales debería incluir una agenda sobre ciberseguridad. Finalmente, el Consejo de Seguridad debería promover una plataforma de diálogo que aliente a las regiones a elaborar un marco relativo a la paz y la seguridad en el ciberespacio.

Concluiré insistiendo en la importancia de que el Consejo de Seguridad establezca una agenda multilateral que afirme con decisión las dimensiones del estado de derecho relacionadas con la paz y la seguridad en el ciberespacio. Ello requiere definir normas y principios de cibergobernanza que reconozcan las responsabilidades de las regiones y los Gobiernos en materia de paz y estabilidad. Al estar más interconectados y más expuestos a tecnologías disruptivas como la inteligencia artificial, nos estamos volviendo también más vulnerables. Por ello, es importante que reforcemos nuestra capacidad humana e institucional para garantizar la ciberseguridad, generando confianza en cuanto al uso de las cibertecnologías.

El Presidente (*habla en inglés*): Formularé ahora una declaración como Ministro de Relaciones Exteriores de la República de Corea.

Quiero comenzar dando las gracias, una vez más, al Secretario General Guterres por su presencia y por su exposición de hoy. Permítaseme que dé las gracias también al representante de CyberPeace Institute, Sr. Stéphane Duguin, así como a la catedrática de la Universidad Leeds Beckett Nnenna Ifeanyi-Ajufo, por habernos transmitido sus perspectivas y sus conocimientos expertos. Hago extensivo mi sincero agradecimiento a los representantes de los Estados Miembros que participan en este debate abierto de alto nivel.

La sesión de hoy es la segunda ocasión en la historia de las Naciones Unidas en la que el Consejo de Seguridad se reúne oficialmente para hablar de las amenazas a la paz y la seguridad internacionales procedentes del ciberespacio. El Consejo convocó un primer debate abierto sobre este tema hace tres años, en junio de 2021 (véase S/2021/621). Sin duda, se han logrado hitos importantes fuera del marco del Consejo de Seguridad. Entidades creadas por la Asamblea General han propuesto normas sobre la conducta responsable de los Estados en el ciberespacio. También se han celebrado varias reuniones sobre ciberseguridad con arreglo a la fórmula Arria, la más reciente de las cuales fue la sesión de abril organizada conjuntamente por la República de Corea, los Estados Unidos y el Japón.

Asimismo, el Secretario General ha demostrado un sólido liderazgo en este ámbito al reclamar medidas que reduzcan los riesgos asociados al ciberespacio y crear el Órgano Asesor de Alto Nivel sobre Inteligencia

Artificial, del que Corea forma parte. Ahora bien, la evolución de los acontecimientos tras esa sesión inicial del Consejo de Seguridad celebrada hace tres años deja claro que el Consejo, en estos momentos, debe ocuparse de manera más proactiva por las amenazas procedentes del ciberespacio. Además de innumerables ciberataques transfronterizos, en el mundo han estallado grandes conflictos armados que han comportado ataques en el ciberespacio, además de en los campos de batalla tradicionales.

Asimismo, el mundo ha sido testigo de que el rápido progreso de la inteligencia artificial refuerza drásticamente la capacidad de actores malignos para causar aún más caos y perturbaciones en el ciberespacio. El mundo ha sido testigo de que la ciberactividad malintencionada puede tener repercusiones en el mundo real, al socavar la confianza en la integridad de elecciones políticas, la seguridad de infraestructuras críticas y el propio tejido de la paz y la seguridad. En efecto, un Estado Miembro llegó a declarar el estado de emergencia tras ser objeto de ataques con *ransomware* originados en otro país.

Por su propia naturaleza, las tecnologías cibernéticas son de doble uso: cualquier actor malintencionado puede introducir nuevas amenazas o bien desencadenar, amplificar o acelerar amenazas existentes. Como señaló en una ocasión el célebre futurólogo Alvin Toffler: “Nuestras capacidades tecnológicas van en aumento, pero también se multiplican los efectos secundarios y los peligros potenciales”.

La República de Corea no es ajena a las amenazas que plantean las ciberactividades maliciosas ni a su repercusión en la seguridad, ya que el desarrollo de armas de destrucción masiva que han puesto en peligro a Corea se ha financiado en gran medida con ese tipo de actividades. En el informe más reciente del grupo de expertos del Comité establecido en virtud de la resolución 1874 (2009) (S/2024/215) se indica que el 40 % de los programas de armas de destrucción masiva de la República Popular Democrática de Corea se financian con medios cibernéticos ilícitos. El grupo había comenzado a investigar unos 60 ciberataques que la República Popular Democrática de Corea llevó presuntamente a cabo con el uso de empresas de criptomonedas entre 2017 y 2023. Lamentablemente, ese grupo de expertos ya no existe, por razones de todos conocidas.

Con el uso de medios digitales, la República Popular Democrática de Corea elude sistemáticamente las sanciones impuestas por el Consejo y desafía el régimen internacional de no proliferación, que es parte integrante de la labor del Consejo. En un momento en que la paz y la seguridad en el mundo físico y en el cibermundo están cada vez más interrelacionadas, el Consejo de Seguridad no debe adoptar la táctica del avestruz. Como mínimo, debe estar al tanto de las tendencias existentes fuera del Consejo y reforzar su determinación de responder a las amenazas reales y actuales que se plantean en el ciberespacio. Del mismo modo que el Consejo de Seguridad y la Asamblea General trabajan de manera sinérgica en relación con las armas de pequeño calibre, el terrorismo y la no proliferación, el Consejo de Seguridad y la Asamblea General pueden desempeñar papeles complementarios en materia de ciberseguridad.

Si bien aún no existe un enfoque autorizado sobre la vía a seguir, la República de Corea quiere plantear tres sugerencias a la consideración del Consejo de Seguridad.

En primer lugar, el Consejo debe disponer de un diagnóstico claro sobre la situación actual. Para ello, el Consejo de Seguridad puede solicitar informes periódicos que ayuden a entender el grado en que las ciberamenazas afectan al mandato del Consejo y el modo en que su evolución repercute en la paz y la seguridad internacionales.

En segundo lugar, las indicaciones siguientes se aplican a la totalidad de los expedientes de los que se ocupa el Consejo. La ciberseguridad podría ser uno de los temas de los que se ocupa el Consejo del mismo modo que se han incorporado otras cuestiones transversales, como las mujeres y la paz y la seguridad, la juventud y el cambio climático. Como señalaron varios Estados Miembros en la reunión celebrada en abril con arreglo a la fórmula Arria, hay una relación directa entre el uso malintencionado de las tecnologías de la información y la comunicación y diversas cuestiones que son competencia del Consejo de Seguridad, como las sanciones, la no proliferación y el terrorismo. En ese sentido, el Consejo puede considerar la ciberseguridad como un componente importante que está presente de manera transversal en las cuestiones regionales y temáticas de las que se ocupa.

En tercer lugar, a mediano y largo plazo, el Consejo de Seguridad debería estar en condiciones de abordar adecuadamente este desafío. El Consejo puede convocar sesiones en las que se hable de las ciberactividades malintencionadas que contravengan el derecho internacional y perjudiquen a la paz y la seguridad. Además, podría instar a los agentes en cuestión a utilizar la cibertecnología de manera responsable, así como exigir

responsabilidades recurriendo a las herramientas que están a su disposición. Huelga decir que el Consejo de Seguridad debería elaborar un programa de trabajo sobre ciberseguridad que complemente los debates mantenidos en la Asamblea General.

Históricamente, el Consejo de Seguridad ha ido definiendo su propia agenda a medida que surgían nuevos desafíos en materia de seguridad. Poco imaginaban los artífices de la Carta de las Naciones Unidas que el cambio climático, los abusos contra los derechos humanos y la pandemia serían competencia del Consejo de Seguridad. El Consejo de Seguridad debe afrontar claramente la cuestión de la ciberseguridad si quiere seguir siendo relevante y abordar con agilidad uno de los desafíos en materia de seguridad más acuciantes de nuestro tiempo. Espero sinceramente que el debate abierto de hoy genere la dinámica necesaria para lograrlo.

Antes de concluir, permítaseme hacer una última observación. El hecho de que el ciberespacio no tenga fronteras deja a todas las naciones, independientemente de su vulnerabilidad o de su progreso digital, expuestas a los daños causados por ciberactividades malintencionadas. La seguridad internacional en el ciberespacio es tan fuerte como su eslabón más débil. Por consiguiente, el nexo acción humanitaria-desarrollo-paz es igual de real en el cibermundo. Un ciberespacio libre de actividades maliciosas facilitará el desarrollo digital y creará oportunidades digitales que, en último término, contribuirán a la consecución de los Objetivos de Desarrollo Sostenible. Un ciberespacio abierto, seguro, accesible y pacífico, en el que sea posible atajar las ciberamenazas, protegerá también la libertad y los derechos humanos en línea.

Vuelvo a asumir las funciones de Presidente del Consejo.

Doy ahora la palabra a la Representante Permanente de los Estados Unidos y miembro del Gabinete del Presidente Biden.

Sra. Thomas-Greenfield (Estados Unidos de América) (*habla en inglés*): Quiero empezar dando las gracias a la República de Corea por habernos reunido de nuevo para examinar esta cuestión crítica y este asunto de paz y seguridad. Quiero darle la bienvenida al Consejo de Seguridad, Señor Presidente, y expresarle mi más sincero agradecimiento. Tuve el honor de conocerle en Seúl durante mi visita hace unos meses, y es maravilloso tenerlo aquí. Agradezco al Secretario General y a los exponentes sus exposiciones informativas y doy la bienvenida a los demás Ministros, que hoy nos honran con su presencia.

Desde nuestra anterior sesión celebrada en abril, hemos seguido constatando el imperativo de una seguridad sólida en el ciberespacio y, en consecuencia, la necesidad de examinarla en el Consejo. La ciberseguridad permite que funcionen nuestros sistemas más básicos: nuestras economías e instituciones democráticas y, sí, incluso las propias Naciones Unidas. Los Estados Unidos se comprometen a colaborar con todos los agentes responsables para salvaguardar los beneficios del ciberespacio, construir la solidaridad digital y aprovechar la tecnología para lograr los Objetivos de Desarrollo Sostenible. Sin embargo, demasiados agentes estatales y no estatales han adoptado la posición contraria. En todo el mundo se han aprovechado de la conectividad digital para extorsionar a sus víctimas con fines lucrativos, robar dinero e ideas a gobiernos y entidades privadas, atacar a periodistas y defensores de los derechos humanos, prepararse para conflictos futuros y amenazar nuestras infraestructuras críticas, incluidas las de las Naciones Unidas.

Como Consejo, debemos trabajar de consuno para hacer frente a las ciberamenazas que plantean los agentes no estatales y estatales y fortalecer las normas de comportamiento responsable de los Estados, hacer que los países rindan cuentas por su comportamiento irresponsable en el ciberespacio y apoyar a las víctimas que se ven afectadas por ese comportamiento, así como desarticular las redes de delincuentes que están detrás de peligrosos ciberataques en todo el mundo. Ya existe un marco para hacerlo. El marco de comportamiento responsable de los Estados en el ciberespacio, aprobado en reiteradas ocasiones y por consenso, deja claro que el derecho internacional se aplica al ciberespacio y que se espera que los Estados cumplan las normas voluntarias de comportamiento estatal en tiempos de paz. Entre esas normas se encuentra la expectativa de que los Estados investiguen y mitiguen la actividad cibernética maliciosa originada en su territorio y tenga como objetivo la infraestructura crítica de otro. Y, sin embargo, algunos de los que han respaldado ese marco optan por ignorar —o peor aún, empoderar— a agentes malintencionados.

Así se puso de relieve en la reunión de abril con arreglo a la fórmula Arria sobre ciberseguridad, en la que se mencionaron las ciberoperaciones maliciosas llevadas a cabo por la República Popular Democrática de Corea, utilizadas para financiar sus programas de armas de destrucción masiva y misiles balísticos. Hay que citar también la actividad cibernética rusa en Ucrania, Alemania, Chequia, Lituania, Polonia, Eslovaquia y Suecia, donde, entre otras actividades, la Dirección

Principal de Inteligencia del Estado Mayor de Rusia ha atacado a partidos políticos e instituciones democráticas. No solo eso, sino que el Gobierno ruso también ha servido de refugio seguro para agentes de *ransomware*, que en los últimos años han causado pérdidas de miles de millones de dólares e importantes daños a hospitales y otras infraestructuras críticas.

Por su parte, los Estados Unidos y el Reino Unido anunciaron en febrero operaciones para desarticular el grupo de *ransomware* LockBit, que se ha cebado con 2.000 víctimas y ha exigido rescates por valor de cientos de millones de dólares, de los que se pagaron más de 120 millones. En los últimos meses, hemos hecho pública una acusación contra los ciudadanos rusos Artur Sungatov e Ivan Kondratyev, también conocidos como Bassterlord, por utilizar LockBit contra numerosas víctimas en los Estados Unidos y a escala internacional. Eso se suma a los esfuerzos desplegados a través de la Iniciativa Internacional contra el *ransomware* que creamos en 2021, y que ahora constituye la mayor ciberasociación del mundo. Como Estados individuales, a través de esa asociación y en los foros multilaterales, incluidas las Naciones Unidas, exhortamos a todos los Estados a que hagan la parte que les corresponde para aplicar el marco y promover la paz y la estabilidad en el ciberespacio. Y exhortamos al Consejo a que garantice que la ciberseguridad sea una prioridad intersectorial que se tenga en cuenta en todos los aspectos de nuestro mandato. Ya se trate de estudiar cómo las operaciones de mantenimiento de la paz pueden promover una buena ciberhigiene para limitar los riesgos o comprender mejor cómo la ciberseguridad puede potenciar los esfuerzos de no proliferación, el Consejo debe seguir contemplando los retos a través de la lente de la ciberseguridad.

Tenemos la capacidad de proteger nuestras infraestructuras más críticas y a todos los que cuentan con ellas. Y tenemos el potencial de salvaguardar los beneficios del ciberespacio para todos. Así pues, con el marco de comportamiento responsable de los Estados en el ciberespacio como guía, debemos reafirmar la aplicabilidad del derecho internacional al comportamiento entre Estados. Tenemos que fomentar la adhesión a normas voluntarias de comportamiento estatal responsable en tiempos de paz y contribuir a reducir el riesgo de conflicto derivado de los ciberincidentes. Y tenemos que defender el orden internacional basado en normas y garantizar que el mundo digital influya en el mundo material para mejor.

Le agradezco de nuevo, Sr Presidente, que nos haya reunido para examinar esta cuestión importante.

Sr. Persaud (Guyana) (*habla en inglés*): Doy las gracias al Ministro de Relaciones Exteriores, Excmo. Sr. Cho Tae-yul, y a la Presidencia de la República de Corea por haber organizado el debate abierto de hoy sobre cómo hacer frente a la evolución de las amenazas en el ciberespacio. También doy las gracias al Secretario General y a los demás exponentes por sus importantes aportaciones a las deliberaciones.

Los rápidos avances tecnológicos han creado un mundo de posibilidades ilimitadas, que presenta ventajas económicas, sociales y geopolíticas inmensas. Sin embargo, a medida que las tecnologías digitales se vuelven más sofisticadas y son desplegadas por agentes malintencionados, plantean riesgos sin precedentes tanto para la seguridad humana como para la nacional. El uso malintencionado de las tecnologías digitales también ha demostrado su potencial para causar perturbaciones en las instituciones y plantear retos normativos y políticos relacionados con la gobernanza. Además, la índole transnacional de las ciberamenazas ha dejado obsoletas las nociones tradicionales de seguridad y defensa nacionales.

Las amenazas a la ciberseguridad a las que ahora estamos expuestos pueden tener un impacto paralizante en la salud, la seguridad y la protección de nuestros ciudadanos, así como en el funcionamiento de servicios esenciales. Las amenazas contemporáneas a la ciberseguridad son cada vez más sofisticadas y multifacéticas, ya se trate del ciberespionaje patrocinado por los Estados, la injerencia en los procesos democráticos, las violaciones de los derechos humanos, los ataques a infraestructuras críticas o la propagación de información errónea, la desinformación y el discurso de odio, y las respuestas que les demos también deben serlo.

En ese sentido, sugiero que se examinen tres esferas importantes.

En primer lugar, deben existir mecanismos de rendición de cuentas y supervisión para protegerse de los ciberataques. A ese respecto, tomamos nota de las recientes deliberaciones sobre si los ciberataques dirigidos contra infraestructuras críticas, como centros médicos o centrales eléctricas, que tienen consecuencias graves para la vida, pueden constituir crímenes de guerra, crímenes de lesa humanidad, genocidio o crímenes de agresión. Eso debe examinarse a fondo e incluirse en un marco jurídico amplio que también debe garantizar que las herramientas y tecnologías digitales se desarrollen y se utilicen respetando debidamente consideraciones éticas y los derechos humanos. A ese respecto, Guyana reconoce la importancia de que concluyan los

trabajos 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 y la necesidad de contar con una convención ampliamente ratificada.

