



Consejo de Seguridad

Septuagésimo séptimo año

Provisional

9039^a sesión

Lunes 23 de mayo de 2022, a las 10.00 horas

Nueva York

Presidenta: Sra. Thomas-Greenfield (Estados Unidos de América)

Miembros:

Albania	Sr. Hoxha
Brasil	Sr. De Oliveira Marques
China	Sr. Zhang Jun
Emiratos Árabes Unidos	Sra. Nusseibeh
Federación de Rusia	Sr. Nebenzia
Francia	Sr. De Rivièrre
Gabón	Sr. Biang
Ghana	Sr. Agyeman
India	Sr. Tirumurti
Irlanda	Sr. Flynn
Kenya	Sr. Kiboino
México	Sr. Gómez Robledo Verduzco
Noruega	Sra. Juul
Reino Unido de Gran Bretaña e Irlanda del Norte	Sr. Roscoe

Orden del día

Mantenimiento de la paz y la seguridad internacionales

Tecnología y seguridad

La presente acta contiene la versión literal de los discursos pronunciados en español y la traducción de los demás discursos. El texto definitivo será reproducido en los *Documentos Oficiales del Consejo de Seguridad*. Las correcciones deben referirse solamente a los discursos originales y deben enviarse con la firma de un miembro de la delegación interesada, incorporadas en un ejemplar del acta, a la Jefatura del Servicio de Actas Literales, oficina U-0506 (verbatimrecords@un.org). Las actas corregidas volverán a publicarse electrónicamente en el Sistema de Archivo de Documentos de las Naciones Unidas (<http://documents.un.org>).

22-35748 (S)



Documento accesible

Se ruega reciclar



Se abre la sesión a las 10.05 horas.

Aprobación del orden del día

Queda aprobado el orden del día.

Mantenimiento de la paz y la seguridad internacionales

Tecnología y seguridad

La Presidenta (*habla en inglés*): De conformidad con el artículo 39 del Reglamento Provisional del Consejo, invito a los siguientes ponentes a participar en esta sesión: la Secretaria General Adjunta de Asuntos Políticos y de Consolidación de la Paz, Sra. Rosemary DiCarlo; la Directora de Advox, proyecto de Global Voices sobre derechos digitales, Sra. Nanjala Nyabola, y el Profesor Adjunto del Centro de Estudios sobre la Paz y la Seguridad Internacionales de la Universidad McGill y miembro no residente de International Peace Institute, Sr. Dirk Druet.

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

Tiene ahora la palabra la Sra. DiCarlo.

Sra. DiCarlo (*habla en inglés*): Las tecnologías digitales han transformado profundamente todas las facetas de nuestras sociedades. Ofrecen oportunidades ilimitadas para el desarrollo sostenible, la educación y la inclusión. Los medios de comunicación social, por ejemplo, han transformado la defensa de los derechos humanos y la ayuda humanitaria, haciendo posible que personas de todo el mundo se movilicen de forma rápida y eficaz en torno a cuestiones que requieren una atención urgente. Además, han generado nuevas posibilidades para nuestra labor de paz y seguridad. Los avances tecnológicos han mejorado nuestra capacidad para detectar las crisis, posicionar mejor de manera anticipada nuestras reservas humanitarias y elaborar programas de consolidación de la paz basados en datos.

En la actualidad utilizamos las tecnologías digitales en nuestra labor de prevención de conflictos, establecimiento de la paz y consolidación de la paz. Permítaseme dar a conocer un par de ejemplos.

Las herramientas digitales fortalecen nuestra capacidad de recopilación de información y de alerta temprana. En el Yemen, la Misión de las Naciones Unidas en Apoyo del Acuerdo sobre Al-Hudayda ha utilizado diversas herramientas de cartografía, sistemas de información geográfica y tecnología de satélites para mejorar

su vigilancia del alto el fuego en la provincia. Gracias a ellas ha mejorado nuestro estado de preparación para comprender, analizar y responder a las crisis que puedan tener una dimensión digital y para hacer frente a los riesgos digitales. Por ejemplo, hemos trabajado con asociados para crear una plataforma de aprendizaje electrónico sobre la gestión de riesgos digitales.