En segundo lugar, debemos dar prioridad a la cooperación, la colaboración y las asociaciones para crear capacidad y resiliencia en materia de ciberseguridad e investigar y enjuiciar los ciberdelitos en todos los países y regiones. En cuanto a las asociaciones, debemos invertir en la generación de confianza y la mejora de la colaboración regional e internacional para fomentar la puesta en común de conocimientos, el intercambio de información y la transferencia de tecnología. También debemos tratar de desarrollar la interoperabilidad entre nuestros sistemas nacionales, regionales e internacionales que se ocupan del rastreo y la vigilancia de las amenazas a la ciberseguridad. Para que ello sea eficaz, es preciso desarrollar un marco global que posibilite el intercambio de información entre los Estados y las partes interesadas sobre las nuevas amenazas a la ciberseguridad. Aunque los debates que se están entablando en el seno de las Naciones Unidas y de los mecanismos regionales han contribuido positivamente a ese empeño, particularmente en el marco de la Hoja de Ruta del Secretario General para la Cooperación Digital y de la Agenda de Aceleración Digital de los Objetivos de Desarrollo Sostenible, aún queda mucho trabajo por hacer. También debemos aprovechar las oportunidades que brinda el ciberespacio para adoptar un enfoque que abarque a toda la sociedad con el fin de contrarrestar las ciberamenazas y reforzar la ciberseguridad.

Las nuevas tecnologías, como los sistemas de inteligencia artificial, pueden ayudar a identificar y mitigar esas amenazas. A ese respecto, los Gobiernos debemos redoblar nuestros esfuerzos para colaborar con las empresas tecnológicas y el sector privado con el fin de desarrollar herramientas y políticas de seguridad más sólidas y mejorar el intercambio de información en el análisis de la inteligencia sobre amenazas. Además, muchos países en desarrollo, como Guyana, carecen de los recursos y los conocimientos necesarios para luchar contra las ciberamenazas y reforzar su resiliencia. La creación de capacidad técnica en esos países debe entenderse como una inversión en nuestra seguridad colectiva que serviría para poner fin a las desigualdades y los desequilibrios existentes en las capacidades de ciberseguridad. Habida cuenta de lo antedicho, los miembros de la comunidad mundial podemos explorar la posibilidad de crear un fondo mundial que se ocupe de la formación y el desarrollo de las capacidades, así como del desarrollo de software y hardware. Además, Guyana exhorta a aquellos países desarrollados dotados de capacidades tecnológicas avanzadas a que proporcionen asistencia técnica y financiación para mejorar la infraestructura de ciberseguridad y la capacidad de respuesta en los países en desarrollo. No deben escatimarse esfuerzos para garantizar que ningún país o entidad monopolice las herramientas y capacidades tecnológicas que podrían exacerbar aún más las vulnerabilidades de los países en desarrollo, por ejemplo, mediante la imposición de leyes y normativas que tienen repercusiones extraterritoriales.

En tercer lugar, sin perjuicio de los procesos en curso en otros foros de las Naciones Unidas, el Consejo de Seguridad debe formar parte del debate sobre ciberseguridad, habida cuenta de la amenaza que la ciberactividad maliciosa supone para el mantenimiento de la paz y la seguridad internacionales. Por consiguiente, el Consejo debe intensificar su debate sobre esta cuestión basándose en las sesiones celebradas con arreglo a la fórmula Arria y en los debates abiertos, incluido el debate actual, para concienciar sobre las amenazas emergentes que plantean las nuevas tecnologías y examinar colectivamente las medidas eficaces que pueden desplegarse contra el uso malintencionado de esas tecnologías.

Para terminar, los retos que plantean las amenazas a la ciberseguridad son descomunales, pero no insuperables. Gracias a nuestro esfuerzo y voluntad colectivos y a una acción concertada, podemos construir un mundo digital resiliente y seguro que fomente la confianza, la innovación y la prosperidad para todos. Aprovechemos el momento, no solo para responder a las amenazas que se ciernen sobre nosotros, sino para forjar proactivamente un futuro en el que se garantice que nadie se quede atrás. Guyana está dispuesta a colaborar con todos los Estados Miembros en ese empeño.

Sr. Nebenzia (Federación de Rusia) (*habla en ruso*): Señor Presidente, nos congratulamos de que ocupe la Presidencia del Consejo de Seguridad. Damos las gracias al Secretario General por su exposición informativa. También hemos escuchado atentamente a los exponentes.

Rusia estuvo presente en el inicio de los debates sobre cuestiones de seguridad de la información internacional en las Naciones Unidas. En 1998, hace 26 años, planteamos el tema por primera vez en la Asamblea General, presentando la primera resolución (resolución

53/70 de la Asamblea General) sobre ese tema específico. Desde entonces, la aprobación de resoluciones sobre este tema se ha convertido en un acontecimiento anual apoyado por la inmensa mayoría de los Estados Miembros.

Por iniciativa nuestra, se creó el correspondiente Grupo de Expertos Gubernamentales de las Naciones Unidas para debatir cuestiones de seguridad en el uso de las tecnologías de la información y las comunicaciones. Más tarde, el Grupo evolucionó hacia un formato inclusivo —el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones— que es una plataforma de negociación única y unificada bajo los auspicios de las Naciones Unidas para debatir todas las cuestiones de seguridad de la información internacional.

En el transcurso de sus actividades, el grupo de trabajo de composición abierta ha demostrado su eficacia y pertinencia. Entre sus resultados prácticos figura el lanzamiento en mayo —a instancias de Rusia— de un directorio de puntos de contacto para el intercambio de información sobre ataques o incidentes informáticos. Se está llevando a cabo un examen detallado de las amenazas existentes y potenciales en el ámbito de la seguridad de la información internacional. Se están adoptando medidas concretas para desarrollar la capacidad digital de los Estados. El año pasado se acordaron principios universales para la asistencia en ese ámbito.

Creemos que los esfuerzos de la comunidad internacional deben centrarse en seguir reforzando la cooperación entre los Estados en el marco del grupo de trabajo de composición abierta para lograr resultados concretos y prácticos que garanticen la seguridad de la información internacional. Consideramos que reviste una importancia crucial consolidar y aprovechar los resultados logrados por el grupo de trabajo de composición abierta, tanto en el marco de su mandato actual como en un futuro formato de negociación. Rusia ya ha presentado su visión de un mecanismo inclusivo permanente en ese ámbito. Creemos que convendría salvaguardar nuestros logros comunes creando un grupo de trabajo permanente de composición abierta con una función decisoria después de 2025.

De los hechos mencionados se desprende claramente que las Naciones Unidas ha acometido históricamente una dilatada labor constante y progresiva en materia de seguridad de la información internacional. Por consiguiente, la necesidad de implicar al Consejo de Seguridad plantea serios interrogantes. El tema tiene sus propias especificidades y debe debatirse en foros especializados donde se cuente con los conocimientos especializados pertinentes. Es crucial asegurarse de que los debates sean profesionales y constructivos y de que se evite la politización. La duplicación de los esfuerzos de la comunidad internacional y la difusión del tema en diversos foros de las Naciones Unidas son contraproducentes y podrían revertir todos los resultados logrados a lo largo de decenios bajo los auspicios de la Asamblea General.

Igualmente importante es que los debates del grupo de trabajo de composición abierta sean inclusivos. Todos los Miembros de las Naciones Unidas pueden participar sin excepción y en pie de igualdad, ya que las decisiones se toman por consenso. Si el tema se encomendara al Consejo de Seguridad, se excluiría automáticamente de la toma de decisiones a todos los Estados que no son miembros del Consejo. Quienes han apoyado hoy el llamamiento de la Presidencia para que la seguridad de la información internacional forme parte de la agenda del Consejo de Seguridad deben, obviamente, tener ese extremo en cuenta.

Por último, en todo debate sobre los riesgos potenciales se deben tener en cuenta las peculiaridades tecnológicas del ciberespacio. A diferencia del mundo físico, las amenazas en el ciberespacio son extremadamente difíciles de identificar, y la identificación del origen de un ataque —la denominada atribución— se torna aún más complicada. A menudo se tarda mucho tiempo en tener conocimiento, a través de pruebas circunstanciales, de que se ha producido un ataque. Por consiguiente, aún no tenemos siquiera una comprensión básica de qué casos de uso malintencionado de las tecnologías de la información y las comunicaciones pueden considerarse, sin temor a equivocarnos, amenazas directas a la paz y la seguridad internacionales. Hasta que no se resuelva el problema de la atribución y se desarrolle un enfoque unificado de otros aspectos complejos de ese problema polifacético y específico, incluidos los jurídicos, cualquier debate en el Consejo de Seguridad puede convertirse en otro intercambio de acusaciones sin fundamento y exacerbar la división en la comunidad internacional. Ello socavaría la autoridad del Consejo y no ayudaría en absoluto a desarrollar soluciones constructivas.

Todos los Estados que han intervenido o que intervendrán hoy son participantes en el grupo de trabajo de composición abierta, y los temas propuestos para el debate son similares a los debatidos por el Grupo. En mayo se convocó una mesa redonda a nivel ministerial sobre creación de capacidades en el ámbito de la seguridad de la información internacional, y en julio se celebrará la octava sesión del grupo de trabajo de composición abierta.

De hecho, el debate sobre el tema ya está en marcha, y sus avances y resultados están a disposición de todos.

Por consiguiente, no apoyamos el llamamiento para que se conciencie a la comunidad internacional sobre las cuestiones de seguridad de la información internacional mediante la convocación de sesiones periódicas del Consejo de Seguridad. En el mandato del Consejo de Seguridad se contempla una respuesta rápida a las amenazas reales a la paz y la seguridad internacionales, más que un intercambio filosófico de opiniones sobre temas comunes de dominio público. Para ese fin existen otros foros y formatos.

También preocupan en extremo los intentos de los colegas occidentales de alegar la existencia de actividades maliciosas que utilizan las tecnologías de la información y las comunicaciones para luego ir en contra de Estados "indeseables". Peor aún, nunca ofrecen ninguna prueba convincente que respalde esas alegaciones.

En repetidas ocasiones, el Grupo de Expertos sobre la República Popular Democrática de Corea del Comité del Consejo de Seguridad establecido en virtud de la resolución 1718 (2006) ha servido de instrumento en ese juego sin escrúpulos. A partir de un dato que aportó un Estado Miembro concreto, el Grupo se puso en contacto con la parte rusa en relación con los ataques informáticos atribuidos a Pyongyang. Cuando solicitamos los datos precisos necesarios para investigar los supuestos incidentes, los expertos respondieron que no habían recibido ninguna información adicional de sus "fuentes". Sin embargo, la falta de detalles no impide que nuestros colegas occidentales acusen sin fundamento de todo tipo de "ciberpecados" a los países que no están de acuerdo con sus acciones. Normalmente, califican esas acusaciones de "muy probables", la expresión favorita de los países occidentales. Esas insinuaciones infundadas son inaceptables. Para atribuir responsabilidades, se necesita un enfoque profesional y pruebas técnicas exhaustivas.

Rechazamos con rotundidad toda especulación de que Rusia supuestamente fomenta actos maliciosos en línea. Llevamos un cuarto de siglo propugnando la prevención de la militarización del espacio en línea, y empezamos a proponer medidas concretas en ese ámbito mucho antes de que los países occidentales reconocieran siquiera la existencia de ese riesgo.

La prioridad de nuestro país es establecer instrumentos universales jurídicamente vinculantes en materia de ciberseguridad, los cuales contribuirán a prevenir los conflictos interestatales en ese ámbito. Para ello, en 2023 Rusia presentó a la Asamblea General un prototipo de tratado internacional especializado en el que se proponía una convención de las Naciones Unidas para garantizar la seguridad de la información internacional. La aprobación de un acuerdo universal de ese tipo no solo permitiría establecer jurídicamente los derechos y las obligaciones de los países en relación con sus actividades en el ámbito de las tecnologías de la información y las comunicaciones, sino que también regularía la cuestión de la atribución política de los ataques informáticos en las relaciones internacionales. Asimismo, ayudaría a garantizar el pleno cumplimiento en línea del principio de igualdad soberana de los Estados, del que, en la actualidad, muchos países con tecnología avanzada hacen caso omiso abiertamente. Invitamos a todos los Estados Miembros a entablar un debate de fondo sobre la base de nuestra propuesta en la Asamblea General.

Lamentablemente, los países occidentales, sobre todo los Estados Unidos, rechazan esa idea, pues intentan preservar la mayor libertad de acción posible para sí mismos. Eso queda muy claro si se tiene en cuenta que las altas esferas estadounidenses reconocen que se cometieron ataques ofensivos contra Rusia mediante el uso de tecnologías de la información y las comunicaciones. También se evidencia en que las doctrinas de Washington y la OTAN establecen estrategias "ofensivas" —que en realidad son agresivas—.

Nuestros exponentes de hoy y las delegaciones que han intervenido antes han hablado de ciberataques. No obstante, olvidaron mencionar que se está librando una guerra de desinformación sin precedentes contra Rusia. Toda esa actividad maliciosa es coordinada desde Gran Bretaña por organizaciones con sede en Londres, como Public Relations and Communications Association y PR Network, así como IT Army of Ukraine. Esta última trabaja sin descanso en el campo de la desinformación. Mediante esos recursos digitales, se está difundiendo gran cantidad de desinformación y de mentiras sobre Rusia y la operación militar especial rusa.

Por otra parte, nos preocupan los intentos de desdibujar el debate mundial sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos. Un claro ejemplo de ello es la "Iniciativa de lucha contra el *ransomware*". Esos "clubes exclusivos", que no hacen demasiado por ocultar sus objetivos politizados, socavan los esfuerzos de los Estados Miembros por desarrollar mecanismos universales de lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos, en particular, los que se emprenden a través 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.

Desde hace más de 26 años, la Federación de Rusia promueve un programa constructivo en el ámbito de la seguridad de la información internacional, con lo que hace su propia contribución al mantenimiento de la paz y la estabilidad, tanto en el mundo físico como en línea. Seguiremos abogando por la creación de un entorno de tecnologías de la información y las comunicaciones que sea pacífico y seguro a escala mundial.

El Presidente (*habla en inglés*): Quisiera recordar a quienes vayan a intervenir que limiten sus intervenciones a un máximo de tres minutos para que el Consejo pueda llevar a cabo su labor en forma diligente. Transcurridos los tres minutos, la luz de los micrófonos parpadeará para indicar que se debe concluir la intervención.

Sr. Afonso (Mozambique) (*habla en inglés*): Mozambique desea transmitir su gratitud a usted, Señor Presidente, y a la República de Corea, por la elección pertinente de este tema significativo como evento destacado de su presidencia del Consejo de Seguridad durante el mes de junio. Agradecemos encarecidamente al Secretario General por su enfoque muy perspicaz del tema, alineado a la perfección con la Carta de las Naciones Unidas. Hemos seguido con mucha atención las importantes perspectivas aportadas por el Presidente de CyberPeace Institute, Sr. Stéphane Duguin, y la Profesora Nnenna Ifeanyi-Ajufo, Catedrática de Derecho y Tecnología.

Saludamos a los Ministros y altos dignatarios que están presentes hoy en este Salón.

Todas las declaraciones formuladas hasta ahora han dejado claro que las fronteras entre el ciberespacio y el mundo físico siguen difuminándose a gran velocidad. Como resultado, casi todos los aspectos de nuestra vida moderna han migrado a la tecnología digital y dependen de ella. Así pues, la necesidad de que el Consejo se implique se ve respaldada por el convencimiento de muchos países, grandes y pequeños, de que el ciberespacio —que no tiene fronteras— es un ámbito donde pueden surgir conflictos, al igual que las dimensiones terrestre, marítima, aérea y espacial.

De hecho, podemos considerar que se estableció un punto de partida en 2013, cuando la Asamblea General convino que el derecho internacional, incluida la Carta de las Naciones Unidas, se aplica al ciberespacio. Sin embargo, hasta ahora, las conversaciones diplomáticas mundiales sobre las reglas de enfrentamiento en el ciberespacio han avanzado con más lentitud. A ese respecto, todavía no han rendido frutos los debates celebrados bajo los auspicios del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso.

El panorama y el alcance de las ciberamenazas evolucionan con rapidez debido al avance veloz de la inteligencia artificial, y existen amenazas considerables que plantean nuevos retos para la paz, la seguridad y la estabilidad nacionales e internacionales. Las ciberamenazas van en aumento y apenas pasa un día sin que se informe de ataques de *ransomware* contra entidades públicas o privadas, de la proliferación de ultrafalsificaciones muy realistas generadas con inteligencia artificial o de intentos de denegación de servicio contra partes de un país o sus servicios esenciales, como las finanzas, la salud, las redes eléctricas, el gobierno electrónico y otras infraestructuras críticas. Habida cuenta de que las herramientas que posibilitan la vida moderna se utilizan de forma indebida y se emplean como armas, la ciberdelincuencia se ha convertido en uno de los multiplicadores de amenazas más importantes, que socava la confianza pública en las instituciones y amplifica las tensiones políticas y sociales.

Para agravar estos desafíos, la intensificación de la competencia geopolítica se ha convertido en una fuerza motriz de la ciberseguridad. Los adversarios se esfuerzan por adquirir cibercapacidades militares y de inteligencia, desencadenando así una carrera de ciberarmas en un contexto de acusaciones, atribuciones, represalias y escaladas cada vez mayores. A medida que la ciberseguridad se entrelaza más con la geopolítica, las perspectivas de avanzar hacia un acuerdo internacional sobre mejores normas de ciberseguridad siguen estancadas o incluso retroceden. Esta inmovilidad o falta de progreso en una cuestión tan importante para la humanidad podría socavar nuestra seguridad colectiva.

Habida cuenta de la rápida evolución del panorama de amenazas y la ausencia de reglas de enfrentamiento acordadas, el Consejo de Seguridad debería convenir en llevar a cabo, con carácter de urgencia, varias funciones y acciones específicas que incluyan los siguientes aspectos.

En primer lugar, debería establecer normas y marcos internacionales para el comportamiento responsable de los Estados y las entidades privadas en el ciberespacio, basados en la cooperación mundial.

En segundo lugar, con el ánimo de fomentar nuestra seguridad colectiva, el Consejo podría apoyar iniciativas

en el ámbito de la creación de capacidades para reforzar las capacidades de ciberdefensa de los Estados Miembros, en particular de aquellos con recursos limitados.

En tercer lugar, el Consejo podría promover reuniones informativas sobre conciencia situacional y facilitar el intercambio de información entre naciones sobre amenazas y mejores prácticas, a fin de mejorar nuestra capacidad de resiliencia común en materia de ciberseguridad.

En cuarto lugar, las ciberamenazas deberían estar intrínsecamente vinculadas a otros temas del programa de trabajo del Consejo de Seguridad, como la lucha contra el terrorismo, la injerencia electoral, la protección de infraestructuras críticas y la salvaguarda de las operaciones de paz y la acción humanitaria.

Consideramos que es crucial actualizar y ampliar el debate sobre la ciberseguridad. Las cuestiones relacionadas con el robo de ideas, los datos, la propiedad intelectual, los derechos humanos y la privacidad, así como los parámetros de diseño de productos de consumo críticos y servicios públicos, merecen la misma atención. Para países como Mozambique, es indispensable que las voces y las perspectivas del Sur Global se escuchen en el debate mundial sobre ciberseguridad. Es crucial contar con una diversidad de perspectivas en la mesa y evitar los enfoques únicos para avanzar a escala mundial hacia un marco de gobernanza más justo y resiliente. Alentando debates como el que estamos celebrando bajo la Presidencia de la República de Corea, el Consejo puede desempeñar un papel cardinal para salvaguardar la paz y la seguridad internacionales en la era digital. Mozambique se compromete a seguir implicándose.

Sr. Kanu (Sierra Leona) (*habla en inglés*): Le doy las gracias, Señor Presidente, por haber convocado este importante debate abierto. También agradezco al Secretario General, Excmo. Sr. António Guterres, por su esclarecedora exposición informativa. Damos las gracias asimismo al Sr. Stéphane Duguin y a la Sra. Nnenna Ifeanyi-Ajufo por sus reflexiones. Celebramos la participación de los Ministros de alto nivel en esta sesión.

Sierra Leona agradece la oportunidad que se le brinda de hablar sobre la cuestión fundamental de hacer frente a las amenazas cambiantes en el ciberespacio, consciente al mismo tiempo de los inmensos beneficios y los desafíos interconectados que las tecnologías de la información y las comunicaciones (TIC) representan en el ámbito de la paz y la seguridad internacionales. También reconocemos el desafío fundamental en materia de desarrollo que supone abordar la brecha digital mundial y el riesgo de que esta se profundice ante la proliferación de la inteligencia artificial (IA), en particular la IA generativa.

En esta declaración, Sierra Leona se referirá específicamente a las cuestiones orientativas. Entre las principales tendencias emergentes y en evolución de las actividades malintencionadas en el ciberespacio que plantean desafíos a la paz y la seguridad internacionales figuran la proliferación de programas maliciosos, el *ransomware* como señuelo, los modelos de *ransomware* como servicio y los robos de criptomoneda. Estas actividades constituyen un riesgo importante para la población civil y tienen efectos devastadores en la seguridad nacional y la estabilidad general de nuestros países, lo que plantea riesgos considerables para la paz internacional.

Nos preocupa sobremanera la evolución de las tácticas empleadas en el ciberespacio, que no solo alimentan las actividades terroristas, sino que también ponen en peligro la integridad de los sistemas financieros y los servicios críticos. Subrayamos que el uso creciente de modelos de *ransomware* como servicio y de robos de criptomoneda para apoyar actividades nefastas pone de relieve la necesidad acuciante de reforzar la cooperación y la creación de capacidades para combatir esas amenazas con eficacia. La reciente escalada en la frecuencia y el alcance de los ataques de *ransomware* dirigidos contra infraestructuras críticas y servicios públicos esenciales, demuestra los graves efectos de las ciberamenazas en la seguridad pública y la estabilidad política y exige una vigilancia continua. Sierra Leona está profundamente preocupada por las consecuencias de las ciberamenazas, incluido el uso de los ciberdelitos para financiar actividades ilícitas y evadir sanciones internacionales. Todos ellos subrayan la urgencia de intensificar la cooperación internacional y los esfuerzos de creación de capacidades para combatir esas amenazas con eficacia. Pedimos una mayor colaboración entre los Estados Miembros para reforzar la capacidad del Consejo de Seguridad de responder de manera eficaz a las actividades malintencionadas en el ciberespacio, en particular las que amenazan las infraestructuras críticas, las operaciones humanitarias y la protección de la población civil. Un enfoque holístico es fundamental para mantener la paz y la seguridad en la era digital.

Consideramos que el uso malintencionado de las TIC es un multiplicador de amenazas cuando exacerba los conflictos y los desafíos existentes. La creciente prevalencia de las ciberactividades maliciosas dirigidas contra infraestructuras críticas, como los hospitales y otros sistemas sanitarios, servicios financieros, el

sector energético, los satélites, el transporte y otros sistemas de emergencia, subraya la urgencia de emprender una acción mundial concertada para salvaguardar nuestras redes y sistemas digitales y la importancia del compromiso del Consejo de Seguridad a la hora de abordar estas cuestiones y gestionar y resolver conflictos en los que intervengan ciberelementos.

Como ya hemos escuchado, a pesar de sus enormes beneficios, la IA puede convertirse en un arma para aumentar la magnitud, la velocidad y la sofisticación de los ciberataques. Los sistemas autónomos pueden realizar ataques continuos y adaptativos, aprendiendo de su entorno para explotar las vulnerabilidades con mayor eficacia. Estos ataques impulsados por la IA pueden dirigirse contra infraestructuras críticas, sistemas financieros e incluso la intimidad de las personas, provocando así trastornos y daños generalizados. Sin embargo, también reconocemos que aprovechar la IA para la ciberdefensa puede ayudarnos a adelantarnos a las amenazas emergentes. La IA puede mejorar la detección de amenazas, los tiempos de respuesta y la gestión de incidentes. Si invertimos en tecnologías defensivas basadas en la IA, podremos construir ciberinfraestructuras más resilientes. Al invertir en la creación de capacidades y en la transferencia de tecnología, podemos aumentar las capacidades de los Estados en desarrollo. Sierra Leona considera que el Consejo de Seguridad puede tener un papel crucial a la hora de abordar el carácter cambiante de las ciberamenazas y promover la paz y la seguridad internacionales mediante una colaboración amplia con los comités de la Asamblea General pertinentes y con los órganos y organismos especializados.

Durante el último decenio, el Consejo de Seguridad ha venido ocupándose en mayor medida de las repercusiones del ciberespacio en la paz y la seguridad internacionales. Desde 2016, los miembros del Consejo han convocado varias reuniones con arreglo a la fórmula Arria en las que los Estados han hablado de ciberseguridad, asociándola a temas como la protección de la infraestructura crítica, la protección de los civiles, y la desinformación y el discurso de odio en el ciberespacio.

Por ello, Sierra Leona encomia a Estonia por haber convocado el primer debate abierto de alto nivel sobre este tema durante su Presidencia del mes de junio de 2021. En vista del creciente interés del Consejo de Seguridad por la ciberseguridad, apoyamos la propuesta de convocar sesiones informativas periódicas que nos permitan evaluar cómo evoluciona el panorama de las ciberamenazas, incorporando las perspectivas de múltiples partes interesadas para llegar a un entendimiento general de los desafíos emergentes y adelantarnos a ellos. Insistimos en la necesidad de coordinación, cooperación y dedicación efectivas por parte del Consejo si queremos luchar de manera global contra las ciberamenazas.

Subrayamos que el Consejo de Seguridad puede actuar de una manera que complemente otros procesos de las Naciones Unidas relacionados con las TIC, en particular los debates sobre las normas de comportamiento responsable de los Estados en el uso de las TIC o el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, que fue aprobado por consenso bajo los auspicios de la Asamblea General.

La elaboración de evaluaciones y estrategias para afrontar el panorama cambiante de las ciberamenazas, incorporando las múltiples perspectivas aportadas por el sistema de las Naciones Unidas, el sector privado, la sociedad civil y el mundo académico, garantizaría que el Consejo de Seguridad estuviera al tanto de los nuevos acontecimientos y de sus consecuencias para la paz y la seguridad internacionales.

Considerando los nexos existentes entre las ciberamenazas y otros temas de los que se ocupa el Consejo de Seguridad, los Estados Miembros deberían estudiar el modo de incorporar eficazmente las preocupaciones relacionadas con el ciberespacio y con las TIC en el actual trabajo del Consejo. Sierra Leona sugiere incluir las preocupaciones relativas al ciberespacio en las deliberaciones del Consejo sobre otros expedientes temáticos, como las misiones de mantenimiento de la paz, las sanciones impuestas por el Consejo y las medidas de no proliferación y de lucha contra el terrorismo.

Fortalecer las capacidades nacionales en materia de ciberseguridad y fomentar la cooperación internacional son aspectos vitales de ese enfoque y podrían integrarse también en cada una de esas líneas de trabajo. Incorporando los temas relacionados con el ciberespacio en su labor, el Consejo podrá abordar de una manera más amplia y general los complejos desafíos asociados a las ciberamenazas.

Por nuestra parte, la creación de un Centro nacional de coordinación de la respuesta ante incidentes de seguridad informática ha permitido centralizar la gestión de todos los temas de ciberseguridad en Sierra Leona, en particular la respuesta a los incidentes de ciberseguridad.

Desde su creación, dicho Centro ha logrado hitos importantes que han mejorado la resiliencia de la ciberseguridad nacional, mediante un enfoque

multidimensional basado en la creación de capacidades y la colaboración. Entre otras actividades, destacan las iniciativas de capacitación centradas en la ciberseguridad y la delincuencia. El Centro ha tenido un papel fundamental con su labor de sensibilización e impartición de formación para diversas partes interesadas y ha colaborado con asociados regionales y para el desarrollo en la organización de cursos especializados sobre ciberdelincuencia y pruebas electrónicas para el sector judicial y los organismos encargados de la aplicación de la ley, así como en el intercambio de conocimientos y la puesta en común de buenas prácticas en materia de ciberseguridad e investigación de ciberdelitos. Este tipo de colaboración mejora nuestra capacidad colectiva para luchar eficazmente contra las ciberamenazas mundiales mediante el fortalecimiento de las capacidades nacionales.

Para concluir, permítaseme decir, en primer lugar, que nuestras instituciones judiciales, multilaterales e internacionales, lamentablemente, son objeto con creciente frecuencia de ciberamenazas flagrantes. En ese sentido, Sierra Leona condena de manera inequívoca los ataques dirigidos contra la Corte Penal Internacional. Uno de ellos ha sido descrito por la propia Corte como un “ataque selectivo y sofisticado cuyo objetivo era el espionaje y que, por consiguiente, puede entenderse como un intento grave de socavar el mandato de la Corte”. Como Estado parte en el Estatuto de Roma, Sierra Leona reitera su compromiso de mantener y defender los principios y valores consagrados en él y de preservar su integridad frente a cualquier injerencia o presión ejercidas contra la Corte, sus funcionarios o quienes cooperan con la Corte.

En segundo lugar, permítaseme reafirmar la determinación de Sierra Leona de promover la ciberseguridad como aspecto fundamental de la paz y la seguridad internacionales y de trabajar en colaboración con el Consejo de Seguridad y el conjunto de la comunidad internacional para hacer frente a las complejas y cambiantes amenazas asociadas a las actividades malintencionadas en el ciberespacio.

Sr. Bendjama (Argelia) (*habla en inglés*): Señor Presidente, le doy las gracias por haber organizado este importante debate abierto sobre los riesgos crecientes de las ciberamenazas para la seguridad mundial. Doy las gracias también al Secretario General y a los exponentes por sus presentaciones sobre el preocupante aumento de las ciberactividades dañinas.

Los ataques con *ransomware* contra infraestructura crítica y el robo de activos y datos digitales ponen en peligro la seguridad pública y la estabilidad política. La implicación de actores gubernamentales y no gubernamentales hace que esta situación sea aún más compleja y alarmante. La difusión de desinformación en plataformas en línea alimenta la división, el odio, la intolerancia y, en última instancia, el terrorismo, ya que la información falsa interfiere en los asuntos de los Estados, obstaculiza la cooperación y, en definitiva, plantea una amenaza para la paz y la seguridad en el mundo.

Las nuevas tecnologías, en particular la inteligencia artificial, hacen que las ciberamenazas sean aún más graves y más difíciles de afrontar. Por ello, tenemos que abordar esos desafíos de una manera global y urgente. En vista de estas realidades, quiero subrayar varios aspectos importantes.

En primer lugar, los principios de la Carta de las Naciones Unidas deben aplicarse también al ciberespacio. El uso de las tecnologías de la información y las comunicaciones debe ser acorde a esos principios.

En segundo lugar, tenemos dificultades para garantizar un ciberespacio abierto y seguro, un requisito vital para alcanzar los objetivos de desarrollo mundiales de la Agenda 2030 para el Desarrollo Sostenible. Por este motivo, necesitamos un marco jurídicamente vinculante, establecido en el marco de las Naciones Unidas.

En tercer lugar, debemos ayudar a los países en desarrollo a protegerse contra las ciberamenazas y acabar con la brecha digital. El desarrollo de las capacidades de esos países es indispensable si queremos un ciberespacio seguro para todas las naciones, y debe considerarse una prioridad absoluta.

En cuarto lugar, la comunidad internacional debe luchar conjuntamente contra la difusión de información falsa en Internet. Los Gobiernos son partes implicadas, y las partes implicadas deben cooperar en el marco del derecho internacional. La cooperación internacional es clave en nuestro empeño de luchar eficazmente contra unas ciberamenazas en constante evolución.

En quinto lugar, debemos fortalecer el marco jurídico que permite prevenir y sancionar los ciberdelitos. A ese respecto, quisiera señalar mi país tiene un papel activo en esfuerzos internacionales de lucha contra el uso perjudicial de la tecnología con fines delictivos. Eso es especialmente claro en la dirección de Argelia 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. Esperamos que

ese Comité logre resultados satisfactorios en su próxima sesión este verano.

En conclusión, Argelia apoya con firmeza el papel de las Naciones Unidas en el tratamiento de las cuestiones relativas al uso de las tecnologías de la información y la comunicación que afectan a la paz y la seguridad internacionales. El grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso y la Asamblea General son plataformas esenciales para un examen inclusivo sobre las ciberamenazas. Garantizan que todos los Miembros puedan participar en la configuración de la respuesta mundial a los retos de la ciberseguridad, y reiteramos nuestro empeño de apoyar su labor valiosa.

Sr. Žbogar (Eslovenia) (*habla en inglés*): Doy las gracias a la República de Corea por la organización del debate de hoy. También quisiera las gracias al Secretario General por su exposición informativa, al igual que a los dos exponentes por sus perspectivas y sus recomendaciones.

Permítaseme abordar dos aspectos que son pertinentes para el tema del debate de hoy.

En primer lugar, en lo que respecta a la evolución de las amenazas en el ciberespacio, consideramos que disponer de una comprensión precisa del panorama de las ciberamenazas en constante evolución, especialmente en el contexto del rápido crecimiento de las tecnologías emergentes, como la inteligencia artificial, es primordial para examinar las medidas de cooperación que la comunidad internacional puede adoptar en respuesta a las actividades cibernéticas maliciosas. A ese respecto, elogiamos la actual labor del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, creado por la Asamblea General, pero también reconocemos el potencial complementario de que el Consejo examine el tema en mayor profundidad, por ejemplo, abordando las conclusiones del informe del Secretario General sobre las ciberamenazas (A/77/92). Las actividades cibernéticas maliciosas, como los ataques de programas de *ransomware* y los ataques dirigidos contra infraestructuras civiles críticas, especialmente cuando son de índole transfronteriza, pueden plantear nuevos retos y exacerbar las amenazas existentes a la paz y la seguridad internacionales.