Las nuevas tecnologías pueden ser beneficiosas para apoyar los procesos políticos, especialmente para promover la inclusión. En diversas negociaciones de paz, hemos utilizado diálogos digitales asistidos por inteligencia artificial para llegar a miles de interlocutores y escuchar sus puntos de vista y prioridades. Esta ha sido una forma especialmente útil de llegar a grupos tradicionalmente excluidos, en particular las mujeres.

En Libia, la Misión de las Naciones Unidas celebró cinco diálogos digitales, cada uno de ellos con más de 1.000 participantes. Ese esfuerzo incrementó la legitimidad del proceso, ya que las diferentes comunidades se dieron cuenta de que sus voces podían ser escuchadas. En el Yemen, a través de las consultas digitales, el Envío Especial entró en contacto con centenares de mujeres de varias provincias, lo que proporcionó una perspectiva más profunda de la dimensión de género de la guerra.

El uso de las tecnologías digitales también puede mejorar la seguridad y protección de nuestro personal de mantenimiento de la paz y del personal civil sobre el terreno. El lanzamiento de la Estrategia para la Transformación Digital del Mantenimiento de la Paz de las Naciones Unidas representa un paso esencial para lograr ese objetivo, así como para aplicar más eficazmente los mandatos, aumentando de ese modo las capacidades de alerta temprana.

Por último, con esas herramientas podemos visualizar la información y transmitir un análisis rico en datos para apoyar la toma de decisiones del Consejo de Seguridad. Nuestra reciente presentación de realidad virtual ante el Consejo de Seguridad sobre Colombia muestra cómo podemos llevar nuestro trabajo sobre el terreno a la atención de este órgano de nuevas maneras.

Los beneficios de las tecnologías digitales para el mantenimiento de la paz y la seguridad internacionales son múltiples. Sin embargo, los progresos tecnológicos también han generado riesgos nuevos considerables y que pueden tener efectos nefastos en la dinámica de los conflictos. Diversas esferas son objeto de preocupación.

Según ciertas estimaciones, el número de incidentes de uso malintencionado de las tecnologías digitales

con fines políticos o militares, patrocinados o no por los Estados, casi se ha cuadruplicado desde 2015. Son especialmente preocupantes las actividades dirigidas contra las infraestructuras que prestan servicios públicos básicos, como la salud y los organismos humanitarios. Entretanto, las armas autónomas letales plantean cuestiones relativas a la responsabilidad humana por el uso de la fuerza.

Como ha señalado con claridad el Secretario General, las máquinas que tienen el poder y la discreción de segar vidas sin una intervención humana son políticamente inaceptables, moralmente repugnantes y deberían estar prohibidas en virtud del derecho internacional. Además, los agentes no estatales son cada vez más expertos en la utilización de tecnologías digitales de bajo costo y amplia disponibilidad para llevar adelante sus agendas. Grupos como el Estado Islámico en el Iraq y el Levante y Al-Qaida siguen activos en las redes sociales y utilizan plataformas y aplicaciones de mensajería para compartir información y comunicarse con sus seguidores con fines de reclutamiento, planificación y recaudación de fondos. La disponibilidad cada vez mayor de métodos de pago digitales, como las criptomonedas, plantea desafíos adicionales.

Además, las tecnologías digitales han suscitado preocupaciones graves en materia de derechos humanos, desde sistemas de inteligencia artificial que pueden ser discriminatorios hasta la disponibilidad generalizada de tecnologías de vigilancia que pueden desplegarse contra las comunidades o las personas. Asimismo, nos preocupa el uso creciente de los cortes de Internet, incluso en situaciones de conflicto activo, que privan a las comunidades de sus medios de comunicación, trabajo y participación política.

En Myanmar, por ejemplo, los cortes de Internet y de los servicios de telefonía móvil han aumentado en número y duración desde el golpe militar del 1 de febrero de 2021, en especial en las zonas de operaciones militares. Las redes sociales pueden alimentar la polarización y, en ocasiones, la violencia. El uso indebido de los medios sociales y la respuesta, a veces limitada o no del todo adecuada, de las empresas encargadas de ellos están permitiendo la propagación de la desinformación, la radicalización, el racismo y la misoginia. Ello puede agudizar las tensiones y, en algunos casos, exacerbar los conflictos. En Etiopía, a medida que se intensificaban los combates, se produjo un aumento alarmante de las publicaciones en las redes sociales que difundían un discurso incendiario, y algunas llegaban a incitar a la violencia étnica, como reconoció el

Consejo de Seguridad en su comunicado de prensa de 5 de noviembre de 2021 (SC/14691).