Eso me lleva al segundo aspecto, a saber, abordar la evolución de las amenazas en el ciberespacio. El Consejo de Seguridad es el principal responsable del mantenimiento de la paz y la seguridad internacionales. Para cumplir su responsabilidad de acuerdo con su mandato, el Consejo debe desempeñar un papel decisivo en la reducción de tensiones y el fomento de la rendición de cuentas cuando las actividades cibernéticas maliciosas amenacen la paz y la seguridad internacionales. A nuestro juicio, las actividades que apoyan el terrorismo o la proliferación de armas de destrucción masiva o que exacerban los conflictos existentes o tienen como objetivo infraestructuras civiles críticas, suponen una amenaza de ese tipo y, por tanto, justifican la respuesta del Consejo. En ese mismo sentido, el Consejo debe abordar las actividades cibernéticas maliciosas, como las campañas de desinformación, que incitan a la violencia contra la población civil, causan sufrimiento humanitario o perturban la labor de las organizaciones humanitarias y las operaciones de mantenimiento y consolidación de la paz.

En una época caracterizada por la digitalización cada vez mayor de los conflictos, es crucial hacer hincapié en la aplicabilidad del derecho internacional, incluidos el derecho internacional humanitario y el derecho internacional de los derechos humanos, que deben cumplirse.

Permítaseme concluir asegurando al Consejo nuestro empeño de colaborar con los miembros del Consejo y con el conjunto de los miembros de las Naciones Unidas en la continuación de los debates sobre las ciberamenazas a la paz y la seguridad internacionales. También mantenemos nuestra firmeza en el empeño de aplicar medidas encaminadas a mitigar esos riesgos, incluida la aplicación de las normas vigentes sobre el comportamiento responsable de los Estados en el ciberespacio.

Sra. Frazier (Malta) (*habla en inglés*): Empiezo dando las gracias a la República de Corea por haber organizado este debate abierto sobre esta cuestión de tanta actualidad e importancia. También doy las gracias al Secretario General y a los exponentes por sus exposiciones informativas esclarecedoras.

Las actividades cibernéticas maliciosas plantean retos multifacéticos que pueden tener graves repercusiones en el mantenimiento de la paz y la seguridad internacionales. Van desde ataques de programas de *ransomware* contra instituciones gubernamentales, infraestructuras críticas y servicios públicos esenciales hasta el acceso y uso no autorizados de datos almacenados electrónicamente.

Nos alarman las actividades cibernéticas maliciosas dirigidas contra instituciones gubernamentales y procesos democráticos, a menudo con la intención directa de

socavar la estabilidad y la seguridad y socavar la confianza en el resultado de elecciones democráticas. La dependencia cada vez mayor de las tecnologías digitales por parte de las defensoras de los derechos humanos y otras activistas aumenta su riesgo de exposición al acoso y los ataques en línea. Además, los derechos humanos y las libertades fundamentales, entre ellas la libertad de expresión y reunión, se ven cada vez más restringidas por la vigilancia estricta, los cortes de Internet y la limitación del ancho de banda. Al mismo tiempo, las plataformas digitales se explotan a menudo para difundir desinformación, información errónea y discurso de odio, incluidos contenidos misóginos, homófobos y radicales.

Nuestros esfuerzos colectivos para promover la estabilidad en este ámbito deben basarse en los derechos humanos, tanto en línea como fuera de ella. Las ciberpolíticas deben tener en cuenta los conflictos, la edad y el género para detectar y prevenir los efectos nocivos de las amenazas a la seguridad digital, como la violencia de género facilitada por la tecnología. El liderazgo y la participación plena, igualitaria, segura y significativa de las mujeres en la toma de decisiones cibernéticas es crucial, especialmente en contextos de conflicto y posconflicto.

Reiteramos que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable a las actividades en el ciberespacio, como la Asamblea General ha reconocido. En el mismo sentido, el marco del comportamiento responsable de los Estados en el ciberespacio proporciona directrices acordadas para los Estados Miembros. Todos los Estados Miembros deben cumplir el marco, y apoyamos la creación de un programa de acción que garantice un diálogo continuo e institucionalizado. Además, hacemos un llamamiento a todos los Estados para que actúen con diligencia, adopten las medidas adecuadas en consonancia con las normas del marco de comportamiento responsable de los Estados en el ciberespacio y se abstengan de participar en actividades cibernéticas maliciosas originadas en sus territorios o de prestarles ayuda.

Los agentes malintencionados patrocinados por el Estado explotan los programas de *ransomware* y los robos digitales para generar ingresos ilícitos. Entre ellos se incluyen ataques contra infraestructuras críticas, instituciones financieras y empresas de criptomoneda. Los ciberataques y los delitos no conocen fronteras, y ningún país es inmune a ellos. Según estimaciones de los informes, solo en 2023, las actividades cibernéticas maliciosas perpetradas por *hackers* patrocinados por la República Popular Democrática de Corea generaron el equivalente a 1.000 millones de dólares. El régimen utiliza esos ingresos para financiar su programa ilícito de armas de destrucción masiva, que amenaza la paz y la seguridad en la península y fuera de ella. Esas actividades han quedado perfectamente documentadas en los informes del Grupo de Expertos del Comité establecido en virtud de la resolución 1718 (2006), que desempeñó un papel inestimable en la investigación de esos delitos.

Para concluir, el Consejo de Seguridad puede desempeñar un papel importante para abordar la cuestión de la ciberseguridad. Sus esfuerzos pueden y deben ser complementarios a los de otros foros de ciberseguridad con sede en la Asamblea General, incluido su grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. El Consejo puede servir de plataforma sólida para fortalecer los principios acordados y potenciar nuevas deliberaciones. Debe promover un ciberespacio abierto, seguro, accesible y pacífico. Seguiremos apoyando su colaboración renovada en ese tema.

Sr. Yamazaki (Japón) (*habla en inglés*): Señor Presidente, le agradezco sinceramente su liderazgo a la hora de convocar este importante y oportuno debate abierto, y doy las gracias al Secretario General y a los exponentes por sus valiosas aportaciones.

En primer lugar, el Japón desea expresar su determinación de promover un ciberespacio libre, justo y seguro. En los últimos años, hemos asistido a una tendencia preocupante del aumento cualitativo y cuantitativo de las ciberoperaciones utilizadas con fines malintencionados, incluidos los ataques de *ransomware*, los daños a infraestructuras críticas, la injerencia en elecciones democráticas y el robo de datos confidenciales. El aumento alarmante del robo de criptomonedas también supone una amenaza clara y actual para la paz y la seguridad internacionales, ya que con ellas se pueden financiar programas de armamento ilícito. En particular, es de sobra conocido que Corea del Norte está financiando sus programas de armas de destrucción masiva y misiles balísticos mediante operaciones cibernéticas malintencionadas, y la comunidad internacional debe abordar urgentemente esas amenazas, como informó el Grupo de Expertos del Comité establecido en virtud de la resolución 1718 (2006). Además, la proliferación de herramientas comerciales de ciberintrusión, como los programas espía, suscita una enorme preocupación por su repercusión en la seguridad nacional, los derechos humanos y la paz y la seguridad internacionales. Nunca ha habido tanto en juego.

Para hacer frente a esos retos alarmantes y garantizar un ciberespacio libre, justo y seguro, debemos defender el estado de derecho en el ciberespacio promoviendo debates concretos sobre la aplicación del derecho internacional vigente y la implementación de las normas, las reglas y los principios acordados sobre el comportamiento responsable de los Estados. También debemos conceder gran importancia al intercambio de información sobre las amenazas potenciales existentes, al intercambio de buenas prácticas y al fomento de los esfuerzos encaminados a la creación de capacidad. Mediante el diálogo a todos los niveles, debemos tratar de fomentar la confianza, minimizar las amenazas y, lo que es más importante, reducir los errores de cálculo. En el marco de las Naciones Unidas, el Japón proseguirá con su participación constructiva en el actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. El Japón también considera que, ya que es un marco orientado a la acción, 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 debe servir como futura plataforma permanente para apoyar la aplicación de las normas, las reglas y los principios acordados del comportamiento responsable de los Estados.

Al mismo tiempo, el Japón coincide plenamente en que el Consejo de Seguridad, principal responsable del mantenimiento de la paz y la seguridad, debe desempeñar un papel más importante y complementario en el ámbito de la ciberseguridad. El Consejo debe vigilar de cerca los incidentes cibernéticos graves que tienen graves consecuencias para la paz y la seguridad internacionales, en particular los dirigidos contra infraestructura crítica. Las sesiones informativas periódicas del Consejo resultarían sumamente útiles para mantenerse al tanto de la evolución del panorama de las amenazas a la seguridad de las tecnologías de la información y la comunicación. Además, el Consejo debe hacer frente a las crecientes amenazas cibernéticas al régimen mundial de control de armamentos y no proliferación, incluidos los riesgos de proliferación que pueden plantear los agentes no estatales.

En conclusión, el Japón reitera su determinación inquebrantable de salvaguardar un ciberespacio libre, justo y seguro. El Consejo de Seguridad debe permanecer en estado de suma alerta ante los nuevos riesgos para la seguridad asociados a las tecnologías de la información y las comunicaciones. Esperamos con interés los futuros debates sobre los próximos pasos que dé el Consejo para abordar eficazmente este importante tema sobre la base del debate de hoy, que se ha celebrado por iniciativa suya, Señor Presidente.

Dame Barbara Woodward (Reino Unido) (*habla en inglés*): Doy las gracias al Ministro de Relaciones Exteriores de la República de Corea, Sr. Cho Tae-yul, por convocar este debate y brindar al Consejo de Seguridad algunas ideas claras sobre la forma en que podemos avanzar en la labor que desempeñamos en este ámbito. También agradezco al Secretario General y a nuestros exponentes de hoy que hayan explicado cómo las ciberamenazas pueden afectar a la paz y la seguridad internacionales.

Me referiré a tres tendencias importantes para el Reino Unido.

En primer lugar, como se ha indicado, el *ransomware* puede perturbar las funciones gubernamentales y la prestación de servicios públicos vitales. Así se crean las condiciones para la inestabilidad cuando ello se produce a gran escala o durante períodos prolongados, lo que, como sabe el Consejo, puede repercutir en la paz y la seguridad. Cualquier Estado puede ser víctima del *ransomware*. Por eso es necesaria una respuesta internacional que ejerza presión sobre el ecosistema que lo facilita y permita a todos los Estados aumentar su resiliencia y capacidad de respuesta. El Reino Unido desempeña un papel destacado junto con Singapur como países que ocupan el pilar político de la Iniciativa de lucha contra el *ransomware*. Hacemos un llamamiento a todos los Estados para que se sumen a esa iniciativa.

En segundo lugar, a medida que crece el uso de sistemas de inteligencia artificial en nuestras sociedades, necesitamos comprender cómo cambiarán las ciberamenazas, al tiempo que identificamos oportunidades para que la inteligencia artificial respalde nuestros objetivos en materia de ciberseguridad. Los agentes malintencionados e irresponsables pueden explotar las vulnerabilidades de los sistemas de inteligencia artificial para promover determinados comportamientos o manipular su toma de decisiones. Para mantener la paz internacional, la seguridad de los sistemas de inteligencia artificial deberá ser una parte integral de su diseño. Esa es la razón por la que el Reino Unido celebró el año pasado, durante su Presidencia del Consejo, el primer debate sobre inteligencia artificial (véase S/PV.9381) y por la que publicamos directrices para el desarrollo seguro de sistemas de inteligencia artificial junto con los Estados Unidos y un grupo interregional de 18 Estados.

En tercer lugar, los agentes malintencionados e irresponsables también pueden aprovecharse del creciente

mercado de capacidades avanzadas de ciberintrusión, lo que plantea un panorama de amenazas más impredecible para todos nosotros. El Reino Unido y Francia invitan a los asociados internacionales a sumarse a nosotros en el Proceso Pall Mall, en el que participan múltiples partes interesadas, mientras estudiamos la manera de enfocar esa preocupación compartida.

En ese contexto, debemos seguir concienciando sobre las ciberamenazas. Por ejemplo, nos preocupa sobremanera que la República Popular Democrática de Corea lleve a cabo ciberactividades maliciosas para obtener criptomonedas, con las que financia su programa ilegal de armamento. Por eso debemos redoblar nuestros esfuerzos para garantizar la aplicación efectiva del régimen de sanciones impuesto a la República Popular Democrática de Corea.

Por último, las ciberamenazas también aumentan los riesgos de desinformación. Ello plantea claramente un reto importante para nuestra labor. Es asombroso que Rusia acuse al Reino Unido de librar una guerra de desinformación cuando su propia maquinaria de desinformación ha quedado expuesta de forma tan obvia y clara, hasta aquí, en las Naciones Unidas. No fuimos nosotros la delegación que planteó en este Salón y en Internet la teoría conspiranoica de los murciélagos y los patos usados como armas.

Las ciberamenazas presentarán cada vez más riesgos para la paz y la seguridad internacionales, y los Gobiernos deben evolucionar para hacerles frente con eficacia. Como parte de ello, el Reino Unido mantiene su determinación de defender el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio y de trabajar con otros mediante la creación de capacidades y posibilitando las asociaciones entre el sector público y el privado.

Sra. Chanda (Suiza) (*habla en francés*): Doy las gracias a la República de Corea por organizar este importante debate sobre las amenazas a la ciberseguridad. También doy las gracias al Secretario General, a la Profesora Nnenna Ifeanyi-Ajufo y al Director General de CyberPeace Institute en Ginebra, Sr. Stéphane Duguin, por sus exposiciones informativas.

Suiza está siendo testigo de dos acontecimientos decisivos en el ciberespacio que nos preocupan. Por un lado, la creciente digitalización de los conflictos y el uso de las ciberoperaciones en los conflictos armados están transformando su naturaleza. Por otro lado, a Suiza le preocupa sobremanera la intensidad creciente de los ataques con *ransomware* y de los ciberataques patrocinados por algunos Estados contra la infraestructura crítica. El uso de *ransomware* para apropiarse de divisas y criptomonedas y los ataques contra la infraestructura crítica amenazan con paralizar estructuras centrales de nuestras sociedades. Esas actividades también afectan la capacidad de la comunidad internacional para alcanzar los Objetivos de Desarrollo Sostenible, ya que los países en desarrollo son más vulnerables. También pueden suponer una amenaza para la paz y la seguridad internacionales, por lo que son competencia del Consejo.

En la nota conceptual propuesta por la República de Corea (S/2024/446, anexo), se plantea como interrogante qué papel puede desempeñar el Consejo frente a las amenazas derivadas de actividades maliciosas en el ciberespacio. Permítaseme proponer algunas opciones al respecto.

En primer lugar, el Consejo debería tomar nota periódicamente de los acontecimientos y las amenazas actuales en materia de ciberseguridad. Dadas las implicaciones multidimensionales y el alcance geográfico de la cuestión, sería conveniente que el Consejo celebrara una sesión informativa periódica. En esa sesión informativa, podrían exponer representantes de entidades de las Naciones Unidas, el sector privado, la sociedad civil y el mundo académico, así como de otras entidades pertinentes. Gracias a esa concienciación, el Consejo podría tomar decisiones con pleno conocimiento de causa, en particular sobre cuestiones geográficas específicas y en el contexto de las operaciones de mantenimiento de la paz.

En segundo lugar, el Consejo debería reafirmar ciertos principios reconocidos. Concedemos especial importancia a la aplicabilidad del derecho internacional al ciberespacio y, sobre todo, del derecho internacional humanitario a las actividades que tienen lugar en el ciberespacio en el contexto de los conflictos armados. El Consejo también debería hacer hincapié en la importancia de la responsabilidad y de la diligencia debida de los Estados, y reconocer las 11 normas de comportamiento responsable de los Estados en el ciberespacio. Esos elementos, complementados con medidas de fomento de la confianza y de creación de capacidades, constituyen el marco de comportamiento responsable de los Estados en el ciberespacio, el cual han aprobado por consenso todos los Estados Miembros. Apoyaríamos un documento del Consejo que afianzara ese marco y contribuyera así a restablecer la confianza.

Por último, las actividades del Consejo deben complementar las de otros órganos. No corresponde al Consejo fijar normas de comportamiento ni elaborar acuerdos.

Eso es prerrogativa de la Asamblea General y de los procesos de expertos que cuentan con su mandato. El Consejo debería dedicar su atención a comprender mejor los riesgos y a mitigarlos, también en casos concretos.

El uso responsable del ciberespacio ofrece vastas oportunidades para encarar los desafíos del mañana, pese a los riesgos reconocidos. En su Nueva Agenda de Paz, el Secretario General nos anima a hallar nuevas formas de protegernos de estas amenazas nuevas. Aunque las negociaciones en torno a Un Pacto para el Futuro nos brindan la oportunidad de desarrollar un entendimiento común a ese respecto, al Consejo también le corresponde desempeñar un papel decisivo. El debate de hoy así lo confirma.

Sr. Fu Cong (China) (*habla en chino*): Le agradezco, Señor Presidente, por presidir la sesión de hoy. Doy las gracias al Secretario General Guterres por su exposición informativa y a los dos expertos por sus presentaciones.

Estamos viviendo una era digital sin precedentes, en la que la revolución de la tecnología de la información avanza con rapidez, las economías digitales y las cibereconomías prosperan, y la comunidad internacional asiste a la integración acelerada de una comunidad que comparte un futuro donde se entrecruzan los intereses y se viven las mismas penas y alegrías. Al mismo tiempo, los riesgos y los desafíos en el ciberespacio son cada vez más graves. Los ciberataques, el ciberespionaje, la ciberdelincuencia y la desinformación no dan tregua. El ciberterrorismo se ha convertido en una amenaza pública mundial. El ciberespacio está cada vez más militarizado, dividido e ideologizado, y la brecha digital entre países y regiones se sigue ensanchando.

En el ciberespacio, todos los países disfrutan de las mismas oportunidades y tienen intereses comunes, pero también enfrentan los mismos problemas y asumen responsabilidades comunes. La comunidad internacional debe profundizar en los intercambios, aumentar la confianza mutua, trabajar codo a codo y promover conjuntamente la gobernanza del ciberespacio y la elaboración de normas internacionales al respecto. China desea proponer lo siguiente.

En primer lugar, necesitamos construir un ciberespacio más pacífico y seguro. El ciberespacio está muy integrado con el mundo físico y constituye un ancla importante para el desarrollo de la sociedad humana. Nunca debe convertirse en un nuevo campo de batalla. Cierto país dispone que el ciberespacio sea un ámbito para emprender operaciones militares, desarrolla cibercapacidades militares ofensivas, forja ciberalianzas militares e impulsa la definición de reglas de enfrentamiento en el ciberespacio. Ello no hará sino minar la confianza mutua entre los países, aumentar los riesgos de fricción y conflicto en el ciberespacio, y amenazar la paz y la seguridad internacionales. Todas las partes deben abandonar la mentalidad de suma cero y de guerra fría para fomentar una visión de seguridad común, integral, cooperativa y sostenible, defender con ahínco la naturaleza pacífica del ciberespacio, prevenir eficazmente la militarización y la carrera armamentista en el ciberespacio, hacer frente a las amenazas a la ciberseguridad mediante el diálogo y la cooperación, y mantener su empeño de conseguir la seguridad propia a través de la seguridad común.

En segundo lugar, necesitamos construir un ciberespacio más beneficioso y próspero para todos. Las economías digitales y las cibereconomías ya se han convertido en motores fundamentales del crecimiento económico mundial. Todos los países deben adoptar políticas más activas, abiertas, coordinadas e inclusivas, promover la aplicación y la popularización de las tecnologías de la información y las comunicaciones, y garantizar la apertura, la estabilidad y la seguridad de la cadena industrial de esas tecnologías, de modo que más países y personas puedan disfrutar de los dividendos de Internet. Los países desarrollados deben ayudar a los países en desarrollo a potenciar un desarrollo digital que sea inteligente y esté impulsado por Internet, mejorar la capacidad de los países en desarrollo para prevenir riesgos y dar respuesta a emergencias, y garantizar un acceso equitativo a recursos indispensables —como las tecnologías ligadas a la infraestructura cibernética y la potencia computacional— para minimizar la brecha digital y aplicar los Objetivos de Desarrollo Sostenible de la Agenda 2030 para el Desarrollo Sostenible. La práctica de formar camarillas siguiendo líneas ideológicas, exagerar el concepto de seguridad nacional, erigir un telón de acero digital, buscar la dominancia tecnológica y tratar de obtener ventajas en ese ámbito, e incluso interferir y suprimir con descaro el desarrollo económico y tecnológico de otros países solo conseguirá obstaculizar los esfuerzos de la comunidad internacional por promover la gobernanza del ciberespacio.

En tercer lugar, necesitamos construir un ciberespacio más equitativo y ordenado. El establecimiento de normas internacionales sobre el ciberespacio que sean aceptables para todos es clave para mantener una paz y una estabilidad duraderas en el ciberespacio. Todas las partes deben acatar seriamente los propósitos y principios de la Carta de las Naciones Unidas, en

particular la igualdad soberana, la no injerencia en los asuntos internos, la abstención del uso o de la amenaza del uso de la fuerza y el arreglo pacífico de controversias, y cumplir y aplicar el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. A su vez, todas las partes deben defender siempre el papel de las Naciones Unidas como canal principal y, sobre la base de una participación igualitaria y amplia, traducir el consenso internacional de larga data en normas de comportamiento jurídicamente vinculantes para el ciberespacio. Las soluciones constructivas propuestas por China, como la Iniciativa Mundial para la Gobernanza de la Inteligencia Artificial y la Iniciativa Mundial sobre Seguridad de los Datos, pueden servir de modelo para la futura elaboración de normas sobre el ciberespacio.

En cuarto lugar, es preciso construir un ciberespacio más igualitario e inclusivo. La diversidad es la característica fundamental del mundo y un motor del progreso humano. Internet conecta a todos los países, pueblos y civilizaciones de un modo inédito y, naturalmente, debería convertirse en una plataforma importante para que toda la humanidad muestre las diversas culturas y promueva el desarrollo y la herencia de las civilizaciones. Tenemos que aprovechar plenamente las TIC, intensificar los intercambios en línea en el diálogo, fomentar la comprensión mutua y la amistad entre los pueblos de todos los países, promover la tolerancia y la coexistencia entre las distintas civilizaciones y promover mejor los valores compartidos de la humanidad. Debemos estar alerta contra la práctica de un pequeño número de países de imponer sus propios valores como valores universales, e incluso interferir en los asuntos internos de otros países y perturbar su desarrollo y estabilidad. Debemos oponernos de manera resuelta al uso del ciberespacio para difundir el extremismo, el terrorismo, la desinformación y el discurso de odio.

China es testigo y beneficiaria del desarrollo de Internet. Hoy alberga a casi 1.100 millones de usuarios de Internet. Hemos construido la mayor y más avanzada ciberinfraestructura tecnológica del mundo y hemos puesto en marcha un sólido sistema de políticas para la gobernanza del ciberespacio. En los últimos años, China ha estado incrementando activamente su comunicación política y el intercambio de experiencias con el Sur Global; promoviendo la cooperación práctica en la creación de capacidades en ámbitos como la infraestructura, la tecnología, el cumplimiento de la ley y la respuesta a emergencias; participando con dinamismo en los procesos de ciberseguridad en marcos como el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso; el Grupo de los 20; el Foro de Cooperación Económica de Asia y el Pacífico; el grupo del Brasil, Rusia, la India, China y Sudáfrica; la Organización de Cooperación de Shanghái y el Foro Regional de la Asociación de Naciones de Asia Sudoriental, entre otros; y aportando importantes contribuciones al fomento de la gobernanza mundial del ciberespacio.

La revolución de la información, como tendencia de los tiempos, avanza a pasos agigantados. El ciberespacio evoca la infinita esperanza de la humanidad de un futuro brillante. China está dispuesta a colaborar con la comunidad internacional para construir un ciberespacio más pacífico, seguro, abierto, cooperativo y ordenado, y a aunar esfuerzos para construir una comunidad con un futuro compartido en el ciberespacio.

Sr. De La Gasca (Ecuador): Quiero saludar la presencia del Ministro de Relaciones Exteriores de la República de Corea, Sr. Cho Tae-yul. Agradezco también al Secretario General António Guterres por la información proporcionada y a los exponentes, Sr. Stéphane Duguin y Sra. Nnenna Ifeanyi-Ajufo, por sus exposiciones informativas.

En un mundo cada vez más interconectado e interdependiente, la seguridad cibernética es un desafío global, que requiere una respuesta coordinada y cooperativa de toda la comunidad internacional.

El uso malintencionado de las tecnologías de la información y las comunicaciones (TIC) actúa como un multiplicador de amenazas a la paz y la seguridad, incluidos los siguientes ámbitos.

En primer lugar, puede afectar infraestructuras críticas, como sistemas de salud, servicios financieros y redes de energía, que son esenciales para el funcionamiento de las sociedades.

En segundo lugar, puede difundir desinformación y mensajes de odio, polarizando aún más las sociedades y potenciando conflictos.

En tercer lugar, puede apoyar actividades terroristas y financiar actividades ilícitas de actores estatales y no estatales.

A la luz de estos retos, el Consejo de Seguridad no debe quedar rezagado ante la evolución de las amenazas en el ciberespacio, pues están interconectadas con varios temas de agenda de este órgano, incluidas la no proliferación y la lucha contra el terrorismo. En este sentido,

el Consejo de Seguridad debe evaluar la posibilidad de incorporar en sus productos elementos relacionados con la ciberseguridad, de acuerdo con las necesidades en cada expediente. Un ejemplo es el fortalecimiento de las comunicaciones estratégicas en operaciones de paz y en misiones políticas especiales.

La promoción de un espacio cibernético seguro, abierto y pacífico requiere normas de comportamiento responsable en el uso de las TIC. Adicionalmente, el desarrollo del derecho internacional en este ámbito debe estar acompañado del fortalecimiento de las capacidades, en particular, en los países en situación de conflicto, pues son los más susceptibles de sufrir el uso indebido de las TIC. El grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso se encuentra avanzando en este marco. El producto de sus labores podría servir de guía para los trabajos del Consejo.

Concluyo recordando la necesidad de preservar y promover un uso responsable del ciberespacio para garantizar su estabilidad y seguridad, y de esta manera, disminuir el riesgo sustancial que supone para las naciones.

Sr. De Rivière (Francia) (*habla en francés*): Doy las gracias al Secretario General, al Sr. Duguin y a la Sra. Ifeanyi-Ajufo por sus exposiciones informativas, y a usted, Señor Presidente, por haber organizado este debate.

La expansión de las tecnologías de la información y las comunicaciones está contribuyendo al progreso y a la consecución de los Objetivos de Desarrollo Sostenible. Sin embargo, también plantea desafíos importantes a nuestra seguridad colectiva. En las sociedades que dependen en gran medida de esas tecnologías, las ciberactividades maliciosas han seguido creciendo en frecuencia, gravedad y sofisticación. Pueden explotar numerosas vulnerabilidades y utilizar vectores cada vez más diversos, que ahora son accesibles a múltiples actores. Las herramientas y servicios de intrusión se extienden sin control por los mercados, y su uso irresponsable contribuye al aumento de las ciberamenazas.

Los ciberataques pueden constituir, en sí mismos, amenazas a la paz y la seguridad internacionales por su impacto en infraestructuras críticas y los riesgos de escalada que conllevan. Así, los ataques de *ransomware*, que según las autoridades francesas aumentaron un 30 % en 2023, pueden afectar a sectores esenciales como el energético, desestabilizar las economías e incluso perturbar el funcionamiento de las instituciones gubernamentales. Los ciberataques se están llevando a cabo en el contexto de conflictos armados, como vimos en los ataques llevados a cabo por Rusia contra la red de satélites Viasat en las primeras horas de su invasión ilegal de Ucrania.

Las ciberactividades malintencionadas también pueden alimentar otras amenazas a la paz y la seguridad internacionales, incluida la proliferación. El informe más reciente del Grupo de Expertos del Comité establecido en virtud de la resolución 1718 (2006) (S/2024/215) indica que los programas ilegales de armas de destrucción masiva del régimen norcoreano se financiaron hasta en un 40 % por medios cibernéticos ilícitos, como el *ransomware* o los robos de criptomoneda.

No obstante, las Naciones Unidas y el Consejo de Seguridad, en cumplimiento de su mandato, disponen de los medios para poner en práctica una respuesta coordinada a esas amenazas. En primer lugar, recordemos que el ciberespacio no es ni el Salvaje Oeste ni un vacío normativo. El derecho internacional, incluidos la Carta de las Naciones Unidas, el derecho internacional humanitario y el derecho internacional de los derechos humanos, es plenamente aplicable. Las normas de comportamiento responsable de los Estados se definieron por consenso, a fin de promover la cooperación, fomentar la prevención de conflictos y mejorar la estabilidad en el ciberespacio.

Francia apoya los trabajos de la Primera Comisión de la Asamblea General para seguir desarrollando ese marco normativo. A fin de apoyar su aplicación, Francia ha propuesto una estructura para un ambicioso mecanismo de programa de acción futuro para el ciberespacio. El Consejo de Seguridad debe situar el respeto del marco normativo para el comportamiento responsable de los Estados en el ciberespacio en el eje de su labor sobre las ciberamenazas y animar a los Estados a mantener sus compromisos para contribuir a la seguridad y estabilidad del ciberespacio.

Además, el Consejo de Seguridad debe seguir esforzándose por incorporar las cuestiones cibernéticas a las distintas dimensiones de su mandato. Es indispensable que el Consejo reciba, con carácter periódico, informes de expertos sobre la evolución de las ciberamenazas y sus consecuencias para la paz y la seguridad internacionales. El debate de hoy es un valioso ejemplo de ello.

El Consejo también debe seguir prestando atención al uso de medios cibernéticos para eludir los regímenes de sanciones. Las ciberactividades maliciosas emprendidas por el régimen norcoreano para financiar sus programas de armas de destrucción masiva merecen

atención constante en este sentido. Francia seguirá implicándose activamente para que el Consejo, a pesar de no haber prorrogado el mandato del Grupo de Expertos del Comité 1718, continúe vigilando las violaciones de sus resoluciones en este ámbito.

El Presidente: Tiene ahora la palabra el Excmo. Sr. Mamadou Tangara, Ministro de Relaciones Exteriores, Cooperación Internacional y Gambianos en el Extranjero de la República de Gambia, Excmo. Sr. Mamadou Tangara.

Sr. Tangara (Gambia) (*habla en inglés*): Ante todo, quiero dar las gracias a los exponentes por sus esclarecedoras observaciones y felicitar a la República de Corea por la organización de este debate.

En la actualidad, nos encontramos en una encrucijada. La era digital ha creado un tejido de conexiones, oportunidades y avances. Sin embargo, en ese mismo tejido acecha una oscuridad creciente que amenaza la paz y la seguridad internacionales. La amenaza en constante evolución de la ciberdelincuencia no es una mera cuestión de lucro económico o de datos robados. La nueva oleada de ciberamenazas plantea un desafío directo para la paz y la seguridad internacionales, lo que exige nuestra atención urgente. A ese respecto, damos gracias a la República de Corea por haber señalado a nuestra atención otra iniciativa innovadora del Consejo de Seguridad destinada a intercambiar perspectivas sustanciales sobre el tema “Mantenimiento de la paz y la seguridad internacionales: hacer frente a las amenazas cambiantes en el ciberespacio”. Como órgano encargado del mantenimiento de la paz y la seguridad internacionales, el Consejo de Seguridad no puede permanecer en silencio, y encomiamos su constante empeño por alertar sobre esta cuestión importante y compartida. Necesitamos un enfoque amplio para abordar esta amenaza en evolución.

En ese sentido, quisiera hacer tres sugerencias que pueden favorecer nuestro empeño conjunto por atajar las amenazas contra la paz y la seguridad internacionales asociadas al ciberespacio.

En primer lugar, el Consejo de Seguridad debe ser un defensor de la instauración de normas ejemplarizantes sobre la conducta responsable de los Estados en el ciberespacio, lo que se puede lograr con una labor habitual de sensibilización que propicie el debate sobre la ciberseguridad, con miras a amplificar el trabajo de los ciberforos de la Asamblea General y colaborar con los Estados Miembros para llevar esas normas a la práctica, promoviendo el desarrollo de capacidades y el intercambio de información para acabar con la actividad maliciosa.

En segundo lugar, el Consejo de Seguridad puede impulsar la rendición de cuentas en el caso de ciberamenazas contra la seguridad si promueve una mejor capacidad de los Estados Miembros para identificar a los actores maliciosos y establecer un frente unificado contra la impunidad.

En tercer lugar, el Consejo de Seguridad puede aprovechar la experiencia de otras entidades de las Naciones Unidas, como la Oficina de Asuntos de Desarme y la Oficina de Lucha contra el Terrorismo, para abordar adecuadamente las amenazas capaces de socavar la consecución sostenible de la democracia y de la paz y la seguridad internacionales. Además, la colaboración con esos organismos puede desembocar en una coordinación que evitará la duplicación de tareas y asegurará un enfoque integral idóneo.

Estas medidas, emprendidas en el marco del mandato del Consejo, no solo promoverán la paz y la seguridad internacionales sino que reforzarán otras iniciativas existentes al fomentar la sensibilización, promover la rendición de cuentas e impulsar una colaboración eficaz entre los Estados y las instituciones internacionales relacionadas. Por todo ello, el Consejo de Seguridad ocupa una buena posición para liderar la construcción de un ciberespacio más seguro y estable para todos.