Hemos sido testigos de que la desinformación y el discurso de odio en Internet pueden provocar daños fuera de la red, incluso violencia. Somos conscientes de que la desinformación puede obstaculizar la capacidad de nuestras misiones para cumplir sus mandatos, al exacerbar las falsedades y alimentar la polarización. Estamos emprendiendo una serie de acciones para mitigar esos riesgos, impulsadas por la Estrategia y el Plan de Acción de las Naciones Unidas para la Lucha contra el Discurso de Odio, que puso en marcha el Secretario General, e iniciativas como Verified. Por ejemplo, en el Iraq, tras los informes sobre el aumento del acoso en línea a las candidatas en las elecciones del año pasado, la Misión de Asistencia de las Naciones Unidas para el Iraq colaboró con organizaciones de la sociedad civil para vigilar el discurso de odio, emitir informes públicos y fortalecer la educación electoral.

Debemos aprovechar al máximo las oportunidades que brindan las tecnologías digitales para fomentar la paz, pero, con ese fin, también debemos mitigar los riesgos que estas suponen y promover su uso responsable por parte de todos los agentes. Por medio de la Asamblea General, los Estados Miembros han logrado progresos importantes en el establecimiento de un marco normativo para garantizar un comportamiento responsable en el ciberespacio. Los Estados Miembros también están cooperando para elaborar y aplicar una serie de medidas de fomento de la confianza destinadas a prevenir conflictos, evitar percepciones erróneas y malentendidos y aliviar las tensiones.

No obstante, hay que hacer más para promover, elaborar y aplicar el nuevo marco normativo. En su informe titulado “Nuestra Agenda Común” (A/75/982), el Secretario General se mostró partidario de un pacto digital global con principios comunes, que permitan forjar un futuro digital abierto, libre y seguro para todos. Junto con otros aspectos de “Nuestra Agenda Común”, como la nueva agenda para la paz y el código de conducta propuesto que promueve la integridad en la información pública, tenemos una oportunidad fundamental para lograr consenso sobre cómo utilizar las tecnologías digitales en beneficio de las personas y el planeta, al tiempo que se afrontan los riesgos que plantea. Sin embargo, la acción colectiva de los Estados Miembros sigue siendo esencial para lograr ese objetivo.

La Presidenta (*habla en inglés*): Doy las gracias a la Sra. DiCarlo por su exposición informativa.

Tiene la palabra la Sra. Nyabola.

Sra. Nyabola (*habla en inglés*): Es un honor y un placer dirigirme al Consejo de Seguridad con respecto a la cuestión de la tecnología digital en relación con la paz y la seguridad. Como los miembros escucharon en la introducción, soy una investigadora que examina la confluencia de la tecnología, la sociedad y la política, con un interés específico en aumentar nuestra comprensión colectiva de los derechos digitales.

En los últimos dos decenios, hemos presenciado una expansión drástica de la utilización de la tecnología digital en todas las esferas de nuestra vida social: en los planos individual, colectivo, nacional y transnacional. Por desgracia, esa expansión no se ha complementado con una inversión similar para protegernos de los daños que esta ha creado ni con una determinación de comprender y defender los derechos del ser humano en el seno del sistema que estamos construyendo. En pocas palabras, nuestra ansia de digitalización está superando a la conciencia sobre sus repercusiones y, con las crecientes pruebas de los daños que posibilita ese enfoque desordenado, es un momento crucial para hacer balance y decidir si necesitamos cambiar o invertir nuestro modo de proceder.

Sería absurdo intentar resumir todas las consecuencias de la era digital en materia de derechos en el tiempo que se me ha concedido. Más bien, en esta exposición informativa haré hincapié en algunos de los desafíos generales que plantea la digitalización y en tres principios fundamentales, que crean oportunidades de acción para salvaguardar la paz y la seguridad.

Para comenzar, quisiera matizar mis observaciones y afirmar que hablar de la tecnología digital en relación con la paz y la seguridad no debe interpretarse como una invitación a la militarización y la titulización de Internet. Al fin y al cabo, el mandato del Consejo es preservar la paz y la seguridad, y es importante guiarse por un espíritu que esté animado tanto o más, por el deseo de una paz positiva como por el interés en la seguridad. Internet ha sido un espacio de gran innovación, creatividad y oportunidad y, al pensar en resolver los desafíos que afronta en la actualidad, deseo instar al Consejo a que tenga la determinación de preservar Internet como un bien público mundial, de la misma manera que nos guía un espíritu de cooperación al pensar en espacios como la Antártida o el espacio ultraterrestre.

No obstante, tras muchos años de optimismo tecnológico desenfrenado, nos encontramos en un momento de creciente cinismo, ya que las amenazas que se

ignoraron mientras intentábamos acelerar el progreso han empezado a hacerse realidad. En la investigación que dirijo con Advox, utilizamos una tipología sencilla para ayudarnos a dar sentido a esas amenazas, separando los dominios de la tecnología digital en cuatro categorías: datos, acceso, discurso e información.

En lo que respecta al tema de los datos, este incluye prácticas que se dirigen en concreto a la recopilación de datos, como la vigilancia o el creciente uso de la biometría. Se ha producido un aumento preocupante de la economía de la vigilancia mundial, que incluye el uso generalizado de tecnologías como Pegasus contra dirigentes políticos, periodistas y miembros de la sociedad civil. La tecnología que hace posibles esas prácticas se desarrolla en los países ricos y luego se despliega o exporta a los países pobres, sin tener en cuenta el contexto de los derechos, lo que pone en riesgo grave a quienes están a la vanguardia del fomento de la paz.

Por ello, nos sumamos a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos para abogar por una moratoria mundial sobre el desarrollo y la venta de tecnologías de vigilancia e invitamos al Consejo de Seguridad a unirse a la presión a las empresas privadas para que cumplan con esa moratoria. Del mismo modo, se registra un uso cada vez mayor de tecnologías de recopilación masiva de datos por parte de entidades estatales y no estatales, o la dataficación de nuestras vidas, sin un impulso de apoyo para protegernos o incluso concienciar sobre derechos fundamentales como la privacidad o la protección de datos. En las zonas de conflicto, la dataficación de la vida de los refugiados ha aumentado drásticamente, incluido el incremento de la recopilación y el almacenamiento de datos biométricos de los solicitantes de asilo, que se conservan en condiciones opacas y a veces se utilizan para denegar a los refugiados sus derechos o restringir sus libertades.

En la cuestión del acceso, se examinan las prácticas activas y pasivas que restringen la capacidad de las personas para acceder a Internet, desde los cortes de Internet y de las redes sociales hasta las disparidades de género y la falta deliberada de inversión en infraestructura, en detrimento de las comunidades con pocos recursos. En 2021, la organización mundial de derechos digitales Access Now documentó 182 cortes de Internet en 34 países, lo que supone un aumento respecto a los 159 cortes en 29 países que se registraron en 2020. El corte más largo de Internet duró casi tres años. El país con más cortes de Internet experimentó 109 en un solo año.

Además de los cortes de Internet, también han aumentado las prácticas conexas, como la limitación del ancho de banda y el cierre de las redes sociales, en especial en los períodos electorales. Esas interrupciones están concebidas para enfriar el discurso y la participación cívicos y son un ataque directo a la democracia y la paz.

En general, hay varios países donde las mujeres todavía se enfrentan a obstáculos sistemáticos para acceder a Internet, lo que se hizo especialmente visible cuando las escuelas de todo el mundo intentaron recurrir a la educación virtual en respuesta a la pandemia de enfermedad por coronavirus. En varios países donde la transición no se produjo de forma adecuada, las niñas se llevaron la peor parte al no poder acceder a ningún medio tecnológico disponible por ser niñas. Además, en algunos países, incluidos algunos países ricos, si bien se ha producido un aumento en la obligatoriedad de utilizar la tecnología digital para la vida cívica, entre otros, en lo relativo a los registros de nacimientos y defunciones, se ha invertido sorprendentemente poco en hacer que la infraestructura digital sea accesible para las personas con discapacidad o para las personas que hablan lenguas indígenas y no dominantes.