Debemos elevar el debate e incorporar habitualmente la cuestión de las ciberamenazas en nuestras deliberaciones sobre conflictos regionales y expedientes temáticos. De este modo, se amplificará la labor de los foros de la Asamblea General dedicados a las cibernormas. Asimismo, debemos alentar a los Estados Miembros a que traduzcan esas normas en medidas concretas, lo que incluye el desarrollo de capacidades en materia de ciberdefensa, la promoción del intercambio de información y la disuasión de la actividad malintencionada.

Para concluir, felicito una vez más a la República de Corea por su encomiable iniciativa, que brinda a los Estados Miembros la oportunidad de participar en este debate tan importante y oportuno sobre una cuestión de interés común. El Consejo de Seguridad es central en el apoyo crítico tan necesario para mitigar y eliminar las ciberamenazas contra la paz y la seguridad internacionales.

El Presidente (*habla en inglés*): Tiene la palabra el representante de Alemania.

Sr. Lindner (Alemania) (*habla en inglés*): Alemania da las gracias a la República de Corea por su iniciativa de señalar las cuestiones de ciberseguridad a la atención

del Consejo de Seguridad. Quisiera dar las gracias también al Secretario General y a los exponentes por sus esclarecedoras contribuciones.

La comunidad internacional se ve expuesta con creciente frecuencia a incidentes de ciberactividad maliciosa, impulsados por entidades privadas o por Estados. Dichos incidentes repercuten gravemente en el mantenimiento de la paz y la seguridad internacionales. La gravedad de los ataques realizados por los ciberdelincuentes, en particular los ataques con *ransomware*, han demostrado su capacidad para poner en peligro la estabilidad de las instituciones estatales. Sociedades enteras se han visto afectadas.

Recientemente se observa una tendencia a la aparición, en el contexto de conflictos internacionales, de grupos de hacktivistas que toman como objetivo infraestructura crítica, lo cual ha erosionado la confianza en la prestación de los servicios públicos y ha atemorizado a la población civil. La creciente cooperación de una serie de agentes estatales con compañías privadas dedicadas a las tecnologías de la información, grupos de hacktivistas y ciberdelincuentes ha exacerbado los riesgos existentes. Todas esas tendencias multiplican las amenazas, dado que el ciberespacio extiende el campo de batalla convencional al centro mismo del ámbito civil.

En vista de este panorama de amenazas en intensa evolución, Alemania propone cuatro ámbitos en los que el Consejo de Seguridad podría actuar.

En primer lugar, consideramos que el Consejo de Seguridad tiene un papel importante a la hora de evaluar las amenazas, en virtud del Artículo 34 de la Carta de las Naciones Unidas, que autoriza al Consejo de Seguridad a investigar cualquier situación que pueda conducir a fricciones internacionales o dar lugar a controversias, pero también, más en general, en el sentido de que el Consejo debe examinar y analizar más a fondo los riesgos de los ciberataques para la paz y la seguridad internacionales.

En segundo lugar, el Consejo de Seguridad tiene un papel importante en la solución de controversias, basado en la plena aplicabilidad de la Carta de las Naciones Unidas al ciberespacio.

En tercer lugar, vemos posibilidades de que el Consejo de Seguridad tenga un papel sólido en el fomento de la confianza y la creación de normas. Al introducir los ciberconflictos internacionales entre los temas de los que se ocupa, investigar casos de ciberconflicto o facilitar la solución pacífica de este tipo de situaciones, el Consejo contribuirá a establecer un marco en evolución sobre la conducta responsable de los Estados en el ciberespacio. Este proceso debe estar basado en el derecho internacional y complementarse con normas de las Naciones Unidas de adhesión voluntaria y medidas de fomento de la confianza.

Finalmente, Alemania agradecería que el Consejo de Seguridad incluyera las amenazas a la ciberseguridad entre los temas de los que se ocupa. Entre otras cosas, se debe abordar la protección de las Naciones Unidas frente a ciberataques malintencionados, en particular en la presencia sobre el terreno, como es el caso de las operaciones de mantenimiento de la paz.

Para concluir, quisiera subrayar que Alemania seguirá contribuyendo al debate internacional sobre esta importante cuestión. Por poner un ejemplo, el año pasado pusimos en marcha un formato de diálogo global sobre las cuestiones cibernéticas y el conflicto. El objetivo es abordar los crecientes riesgos que el uso de ciberherramientas en los conflictos internacionales plantea para la población civil, ejercer una labor de sensibilización y plantear posibilidades de mitigación. El próximo acto de esta serie tendrá lugar el 8 de julio en Nueva York, en la German House, con la colaboración del Japón, el Senegal y el Comité Internacional de la Cruz Roja.

El Presidente (*habla en inglés*): Tiene la palabra el representante de los Emiratos Árabes Unidos.

Sr. Sharaf (Emiratos Árabes Unidos) (*habla en inglés*): Doy las gracias a su Excelencia el Ministro de Relaciones Exteriores Cho Tae-yul por presidir este debate abierto y felicito a la República de Corea por su papel al frente del Consejo de Seguridad en este mes. Doy las gracias también al Secretario General y a los demás exponentes por sus valiosas contribuciones.

Como hemos escuchado hoy, las amenazas contra el ciberespacio evolucionan con rapidez. Se están utilizando ciberherramientas y cibertécnicas maliciosas, como el *ransomware*, el *phishing* y la denegación de servicio, para atacar redes gubernamentales y del sector privado, lo que pone en peligro la infraestructura crítica y la seguridad pública. Esta situación resulta especialmente preocupante en un momento en el que nuestras naciones, entre ellas los Emiratos Árabes Unidos, están pasando por una transformación digital que nos hace más dependientes de la seguridad de los sistemas en línea. Las instituciones educativas están también en peligro, ya que los agentes maliciosos toman como objetivo infraestructura digital educativa y valiosos activos de información. Además, el uso malintencionado

de las tecnologías de la información y la comunicación, incluidas, entre otras, tecnologías emergentes como la inteligencia artificial (IA), multiplica las amenazas en los conflictos existentes.

Como centro mundial de tecnología e innovación, los Emiratos Árabes Unidos crearon el Consejo de Ciberseguridad en 2020. El objetivo del Consejo es lograr una transformación digital más segura y mejorar la ciberseguridad en el país para todos los sectores destinatarios. Tenemos la determinación de crear capacidad e intercambiar información con nuestros asociados, así como de promover el diseño responsable de la tecnología y el uso de la IA para el bien a fin de luchar contra la propagación y amplificación del discurso de odio, la información errónea y la desinformación. En consonancia con ese empeño, en diciembre de 2023 organizamos, junto con Albania, una sesión con arreglo a la fórmula Arria para abordar esos retos.

Teniendo eso presente, quisiera referirme a cuatro elementos que deben ser objeto de examen.

En primer lugar, el derecho internacional debe orientar el uso de las cibertecnologías. Deben respetarse la Carta de las Naciones Unidas, la soberanía, la no injerencia en los asuntos internos de los Estados, la responsabilidad de los Estados y el derecho de los conflictos armados, incluidas las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio. Para colmar las brechas normativas es necesario que exista una convergencia constante sobre cómo defender y mantener el derecho internacional en el ciberespacio.

En segundo lugar, los Emiratos Árabes Unidos apoyan la integración de las preocupaciones cibernéticas en la labor del Consejo sobre la paz y la seguridad internacionales. Eso puede incluir la mención con mayor periodicidad de las preocupaciones, tendencias y novedades relacionadas con la cibernética en las sesiones informativas, las declaraciones y las cuestiones prioritarias, así como en relación con los expedientes específicos de cada país y otros expedientes temáticos. Por ejemplo, en la resolución 2341 (2017) se reconoce la necesidad de proteger las infraestructuras críticas contra los ataques terroristas, incluida la ciberseguridad, y se subraya la necesidad de abordar mejor el amplio espectro de ciberamenazas que la digitalización y el ciberespacio conllevan.

En tercer lugar, el Consejo debe examinar la posibilidad de convocar una sesión informativa anual sobre las amenazas tecnológicas emergentes y sus consecuencias para la paz y la seguridad internacionales. Además, la publicación de un informe anual sobre ciberseguridad por parte del Secretario General proporcionaría una evaluación exhaustiva del panorama mundial de las ciberamenazas y recomendaciones para mejorar la cooperación internacional. En el informe también se debería incluir un análisis de género para responder mejor a las amenazas en el ciberespacio que se dirigen contra las mujeres y las niñas.

En cuarto lugar, el fomento de asociaciones público-privadas sólidas es crucial para aprovechar la experiencia y los recursos a fin de contrarrestar eficazmente las ciberamenazas. Los Emiratos Árabes Unidos se comprometen a colaborar con el sector privado para idear herramientas de ciberseguridad sólidas y crear capacidades nacionales e internacionales, además de apoyar al sector privado para garantizar la concepción segura y responsable de sus soluciones.

Aprovechar las cibertecnologías es crucial para nuestro futuro, pero, ante sus riesgos, es esencial la vigilancia. La cooperación internacional y la creación de capacidades son vitales para la resiliencia de la seguridad mundial. Los Emiratos Árabes Unidos seguirán promoviendo un comportamiento responsable en el ciberespacio y velando por que ese comportamiento refleje nuestras aspiraciones colectivas de paz y seguridad.

El Presidente (*habla en inglés*): Tiene ahora la palabra la representante de Letonia.

Sra. Melbārde (Letonia) (*habla en inglés*): Letonia quisiera expresar su gratitud a la República de Corea por haber organizado este debate abierto de alto nivel del Consejo de Seguridad. También quisiéramos dar las gracias al Secretario General, al exponente de CyberPeace Institute y a la exponente de la Universidad Leeds Beckett por sus presentaciones esclarecedoras.

El uso y la dependencia de la tecnología digital han aumentado considerablemente desde que las cuestiones relacionadas con la ciberseguridad se incluyeron por primera vez en la agenda de las Naciones Unidas hace más de 20 años. Hoy en día, el ciberespacio se ha convertido en el tejido conectivo del desarrollo económico y social mundial. Aunque ofrece grandes oportunidades de progreso, la expansión del ciberespacio también se ha visto asociada a riesgos y retos cada vez mayores. En los últimos años, hemos observado diversas tendencias negativas en relación con la paz y la seguridad internacionales. Cada vez son más los casos en los que las infraestructuras críticas, en particular infraestructuras de información críticas, son objeto de ciberataques, lo

cual conlleva la amenaza de consecuencias catastróficas en el mundo real. Además, hemos visto cómo los ciberataques se han convertido en parte integrante de la agresión a gran escala de Rusia contra Ucrania.

Las ciberamenazas se asocian a menudo a otros actos hostiles, como la difusión de desinformación y la información errónea y el uso malicioso de la inteligencia artificial y otras tecnologías emergentes. La ciberdelincuencia también está muy extendida, y los pagos por programas de *ransomware* han alcanzado una cifra récord en 2023. Esa evolución tiene efectos para la paz y la seguridad mundiales. La comunidad mundial debe coordinar su respuesta, y el Consejo de Seguridad tiene un papel que desempeñar de conformidad con su mandato.

Por consiguiente, Letonia considera que las amenazas y los retos del ciberespacio merecen ser objeto de un examen periódico en el Consejo. Esas deliberaciones podrían basarse en un informe periódico del Secretario General. Aumentando la atención del Consejo a la ciberseguridad también se puede facilitar la integración de los aspectos relacionados con la ciberseguridad en otros mandatos temáticos, como el mantenimiento de la paz y las mujeres y la paz y la seguridad. El Consejo debe igualmente prever el fortalecimiento de su capacidad de respuesta ante ciberataques a gran escala que puedan tener consecuencias para la seguridad internacional.

Es evidente que desarrollar un papel más sólido del Consejo para tratar las cuestiones de ciberseguridad no es algo que pueda lograrse de la noche a la mañana. Se trata de un esfuerzo paulatino, y sesiones como la de hoy desempeñan un papel fundamental para facilitar ese proceso. También está claro que el Consejo no debe sustituir la labor que ya se lleva a cabo en otros formatos de las Naciones Unidas en el marco de la Asamblea General. Muy al contrario: el Consejo debe fortalecer los acuerdos concluidos en esos formatos, en particular la aplicabilidad del derecho internacional en su integralidad al ciberespacio. También hay que seguir trabajando de manera colectiva en la aplicación del marco de comportamiento responsable de los Estados en el ciberespacio. En previsión de la creación de un mecanismo permanente de las Naciones Unidas para abordar la ciberseguridad, conocido como 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, vemos que existe potencial para que entre el Consejo y la Asamblea General se generen nuevas sinergias en este ámbito.

Para concluir, quisiera destacar el empeño de Letonia de seguir apoyando los esfuerzos en las Naciones Unidas para hacer frente a las amenazas y los desafíos cada vez mayores en materia de ciberseguridad. Hemos participado activamente en las deliberaciones sobre ese tema en las Comisiones de la Asamblea General, y también seguiremos abogando por un papel de mayor peso del Consejo.

El Presidente (*habla en inglés*): Tiene ahora la palabra la representante de Egipto.

Sra. Rizk (Egipto) (*habla en inglés*): Egipto concede gran importancia a los aspectos de la seguridad internacional de las tecnologías de la información y las comunicaciones (TIC) y exhorta encarecidamente a las Naciones Unidas a que desempeñen un papel central y de liderazgo en la promoción y la elaboración de normas y principios para la utilización de las TIC mediante un proceso inclusivo y equitativo en el que participen todos los Estados.

Una serie de Estados están desarrollando capacidades en materia de las TIC para el caso de usos malintencionados y fines militares ofensivos. La utilización de las TIC en futuros conflictos entre Estados se está convirtiendo en una realidad, y el riesgo de ataques dañinos de las TIC contra infraestructuras críticas es real y grave. Esa nueva carrera armamentista tiene repercusiones de gran alcance para la paz, la seguridad y la estabilidad internacionales, sobre todo porque las fronteras que separan las armas convencionales de las no convencionales siguen desdibujándose.

Además, las tecnologías pertinentes desarrolladas por los Estados están siendo transferidas, copiadas y reproducidas por terroristas y delincuentes. El uso malicioso de las TIC por parte de organizaciones terroristas y delictivas constituye una amenaza grave para la paz y la seguridad internacionales, sobre todo a la luz de los retos relacionados con la atribución. En virtud del derecho internacional y de la Carta de las Naciones Unidas, todos los Estados Miembros deben abstenerse de todo acto que, de manera deliberada o intencionada, dañe o comprometa el uso y el funcionamiento de las infraestructuras críticas de otros Estados o cause injerencia en sus asuntos internos. No cabe duda de que los aspectos de la seguridad internacional de las TIC se han vuelto demasiado importantes y estratégicos como para prescindir de normas vinculantes claras a nivel internacional en la materia. Un proceso inclusivo en el sistema de las Naciones Unidas es la mejor y más eficiente manera de establecer acuerdos que sean equitativos, exhaustivos y eficaces en ese ámbito.

Las Naciones Unidas ya han adoptado algunas medidas encaminadas a crear un marco normativo que complemente los principios del derecho internacional. Al aprobarse por consenso dos informes anuales sobre la marcha de los trabajos del grupo de trabajo de composición abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones, creado en virtud de la resolución 75/240 de la Asamblea General, y de otros informes consensuados de procesos relacionados con las Naciones Unidas, la Organización ya ha establecido los elementos iniciales de un marco para la prevención de conflictos y la estabilidad en el ciberespacio.

La Asamblea General hizo un llamamiento a los Estados Miembros para que, en su uso de las TIC, se orienten por el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el ciberespacio contenido en los informes consecutivos de los Grupos de Expertos Gubernamentales dependientes de la Primera Comisión. Sin embargo, la aplicación de esas normas sigue siendo, en el mejor de los casos, mínima, debido a su carácter facultativo y a la falta de un mecanismo de seguimiento.

Al tiempo que se reconocen los progresos logrados en el grupo de trabajo de composición abierta creado en virtud de la resolución 75/240 de la Asamblea General sobre diferentes aspectos de su mandato, es importante que el Grupo siente las bases para un futuro mecanismo, bajo los auspicios de las Naciones Unidas, que esté orientado a la acción, sea unidireccional, se base en el consenso y sea inclusivo. Debe aprovechar los resultados acordados de los procesos relacionados con las Naciones Unidas y centrarse en la aplicación de los resultados acordados, incluido el marco de comportamiento responsable de los Estados en el ciberespacio, seguir desarrollando ese marco y promover la cooperación internacional con los países en desarrollo y la asistencia a los mismos.