La cuestión del discurso se refiere a las restricciones a las libertades de expresión, información u opinión. En muchos países, las plataformas digitales conviven con las plataformas analógicas, como los medios de comunicación y las ágoras físicas, como un lugar donde la población puede reunirse, deliberar y compartir ideas sobre la forma de mejorar su sociedad. Se ha registrado un aumento drástico del uso de la legislación para restringir la capacidad de las personas de participar en ese discurso, en particular de las leyes que amplían injustamente la definición de delito de calumnia para hacer que casi todas las críticas a los funcionarios del Estado sean ilegales. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos señaló que, entre 2020 y 2021, se aprobaron por lo menos 40 leyes sobre medios sociales y 30 se encontraban en fase de examen.

Muchas de esas leyes contienen definiciones amplias de los delitos subyacentes que supuestamente abordan, que se utilizan de forma rutinaria contra los periodistas y contra quienes critican al Estado. La aprobación de esas leyes suele ir seguida de un aumento de las causas civiles y penales contra los periodistas. A estas alturas, cabe subrayar que, a menudo, esas prácticas presentan una dimensión de género, habida cuenta de que se señala a algunas periodistas como Maria Ressa y Rana Ayyub, a mujeres miembros de la sociedad civil

e incluso a mujeres jóvenes de a pie por infringir presuntamente la moralidad pública o sin más, por hacer su trabajo.

Por último, el ámbito de la información abarca las prácticas que manipulan la información en la esfera pública con el fin de tergiversar la forma en que las personas perciben la realidad y, por tanto, la capacidad que tienen para actuar debidamente en respuesta a cuestiones sociales o políticas. Algunas de esas prácticas son la información errónea, la desinformación o la información con fines nocivos, así como el uso de actitudes coordinadas artificiales o *astroturfing* para cambiar la agenda pública en las plataformas de medios sociales. Esas prácticas son posibles gracias a unos servicios de Internet en los que la publicidad impulsa el tráfico y, por tanto, la percepción de popularidad puede comprarse.

En las zonas de conflicto, los Gobiernos hostiles recurren a una actitud coordinada artificial para silenciar las voces críticas, bombardeándolas con tantos comentarios negativos que sus medios sociales quedan inutilizados. Las administraciones de varios países han creado departamentos gubernamentales concebidos expresamente para configurar el discurso en línea u organizaciones similares a las de los informativos para tergiversar la percepción de la actitud del Estado o para corromper las líneas de comunicación de tal modo que la señal no pueda llegar. El conjunto de esas prácticas dificulta la consecución de la paz porque dificulta que la población se ponga de acuerdo sobre las causas del conflicto y, por tanto, sobre lo que hay que hacer para detenerlo.

Tal vez el mayor motivo de alarma sea que el aumento de esas prácticas no se limita necesariamente a determinados tipos de Gobierno ni a los que podríamos calificar fácilmente de autoritarios. Por el contrario, nuestra investigación reveló una tolerancia cada vez mayor a la posibilidad de que las preocupaciones sobre la seguridad nacional superen a las preocupaciones en materia de derechos humanos y democracia.

Es importante que debo dar la alarma ante la práctica de producir y exportar tecnologías que permiten el autoritarismo digital desde países democráticos desde el punto de vista teórico a países explícitamente autoritarios. Todo ello antes de abordar las injusticias que encierran las propias tecnologías, entre ellas la inteligencia artificial.

Al mismo tiempo, el hecho de considerar los desafíos a que se enfrenta Internet en la actualidad como desafíos puramente nacionales tiene como resultado la fragmentación de la respuesta normativa, lo que socava

el valor de Internet como conector. Nuestra investigación concluye que las amenazas derivadas de la digitalización son multilaterales, es decir, rara vez se limitan a afectar a un solo país; transnacionales, habida cuenta de que normalmente implican la transferencia de tecnología a través de las fronteras nacionales, y generacionales porque, debido a la percepción de la seguridad en la actualidad, estamos hipotecando la posibilidad de que las generaciones futuras puedan acceder a Internet de forma gratuita. Esas realidades exigen una respuesta adecuada. No basta con señalar a un país concreto. Lo que tenemos que hacer es detectar las culturas del autoritarismo digital antes de que arraiguen y se expandan a todo el mundo.

Para concluir, quisiera recordar una vez más el mandato del Consejo de Seguridad respecto de la preservación de la paz y la seguridad e instar a que se adopte un enfoque multilateral, transnacional y generacional para abordar los desafíos en el ámbito de los derechos humanos en la era digital. Para lograr ese enfoque, insto al Consejo a que recuerde tres principios.

En primer lugar, los derechos digitales son derechos humanos, y todo esfuerzo por abordar esos desafíos debe comenzar con la protección de lo humano frente a los excesos del poder del Estado y de las empresas privadas.

En segundo lugar, a pesar de estos y otros desafíos, el poder de Internet puede y debe seguir aprovechándose para el bien común y debemos configurarlo y protegerlo como un bien público mundial, sin permitir que los intereses en materia de seguridad o los beneficios acallen los intereses relacionados con la paz.

Por último, cualquier acción que el Consejo decida emprender debe ir más allá de este momento para proteger las aspiraciones de las generaciones futuras. ¿Qué futuro digital compartido hacen posible nuestras acciones? ¿Qué futuros circunscriben? Como es evidente, hay muchas tensiones y contradicciones en esos principios. ¿Queremos que el Gobierno intervenga más o menos? ¿Qué papel deben desempeñar las empresas privadas? ¿Cómo podemos equilibrar nuestro deseo de progreso técnico y el deseo de un uso holístico y equitativo?

Considero que, teniendo en cuenta esos principios, se hacen evidentes algunas medidas que las Naciones Unidas pueden adoptar para proteger los derechos digitales y garantizar que las tecnologías digitales desempeñen un papel positivo en la paz y la seguridad internacionales. Las Naciones Unidas deben seguir utilizando su poder de convocatoria incomparable para fomentar la

deliberación y recabar apoyos para la preservación de Internet como bien público mundial. Las Naciones Unidas deben utilizar su poder de fijación de la agenda para garantizar que los derechos humanos se integren de forma retroactiva y proactiva en las tecnologías digitales que creamos y empleamos. Las Naciones Unidas deben utilizar su poder normativo para fomentar el acuerdo sobre las normas de derechos humanos que harían posible un futuro digital libre, seguro y justo, no solo para esta generación, sino también para las venideras.

Por último, las Naciones Unidas deben recabar apoyo para quienes han estado al frente de esta labor en todo el mundo y a menudo han corrido un gran riesgo personal hablando en defensa de quienes, como Alaa Abd El-Fattah, han sufrido graves injusticias por el modo en que han utilizado Internet para promover los ideales democráticos.

Aunque en este momento nos encontramos en una trayectoria que conducirá a un futuro digital injusto, es posible optar por una vía diferente y más justa, y el Consejo tiene la oportunidad de acercarnos a ese futuro mejor.

La Presidenta (*habla en inglés*): Doy las gracias a la Sra. Nyabola por su exposición informativa.

Tiene la palabra el Sr. Druet.

Sr. Druet (*habla en inglés*): Estoy muy agradecido por esta oportunidad y por el honor de informar al Consejo sobre la forma en que la evolución de las tecnologías digitales influye en la naturaleza de los conflictos violentos, así como sobre las consecuencias que eso tiene para los esfuerzos de las Naciones Unidas encaminados a prevenir la violencia, sostener la paz y mitigar el sufrimiento y la guerra.

Como ha mencionado la Presidencia del Consejo, he participado en la creación de las capacidades tecnológicas de las Naciones Unidas durante varios años, en particular desde la perspectiva de la conciencia situacional, el análisis y la inteligencia para el mantenimiento de la paz. En la actualidad, investigo sobre esas cuestiones en la Universidad McGill y asesoro a diversas partes interesadas sobre las intersecciones de la tecnología, el carácter de los conflictos y las intervenciones en materia de paz y seguridad internacionales.