Los procesos inclusivos en las Naciones Unidas, principalmente bajo los auspicios de la Asamblea General, son la forma más eficiente de crear acuerdos equitativos, globales y eficaces en ese ámbito. Se alienta al Consejo de Seguridad a que, por su parte, tenga en cuenta las oportunidades que ofrecen las tecnologías emergentes cuando examine temas como el mantenimiento de la paz y la lucha contra el terrorismo. No obstante, el Consejo no debe utilizarse como un órgano legislativo que trata de establecer normas y reglas en nombre de los Estados Miembros de las Naciones Unidas sobre asuntos que requieren necesariamente procesos inclusivos y transparentes.

Las recomendaciones refrendadas por consenso por la Asamblea General pueden constituir la base de normas política o jurídicamente vinculantes, sobre todo teniendo en cuenta que se derivan de los principios del derecho internacional y de la Carta de las Naciones Unidas. Aunque creemos que el derecho internacional y los principios de la Carta de las Naciones Unidas se aplican a todos los ámbitos, incluido el ciberespacio, también creemos que existe una necesidad apremiante de definir obligaciones específicas que hagan que el comportamiento de los Estados en el ciberespacio se ajuste al derecho internacional y a los objetivos y principios de la Carta de las Naciones Unidas.

En un mundo cada vez más conectado, cualquier régimen internacional de ciberseguridad será tan fuerte como su eslabón más débil. Felizmente, existe consenso sobre la necesidad de intensificar y redoblar los esfuerzos de capacitación para prevenir posibles ataques contra infraestructuras críticas y desarrollar las capacidades y habilidades técnicas necesarias en los países en desarrollo. Las Naciones Unidas deben liderar un esfuerzo coordinado destinado a prestar la ayuda necesaria a países en desarrollo.

En conclusión, las TIC ofrecen oportunidades y desafíos inmensos, y destacamos que existe una necesidad apremiante de definir y desarrollar normas para un comportamiento responsable de los Estados con el fin de aumentar la estabilidad y la seguridad en el entorno mundial de las TIC y evitar que el ciberespacio se convierta en un nuevo escenario de conflictos y carreras armamentistas.

El Presidente (*habla en inglés*): Deseo recordar a todas las delegaciones que deben limitar sus declaraciones a un máximo de tres minutos a fin de que el Consejo pueda llevar a cabo su labor con diligencia. Transcurridos los tres minutos, la luz de los micrófonos parpadeará para indicar a las delegaciones que deben concluir sus intervenciones.

Tiene ahora la palabra la representante de Ucrania.

Sra. Hayovyshyn (Ucrania) (*habla en inglés*): Agradecemos a la Presidencia del Consejo de Seguridad de la República de Corea la convocatoria de este debate abierto de alto nivel. También agradecemos al Secretario General y a los demás exponentes sus observaciones.

Ucrania se suma a la declaración que formulará la Unión Europea y quisiera hacer algunos comentarios en representación nacional.

Tenemos el pleno convencimiento de que el Consejo de Seguridad desempeña un papel importante

para hacer frente a las amenazas a la paz y la seguridad internacionales, en particular en el ciberespacio. El panorama de las ciberamenazas sigue evolucionando y se ha vuelto más lleno de retos que nunca. El *ransomware* ha supuesto un riesgo cada vez más común e importante para Gobiernos, empresas y particulares. Además, asistimos en la actualidad a un aumento del número de ciberoperaciones maliciosas que se dirigen contra infraestructuras críticas e infraestructuras de información críticas, incluidos el sector energético, los servicios públicos y los procesos electorales. Algunos agentes estatales siguen socavando el orden internacional basado en normas y el marco de comportamiento estatal responsable en el ciberespacio al llevar a cabo ciberactividades maliciosas.

A ese respecto, la República Popular Democrática de Corea ha participado en actividades de ciberespionaje y robo de criptomoneda, con el objetivo de seguir desarrollando sus programas nucleares y de armas de destrucción masiva, en violación de las resoluciones pertinentes del Consejo de Seguridad. Recientemente, el grupo de ciberespionaje APT28 de Rusia llevó a cabo ciberataques contra una serie de Estados miembros de la Unión Europea.

Ucrania ha afrontado la agresión de Rusia, también en el ciberespacio. Desde el comienzo de la guerra, los ciberataques de Rusia se han vuelto más sofisticados y se han dirigido contra organismos gubernamentales y de seguridad, empresas e instituciones financieras. Los ciberdelincuentes de Moscú han llevado a cabo ataques de *phishing*, ciberespionaje y ataques contra infraestructuras críticas, además de difundir desinformación y propaganda.

A fin de prevenir, combatir y mitigar eficazmente las ciberamenazas, Ucrania coopera activamente con asociados internacionales para desarrollar una creación de cibercapacidad efectiva, fundamental para el ejercicio del derecho de legítima defensa en el ciberespacio. Además, Ucrania también ha empezado a investigar y enjuiciar los ciberataques como crímenes de guerra.

Los Estados deben cumplir sus promesas y obligaciones internacionales, en especial en el contexto de la seguridad del uso de las TIC. Como reiteramos aquí, en las Naciones Unidas, el derecho internacional, incluida la Carta de las Naciones Unidas, es aplicable en el ciberespacio. Por lo tanto, todos los agentes estatales que se comporten de manera contraria al marco acordado deben rendir cuentas.

Para concluir, alentamos a los Estados Miembros de las Naciones Unidas a que sigan trabajando de consuno en el fortalecimiento y la aplicación del marco normativo del comportamiento responsable de los Estados en el ciberespacio, la sensibilización y el intercambio de mejores prácticas en respuesta a las amenazas existentes y emergentes en el ciberespacio.

El Presidente (*habla en inglés*): Tiene ahora la palabra el representante de Estonia.

Sr. Tammsaar (Estonia) (*habla en inglés*): Acogemos con agrado el intercambio de puntos de vista de hoy y damos las gracias a los exponentes, al Secretario General en particular, por sus perspectivas valiosísimas.

Letonia hace suya la declaración que formulará la representante de la Unión Europea. Permítaseme formular algunas observaciones en representación de mi país.

No podemos ignorar la creciente sofisticación y los daños causados por ciberincidentes maliciosos de los que tanto agentes estatales como no estatales son responsables. Debido al alto nivel de sus objetivos, como infraestructuras críticas, instituciones financieras y procesos democráticos, el carácter transfronterizo de los incidentes y el aumento de las capacidades, los ciberataques pueden causar daños cada vez mayores. Por lo tanto, la ciberseguridad forma claramente parte de los retos de seguridad tanto nacionales como internacionales, y prevenir y mitigar esas amenazas es nuestra prioridad común.

La agresión de Rusia contra Ucrania ha puesto de relieve cómo las ciberoperaciones se entrelazan con los actos de guerra cinética. Hemos sido testigos de cómo las infraestructuras críticas ucranianas son objetivo de Rusia, en violación del derecho internacional humanitario. Los actos de Rusia han puesto de relieve la necesidad de centrarse en un enfoque amplio de la defensa nacional y la seguridad interior. A fin de fortalecer la preparación y la resistencia de Ucrania a los ciberataques, Estonia ha prestado un apoyo activo a Ucrania en el ciberespacio de forma bilateral, así como a través del Mecanismo de Tallin y la Coalición en favor de la tecnología de la información.

También nos preocupan profundamente las noticias más recientes procedentes de Pyongyang, que sugieren que la cooperación militar de la República Popular Democrática de Corea con Rusia se ha seguido intensificando, en flagrante violación de las resoluciones correspondientes del Consejo de Seguridad. Estonia condena con firmeza las actuales actividades cibernéticas maliciosas perpetradas por la República Popular Democrática de Corea, cuyo objetivo es alimentar el programa

armamentista de la República Popular Democrática de Corea, desestabilizar la seguridad regional y amenazar la paz mundial.

El marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio se basa en el derecho internacional vigente. El derecho internacional —en particular la Carta de las Naciones Unidas, el derecho de la responsabilidad del Estado, el derecho internacional de los derechos humanos y el derecho internacional humanitario— se aplica plenamente a las ciberoperaciones. Tenemos que trabajar de consuno para defender el derecho internacional y garantizar que también se cumpla en el ciberespacio. Para respaldar la aplicación del marco de comportamiento responsable de los Estados en el ciberespacio, Estonia aboga por establecer un programa de acción inclusivo y orientado a la acción como estructura única permanente tras la conclusión del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso en 2025.

No se puede presuponer que existe un entorno de tecnologías de la información y la comunicación abierto, seguro, estable, accesible y pacífico, y este no está separado del mundo físico. Aunque la agresión de Rusia contra Ucrania ha puesto de relieve la naturaleza integrada de los ciberataques y la guerra cinética, consideramos que se trata de un patrón que también se utilizará en futuros conflictos. Por consiguiente, el Consejo de Seguridad tiene un papel importante que desempeñar a la hora de servir de foro para compartir información sobre las ciberamenazas existentes y futuras, así como para concienciar sobre las implicaciones estratégicas de la ciberseguridad, cuestión en la que Estonia ya hizo hincapié durante su mandato en el Consejo de Seguridad.

Para concluir, esa es la razón por la que Estonia encomia a la República de Corea por celebrar el debate actual en el Salón, que es el lugar adecuado. Los debates abiertos sobre ciberseguridad, como el de hoy, serán esenciales para apoyar la mejora de la ciberresiliencia nacional, regional y mundial, lo que contribuirá a la prevención y mitigación de los ciberconflictos.

El Presidente (*habla en inglés*): Tiene ahora la palabra el representante de Chequia.

Sr. Kulhánek (Chequia) (*habla en inglés*): En primer lugar, deseo dar las gracias a la República de Corea por haber organizado este debate abierto tan pertinente. Acogemos con satisfacción el debate de hoy sobre el papel que desempeña el Consejo de Seguridad en el ámbito de la ciberseguridad, en particular en lo que respecta a la aplicación del marco acordado para el comportamiento responsable de los Estados en el ciberespacio.

Huelga decir que compartimos muchas de las preocupaciones y advertencias expresadas hoy aquí. Nos preocupan especialmente los ataques a infraestructuras críticas, el ciberespionaje, los ataques de *ransomware* contra instituciones tanto públicas como privadas, incluido el sector sanitario, los robos de criptomonedas y los esfuerzos por acceder de forma reiterada a sistemas industriales críticos, no solo con fines de espionaje y de robo de propiedad intelectual, sino también con objeto de poder controlarlos de forma abiertamente hostil. El uso creciente de las tecnologías de la información y la comunicación en los conflictos armados y sus efectos nocivos sobre la población civil son alarmantes. Esos actos irresponsables ponen en peligro la paz y la seguridad internacionales, de cuyo mantenimiento es responsable el Consejo de Seguridad. Del mismo modo, el ciberespacio se utiliza cada vez más para difundir desinformación, exacerbar los conflictos sociales existentes e incluso incitar a la comisión de actos terroristas. El Consejo, junto con los foros pertinentes de las Naciones Unidas y otras organizaciones internacionales que se ocupan de la ciberagenda, debe intensificar sus esfuerzos para encontrar formas eficaces de hacer frente a esas actividades maliciosas menos evidentes en el ciberespacio. También debe trabajar para concienciar sobre la verdadera magnitud de esas amenazas y facilitar actividades que promuevan una mayor resiliencia.

En mayo, Chequia, en coordinación con Alemania y otros Estados, condenó públicamente las actividades del agente APT28 controlado por el Estado ruso, que había estado llevando a cabo una campaña de ciberespionaje de larga data en países europeos y dirigida contra instituciones gubernamentales checas. Ese tipo de actividades contravienen las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio. Seguiremos abordándolas con firmeza, junto con nuestros asociados y de conformidad con nuestras obligaciones internacionales.

La República Checa apoya plenamente un orden internacional basado en el derecho internacional que promueva un entorno de la tecnología de la información y las telecomunicaciones abierto, seguro, estable, accesible y pacífico. Reiteramos nuestro apoyo a la creación de un mecanismo permanente, de una sola vía, inclusivo y orientado a la acción bajo los auspicios de las Naciones Unidas y a la conclusión del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso

en 2025. Consideramos que el programa de acción para 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 podría actuar como un mecanismo de esa índole.

Por último, quisiera reiterar que mi país mantiene su voluntad de participar activamente en lo que debe ser una verdadera alianza mundial para hacer frente a las amenazas a la ciberseguridad del presente y del futuro. De hecho, será necesario adoptar un enfoque en el que todos nos pongamos manos a la obra. Ya hemos entablado conversaciones detalladas con varios países de África, la región indopacífica y América Latina para trazar el panorama de las amenazas en evolución y reforzar nuestra respuesta conjunta. Por ejemplo, a finales de abril, Chequia organizó en Bogotá un seminario sobre los retos actuales en el ámbito de las actividades delictivas en el ciberespacio. Agradecemos la asistencia de expertos de Colombia, Costa Rica, el Ecuador, el Salvador, Guatemala, Honduras, Panamá y la República Dominicana, que compartieron con nosotros sus valiosos conocimientos.

Le agradezco de nuevo, Señor Presidente, que me haya brindado la oportunidad de compartir los puntos de vista de mi país sobre este importante tema.

El Presidente (*habla en inglés*): Doy ahora la palabra a la Sra. Samson.

Sra. Samson (*habla en inglés*): Tengo el honor de intervenir en nombre de la Unión Europea y de sus Estados miembros. Se adhieren a esta declaración Macedonia del Norte, Montenegro, Albania, Ucrania, la República de Moldova, Bosnia y Herzegovina y Georgia, países candidatos, así como Andorra.

Le agradezco, Señor Presidente, la organización de este debate abierto de alto nivel. La Unión Europea acoge con satisfacción el debate de hoy para intercambiar puntos de vista sobre la evolución del panorama de las ciberamenazas y sus implicaciones para el mantenimiento de la paz y la seguridad internacionales.

En las declaraciones que se han formulado hace un momento se expone una amplia gama de amenazas emergentes y en evolución, desde ataques de denegación de servicio de escasa repercusión hasta ciberoperaciones y ataques a gran escala contra infraestructuras críticas. A estas preocupaciones se añaden las posibles repercusiones transfronterizas que podrían derivarse de una ciberactividad malintencionada. También observamos la difusa línea que separa las actividades delictivas de los ataques patrocinados por Estados que emplean ciberdelincuentes a sueldo, lo que dificulta aún más la ya de por sí difícil tarea de la atribución. Debemos asumir la determinación conjunta de reforzar nuestro conjunto de herramientas para la resiliencia colectiva, e invitamos a otras delegaciones a que compartan sus puntos de vista y sus experiencias.

La Unión Europea y sus Estados miembros están sumamente preocupados por la cantidad, la sofisticación y la escala de las ciberactividades maliciosas dirigidas contra las instituciones gubernamentales y los procesos democráticos. El mes pasado, Alemania comunicó que el grupo de ciberespionaje APT28, vinculado a Rusia, había accedido ilícitamente a cuentas de correo electrónico del Partido Socialdemócrata alemán. Instituciones, organismos y entidades estatales de los Estados miembros de la Unión Europea, como Chequia, Polonia, Lituania, Eslovaquia y Suecia, ya han sido objeto de los ataques del mismo agente. Hay que poner fin a esas actividades malignas.

Las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio proporcionan orientación a ese respecto. Las principales obligaciones son claras: el derecho internacional rige en el ciberespacio; se espera que los Estados respeten las normas voluntarias de comportamiento estatal; los Estados deben impedir el uso indebido de la cibernética en su territorio; y se necesitan medidas prácticas de fomento de la confianza para ayudar a reducir el riesgo de escalada y de conflicto que plantean los ciberincidentes. La Unión Europea considera que es crucial centrarse en el desarrollo y la aplicación del marco acordado para el comportamiento responsable de los Estados en el ciberespacio a fin de cumplir con nuestra responsabilidad compartida en consonancia con nuestro interés común y de proteger a todos los Estados de los riesgos de la ciberactividad maliciosa. Los Estados pueden lograr avances significativos aclarando la aplicación del derecho internacional vigente y debatiendo la puesta en práctica y la adhesión a las normas existentes de comportamiento responsable. Para que el marco acordado de comportamiento responsable de los Estados sea eficaz, debemos defenderlo juntos. Ello refuerza la importancia de establecer un mecanismo permanente, inclusivo y orientado a la acción bajo los auspicios de las Naciones Unidas. Por ello, apoyamos 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 en el contexto de la seguridad internacional y esperamos llegar a un acuerdo sobre sus modalidades este verano.

Esperamos seguir promoviendo los debates sobre este importante tema, y acogemos con satisfacción esfuerzos como este, encaminados a poner de relieve el importante papel del Consejo de Seguridad en el cumplimiento de su mandato, establecido en la Carta de las Naciones Unidas, de hacer frente a las amenazas a la paz y la seguridad internacionales, destacando las amenazas internacionales únicas y específicas que surgen en el ciberespacio. También deseamos seguir examinando la manera en que la labor conjunta futura del Consejo puede complementar eficazmente otros procesos pertinentes de las Naciones Unidas a ese respecto.

El Presidente (*habla en inglés*): Doy ahora la palabra al representante de Filipinas.