Hoy quisiera ofrecer mi punto de vista sobre tres temas interrelacionados: en primer lugar, la manera en que las tecnologías digitales reconfiguran los conflictos en que se implica el Consejo de Seguridad; en segundo lugar, la forma en que esas tecnologías y su empleo por las partes en conflicto y las propias Naciones Unidas

repercuten en los esfuerzos de la Organización por prevenir la violencia y darle solución, y, en tercer lugar, quisiera presentar algunas sugerencias al Consejo sobre la manera en que el conjunto de instrumentos de paz y seguridad de las Naciones Unidas, en particular sus operaciones de paz, puede adaptarse para trabajar de forma más eficaz y responsable en esos contextos cambiantes.

Con respecto al primer tema, relativo a las repercusiones, el Consejo ha escuchado en varias ocasiones cómo las tecnologías digitales han ayudado a acelerar las dinámicas dentro y fuera de los grupos, las plataformas para la rápida difusión de la desinformación y los instrumentos destinados a la manipulación de la población, sobre todo por parte de agentes estatales, no estatales y extremistas. En Myanmar, por ejemplo, la incitación incontrolada a la violencia en Facebook y los algoritmos que dieron visibilidad a perfiles de ideas extremistas están bien documentados por contribuir a la violencia genocida perpetrada contra el pueblo rohinyá. Desde entonces, el acceso a Internet y a las comunicaciones se ha utilizado como instrumento para controlar a la población de refugiados en Bazar de Cox. Más recientemente, el conflicto en Ucrania ha puesto de manifiesto la importancia que reviste la opinión pública en las estrategias de la mayoría de las partes en los conflictos modernos, si no de todas ellas.

En muchos de los conflictos y entornos inestables en los que intervienen las Naciones Unidas, es importante señalar que la población es claramente vulnerable a la información errónea y la desinformación. Algunos países, como la República Centroafricana, carecen de una cultura profesional de periodismo tradicional y de una infraestructura de medios de comunicación, por lo que la población depende casi exclusivamente de los medios sociales para informarse. Además, aunque las empresas de medios sociales insisten mucho en la labor de lucha contra la desinformación que llevan a cabo en sus plataformas, la divulgación de documentos internos de Facebook en 2021 puso de manifiesto que los recursos de moderación de contenidos estaban muy sesgados hacia los Estados Unidos y Occidente, mientras que algunos entornos inestables y afectados por conflictos prácticamente se ignoraban. En ese sentido, el Consejo de Seguridad tiene la oportunidad de exigir a las empresas de medios sociales que se apliquen sus responsabilidades por igual en todo su alcance mundial.

Además de su repercusión en la dinámica de los conflictos, las tecnologías digitales son cada vez más importantes para la protección de los derechos humanos o para su privación en situaciones de conflicto. En el

Afganistán, la población civil se ha pronunciado sobre el efecto que tiene el rumor constante de los sistemas aéreos no tripulados en su salud mental, mientras que en Myanmar la junta militar ha utilizado su control de Internet para atacar a los opositores al golpe de Estado de 2021 y limitar su capacidad de comunicación y organización. Durante la crisis migratoria provocada por el conflicto en Siria y, más recientemente, en el conflicto en Ucrania, han salido a la luz una serie de cuestiones graves en torno al consentimiento informado para la recogida y gestión de datos biométricos, en particular por parte de los agentes humanitarios.

En cuanto al segundo tema, relativo a la repercusión en las operaciones de paz, a medida que aumenta la importancia de las tecnologías digitales y del discurso en la lógica de la guerra, las operaciones de las Naciones Unidas desplegadas en esos conflictos se han visto inevitablemente arrastradas por las estrategias de las partes en conflicto a influir a su favor en el resultado. En la República Centroafricana, la Misión Multidimensional Integrada de Estabilización de las Naciones Unidas en la República Centroafricana ha sido objeto de campañas deliberadas destinadas a socavar la credibilidad de la Misión ante los ojos de la población. Los factores que motivan esas actividades parecen ser muy diferentes según el entorno y los agentes implicados. En Malí, por ejemplo, la desinformación que algunos agentes de poder locales dirigen contra la Misión Multidimensional Integrada de Estabilización de las Naciones Unidas en Malí parece tener como objetivo socavar las operaciones de la Misión que podrían desbaratar las redes económicas ilegales. En otros casos, la desinformación parece estar motivada por objetivos ideológicos, mientras que en otras situaciones las Naciones Unidas parecen otorgar un papel eficaz a un Estado anfitrión o a sus asociados, que buscan desviar la atención de su actuación a la hora de proporcionar seguridad y servicios a la población. Con independencia de los motivos, esos ataques reducen enormemente el acceso de las Naciones Unidas a la población local necesitada, socavan su relación con los Gobiernos de los países receptores y las partes en los procesos de mediación y paz y, en algunos casos, amenazan gravemente la seguridad del personal de mantenimiento de la paz.