Sr. Lagdameo (Filipinas) (*habla en inglés*): Filipinas aprovecha esta oportunidad para volver a hacer hincapié en la importancia crítica de abordar las amenazas que suponen las tecnologías de la información y las comunicaciones para la seguridad internacional. El rápido avance de las tecnologías digitales plantea nuevos retos que exigen medidas inmediatas y concertadas. A ese respecto, deseamos destacar tres cuestiones clave: las tendencias en las amenazas que plantean las tecnologías de la información y las comunicaciones, las repercusiones de las ciberamenazas para la paz y la seguridad internacionales, y los ciberataques como multiplicadores de amenazas.

En primer lugar, en lo que respecta a las tendencias en las amenazas planteadas por las tecnologías de la información y las comunicaciones, el aumento de las llamadas robotizadas efectuadas mediante inteligencia artificial (IA) con la intención de cometer fraudes, la proliferación de ultrafalsificaciones y de información engañosa, y los ataques con *ransomware* presentan riesgos significativos y desafíos complejos. Para contrarrestar esas amenazas sofisticadas, es imprescindible concebir estrategias integrales. El uso malintencionado de la IA en el ciberespacio plantea riesgos insondables. Debemos dar prioridad a la evaluación de esas amenazas para desarrollar políticas sólidas en materia de ciberseguridad y garantizar el despliegue seguro de las tecnologías de IA.

En segundo lugar, en lo que respecta al impacto de las ciberamenazas para la paz y la seguridad nacionales, Filipinas ha experimentado de primera mano las consecuencias devastadoras de los ciberataques en la seguridad nacional y la confianza pública. Algunos incidentes que tuvieron lugar en el último tiempo, como la desfiguración de sitios web gubernamentales, la violación de la seguridad de los datos de instituciones críticas y el robo a gran escala de información personal, ponen de relieve la necesidad imperiosa de mejorar las medidas de ciberseguridad. Los ciberataques pueden interrumpir servicios esenciales, socavar la confianza en las instituciones y tener consecuencias socioeconómicas de gran alcance. También nos preocupan especialmente las actividades malintencionadas en la esfera de las tecnologías de la información y las comunicaciones que buscan interferir en los asuntos internos de los Estados. Observamos un presunto aumento del uso malintencionado por los Estados de campañas de información encubiertas con ayuda de las tecnologías de la información y las comunicaciones para influir en los procesos, los sistemas y la estabilidad general de otros Estados. Esos usos socavan la confianza y pueden dar lugar a escaladas y amenazar la paz y la seguridad internacionales. Otra consideración alarmante es que esas capacidades sofisticadas de las tecnologías de la información y las comunicaciones están al alcance de agentes no estatales, que son capaces de utilizarlas de forma maliciosa con fines comerciales y eludir su responsabilidad.

En tercer lugar, en cuanto al efecto multiplicador de las amenazas que caracteriza a los ciberataques, las actividades delictivas en el ciberespacio exacerban los desafíos existentes para la paz y la seguridad internacionales. Filipinas ha sido testigo de cómo los ciberataques pueden funcionar como multiplicadores significativos de las amenazas y complicar los esfuerzos por mantener la paz y la estabilidad. La naturaleza transnacional del ciberespacio significa que ningún Estado es inmune, y nuestra seguridad colectiva solo es fuerte en la misma medida que su eslabón más débil. Ante el riesgo grave que plantean las ciberamenazas, Filipinas subraya el papel fundamental del Consejo de Seguridad a la hora de hacerles frente. Aunque los debates en curso del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso son valiosos, también es imprescindible que el Consejo de Seguridad siga implicándose en la configuración de la agenda sobre ciberseguridad mundial.

A ese respecto, Filipinas es partidaria de que, para contrarrestar las ciberamenazas, el Consejo adopte las siguientes medidas colectivas, las cuales se plantearon durante la sesión sobre ciberseguridad que se celebró en abril con arreglo a la fórmula Arria. En primer lugar, se debe reforzar el marco normativo acordado de comportamiento responsable de los Estados en el ciberespacio. En segundo lugar, hay que mantener sesiones anuales para debatir y revisar el panorama de las amenazas que

plantean las tecnologías de la información y las comunicaciones y, a ese respecto, solicitar al Secretario General que prepare un informe anual sobre las tendencias que sirva de base para los debates de los Estados Miembros. En tercer lugar, es preciso tomar la iniciativa al recopilar información y estudiar amenazas o incidentes concretos para brindar orientación y recomendaciones a los Estados Miembros.

Filipinas reafirma su determinación de mejorar la ciberresiliencia y promover un comportamiento responsable en el ciberespacio. Pedimos que continúen la cooperación, los esfuerzos de creación de capacidad y los mecanismos de apoyo, entre ellos un fondo fiduciario regular para ayudar a los países en desarrollo a afrontar las ciberamenazas. Contamos con que se forjen alianzas y se transfiera tecnología para ayudarnos a reducir la brecha digital y reforzar nuestras ciberdefensas.

El Presidente (*habla en inglés*): Doy ahora la palabra al representante de Indonesia.

Sr. Nasir (Indonesia) (*habla en inglés*): Indonesia da las gracias a la República de Corea por haber convocado esta importante sesión. También damos las gracias al Secretario General y a los exponentes por sus presentaciones.

Las amenazas en el ciberespacio se han convertido en un peligro real y actual para la paz y la seguridad nacionales e internacionales. Cada vez estamos más expuestos a nuevas amenazas procedentes de las nuevas tecnologías, en rápida evolución. La comunidad internacional solo podrá mejorar la ciberresiliencia y mitigar eficazmente esos riesgos si adopta una respuesta coordinada y establece marcos jurídicos sólidos.

En ese contexto, permítaseme destacar las siguientes cuestiones.

En primer lugar, debemos dar prioridad a mitigar el costo humano de los ciberataques dirigidos contra la infraestructura crítica. Debemos velar por que el ciberespacio sea un ámbito con salvaguardias y libre de conflictos, y no un escenario de enfrentamientos. Si bien los avances en materia de inteligencia artificial (IA), que incluyen la IA generativa y el aprendizaje automático, pueden beneficiar a la raza humana, también pueden ser destructivos y facilitar los ciberataques, los cuales pueden tener repercusiones negativas considerables en la población mundial. Por lo tanto, es imprescindible proteger la infraestructura crítica como parte de nuestros esfuerzos por evitar que los ciberactores malintencionados y los Estados irresponsables causen daños importantes.

En segundo lugar, es fundamental que haya sinergia y coherencia dentro del sistema de las Naciones Unidas en los ámbitos de la ciberseguridad, las tecnologías de la información y las comunicaciones, y la paz y la seguridad internacionales. Aunque el Consejo de Seguridad tiene el importante mandato de mantener la paz y la seguridad internacionales, otros órganos de las Naciones Unidas tienen mandatos igual de importantes de trabajar en las cuestiones vinculadas a la ciberseguridad y la seguridad digital y de las tecnologías de la información y las comunicaciones. Es importante que el Consejo de Seguridad establezca parámetros y mecanismos que lo ayuden a fomentar la colaboración y la sinergia, a fin de entender mejor los riesgos que suponen las ciberamenazas para la paz y la seguridad internacionales. Indonesia reafirma así su respaldo 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, así como a otros procesos que están teniendo lugar en este ámbito, incluido el proceso de la Cumbre del Futuro.

En tercer lugar, debemos mejorar la ciberseguridad mundial reforzando la cooperación regional. La cooperación con las organizaciones regionales es necesaria, pues estas contribuyen significativamente a adoptar un enfoque sólido e integral de la ciberseguridad. En nuestra región, la Asociación de Naciones de Asia Sudoriental (ASEAN) ha desempeñado un papel decisivo en la creación de marcos e iniciativas, en algunos casos a través del Foro Regional de la ASEAN, para mejorar la resiliencia de la región frente a las ciberamenazas. Aprovechar la experiencia de las organizaciones regionales puede aportar conocimientos valiosos y promover iniciativas internacionales más holísticas.

Por último, debemos salvar la brecha tecnológica para mejorar la ciberresiliencia. El déficit de capacidad en materia de ciberseguridad es un reto crítico para los países en desarrollo, ya que los hace vulnerables a las amenazas cada vez más intensas y socava su estabilidad. Resulta crucial cooperar a todos los niveles, también con las partes interesadas pertinentes del sector privado, para reforzar la estabilidad en el ciberespacio, en particular mediante la creación de capacidades, la asistencia técnica y la transferencia de tecnología. Solo aunando esfuerzos podremos crear un ciberespacio seguro que fomente la paz y la estabilidad mundiales.

El Presidente (*habla en inglés*): Tiene ahora la palabra el representante de Singapur.

Sr. Seah (Singapur) (*habla en inglés*): Agradecemos a la República de Corea la convocatoria de la sesión de hoy sobre esta importante cuestión.

Desde el primer debate abierto del Consejo de Seguridad sobre la ciberseguridad, que tuvo lugar en junio de 2021 (véase S/2021/621), el panorama de las ciberamenazas ha seguido evolucionando a un ritmo preocupante. Con ese telón de fondo, la cooperación internacional en las Naciones Unidas es vital e indispensable para combatir la naturaleza mundial y transfronteriza del panorama de las ciberamenazas. A ese respecto, es necesario que la Asamblea General y el Consejo de Seguridad trabajen de consuno para reforzar la adhesión al marco normativo de comportamiento responsable de los Estados en el ciberespacio, con base en la aplicación del derecho internacional y el respeto de los principios de la Carta de las Naciones Unidas. Al ser un Estado pequeño, Singapur siempre ha apoyado un sistema multilateral basado en el estado de derecho. Tenemos la misma concepción en lo que respecta a la ciberseguridad, que es de vital importancia para muchos Estados pequeños y en desarrollo. Singapur cree firmemente en la importancia de las Naciones Unidas como plataforma clave para deliberar sobre el desarrollo y la aplicación de las reglas, normas y principios de comportamiento responsable de los Estados que rigen el ciberespacio.

Singapur tiene el honor de presidir, desde 2021, el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. El grupo de trabajo de composición abierta sustenta su labor en más de dos decenios de esfuerzos en las Naciones Unidas, que han dado como resultado un marco acumulativo y evolutivo de comportamiento responsable de los Estados en el ciberespacio, que ha sido refrendado por todos los Estados Miembros. Resulta alentador constatar que el grupo de trabajo de composición abierta ha conseguido progresos satisfactorios en los últimos tres años en el fortalecimiento del marco normativo de comportamiento responsable de los Estados en el ciberespacio.

El grupo de trabajo de composición abierta también constituye, en sí mismo, una valiosa medida de fomento de la confianza. Además de los entendimientos comunes que se señalan en los dos informes anuales sobre los progresos realizados del grupo de trabajo de composición abierta acordados por consenso en julio de 2022 (véase A/77/275) y julio de 2023 (véase A/78/265), respectivamente, el grupo de trabajo de composición abierta ha encabezado la formulación y la puesta en marcha de iniciativas concretas orientadas a la acción, que tienen un papel importante que desempeñar para mejorar la paz y la seguridad internacionales en el ciberespacio, en particular el directorio mundial de puntos de contacto, que se presentó oficialmente el 9 de mayo. También en mayo, el grupo de trabajo de composición abierta convocó una fructífera y sustanciosa reunión a nivel ministerial sobre la creación de capacidades en materia de seguridad de las tecnologías de la información y las comunicaciones (TIC). El mensaje clave derivado de esa reunión fue que la creación de capacidades es una necesidad urgente para ayudar a muchos países pequeños y países en desarrollo a alcanzar la ciberresiliencia. También fue importante el reconocimiento generalizado de que la creación de capacidades puede ser un medio esencial para fomentar la confianza entre los Estados.

En sus preguntas orientativas, Sr. Presidente, preguntaba cómo se interrelacionan las ciberamenazas con otros temas del programa de trabajo del Consejo de Seguridad y qué papel específico puede desempeñar el Consejo de Seguridad a la hora de abordar los desafíos que plantea el ciberespacio para la paz y la seguridad internacionales. Habida cuenta de la labor que se está llevando a cabo en la Asamblea General, es importante que el Consejo de Seguridad evite duplicar la labor que ya se está realizando en otros procesos. Al mismo tiempo, sin embargo, debemos reconocer que el Consejo de Seguridad tiene el mandato claro de examinar las cuestiones relativas al mantenimiento de la paz y la seguridad internacionales. No podemos excluir la posibilidad de que un ciberincidente cree malentendidos entre Estados y lleve a una escalada y a un posible conflicto, lo que crearía un incidente en el ámbito de la paz y la seguridad internacionales. Por lo tanto, no podemos descartar que el Consejo de Seguridad desempeñe un papel en el marco de la responsabilidad que le confiere la Carta de mantener la paz y la seguridad internacionales.

Por ello, el Consejo debe adoptar una visión inclusiva de lo que constituyen amenazas a la paz y la seguridad internacionales y actuar consciente de que las ciberamenazas pueden tener consecuencias físicas y en el mundo real. En este sentido, somos receptivos a la idea de que el Consejo de Seguridad siga convocando debates abiertos como el de hoy, como medio de intercambiar información y mejorar el entendimiento entre los Estados Miembros. Los debates del Consejo pueden contribuir a informar los trabajos de la Asamblea General, en particular en materia de fomento de la capacidad y la confianza, y a reforzar aún más el marco del comportamiento responsable de los Estados en el ciberespacio, en particular al estudiar la mejor manera de aplicar las reglas, normas y principios a las ciberamenazas existentes y potenciales.

Para concluir, permítaseme subrayar la necesidad de potenciar la cooperación internacional para reforzar

nuestra resiliencia colectiva en el ciberespacio. Promover una mayor cooperación entre el Consejo de Seguridad y la Asamblea General en cuestiones de paz y seguridad internacionales y trabajar de consuno de forma sostenida, holística y sinérgica permitirá a la comunidad internacional preservar mejor la paz y la seguridad internacionales en el ámbito del ciberespacio. Singapur está dispuesto a colaborar con todos los Estados Miembros en pos de ese objetivo.

El Presidente (*habla en inglés*): Tiene la palabra la representante de Costa Rica.

Sra. Chan Valverde (Costa Rica): Agradezco a la República de Corea por convocar este debate abierto.

Hace dos años, Costa Rica fue víctima de ataques de *ransomware* a gran escala. Todavía sentimos el impacto a largo plazo causado por las interrupciones en nuestro sistema de salud, seguridad social, finanzas y otros sectores críticos. En este sentido, Costa Rica desea plantear tres puntos hoy.

En primer lugar, Costa Rica cree firmemente que la agenda sobre la protección de los civiles debe ampliarse para abarcar las actividades cibernéticas, que afectan a la población civil durante los conflictos armados. Los Estados deben unirse al creciente consenso de que los datos civiles gozan de la misma protección bajo el derecho internacional humanitario que todos los demás objetos civiles, y que las operaciones cibernéticas que deshabilitan o impiden la funcionalidad de los sistemas civiles están prohibidas bajo el derecho internacional humanitario. Los Estados también deben evitar involucrar a civiles en actividades cibernéticas militares, ya que hacerlo puede ponerlos en grave riesgo.

En segundo lugar, Costa Rica considera que es momento de actualizar la agenda sobre las Mujeres y la Paz y la Seguridad para abordar la seguridad de las mujeres en el ámbito digital. Costa Rica hace un llamado a los miembros del Consejo para que consideren adoptar una nueva resolución que establezca medidas para proteger a mujeres y niñas de la violencia, el abuso y la explotación en línea, en especial en situaciones de conflicto y posconflicto. Las consideraciones de seguridad digital también deben integrarse de manera sistemática en todos los nuevos mandatos, objetivos e iniciativas de dicha agenda.

En tercer lugar, todos los Estados, sean miembros del Consejo o no, tienen la responsabilidad de fortalecer el estado de derecho internacional en el ciberespacio. Costa Rica es un miembro orgulloso de un creciente grupo de Estados que han expresado posiciones nacionales sobre la aplicación del derecho internacional en el ciberespacio. Estos documentos de posición se basan en el consenso global de que el derecho internacional, incluidos el derecho internacional humanitario y el derecho internacional de los derechos humanos, es aplicable al uso de las tecnologías de la información y las comunicaciones (TIC) por parte de los Estados y es esencial para mantener la paz y la estabilidad. Animamos a otros Estados a desarrollar documentos de posición y aplaudimos los recursos existentes para el desarrollo de capacidades legales, como la guía sobre derecho cibernético, que pueden orientar los esfuerzos en esta área.

Ante la creciente vulnerabilidad de nuestras sociedades a las amenazas cibernéticas y digitales, Costa Rica insta al Consejo a integrar estas preocupaciones en su trabajo y a hacerlo de manera que se mejore tanto el respeto al derecho internacional en tiempos de paz como durante los conflictos armados.

El Presidente (*habla en inglés*): Aún quedan varias intervenciones en la lista de esta sesión. Habida cuenta de lo avanzado de la hora, con la anuencia de los miembros del Consejo, suspenderé la sesión hasta las 15.00 horas.

Se suspende la sesión a las 13.10 horas.