Sin embargo, también es importante reconocer la función que desempeñan las tecnologías digitales para que las Naciones Unidas puedan ejecutar sus mandatos de manera eficaz en los entornos de conflicto modernos. Las operaciones de paz de las Naciones Unidas en Somalia y Malí, por ejemplo, están recurriendo a tecnologías de

procesamiento del lenguaje natural para obtener rápidamente una comprensión matizada de las percepciones locales y del discurso político nacional. Las tecnologías de control y vigilancia, como los sistemas aéreos no tripulados, se están utilizando con una integración cada vez más eficaz en los instrumentos de recopilación de datos cualitativos y cuantitativos y en los sistemas de análisis de toda la misión, a fin de generar una inteligencia para el mantenimiento de la paz de mayor calidad. Eso se traduce en una detección mejor fundamentada de las amenazas y en una actuación más rápida para proteger a la población civil y, por supuesto, para garantizar la seguridad del personal de las Naciones Unidas.

En ese contexto, quisiera ofrecer algunas reflexiones al Consejo para que estudie la manera de hacer que las Naciones Unidas puedan adaptarse a las repercusiones de las tecnologías digitales en los conflictos, mitigar los efectos negativos de esas tecnologías en sus propias operaciones y utilizar las tecnologías digitales de forma más eficaz y responsable en esos contextos. A ese respecto, cabe mencionar cuatro aspectos concretos.

En primer lugar, las Naciones Unidas deben asumir un papel más explícito y deliberado como agentes de la información en entornos de conflicto. El acceso a una información precisa puede considerarse cada vez más como un derecho humano en situaciones de guerra de información y las Naciones Unidas tienen una función que desempeñar como esclarecedoras de la verdad y como medio de información fiable. Debo señalar que se trata de una función que las misiones de las Naciones Unidas han desempeñado durante muchos años en el marco de los mecanismos de los procesos de paz, por ejemplo, mediante la vigilancia del alto el fuego. Por lo tanto, cabe examinar la forma en que las buenas prácticas establecidas a través de esos mecanismos pueden contribuir a informar a las sociedades en conflicto de manera más amplia.

Sin embargo, para que las Naciones Unidas puedan desempeñar esa función, es fundamental que sus operaciones se ganen y mantengan la confianza de diferentes sectores de la población. No es una tarea fácil, habida cuenta de que algunas actividades de las Naciones Unidas, como la protección de los civiles o el apoyo a las autoridades de los Estados receptores, pueden convertir a las misiones en objeto de críticas —unas veces justificadas y otras no— más aún cuando esas misiones se ven afectadas por campañas de desinformación. Por ello, como segunda prioridad, las operaciones de paz de las Naciones Unidas tienen que aumentar de manera considerable sus capacidades para vigilar y analizar

el espacio informativo y responder con eficacia a las comunicaciones malintencionadas. Según un informe reciente del International Peace Institute, las misiones deben anticiparse a las crisis y replantear la retórica utilizada de forma proactiva, con el fin de entablar una comunicación bidireccional en lugar de unidireccional, así como adaptar sus mensajes a públicos específicos.

En tercer lugar, las propias Naciones Unidas necesitarán nuevas tecnologías y la capacidad de utilizarlas de forma eficaz, tanto en la esfera de las comunicaciones como de la conciencia situacional y la inteligencia para el mantenimiento de la paz, el análisis de datos para la planificación estratégica o las nuevas tecnologías para el diálogo y la mediación. A medida que las Naciones Unidas avanzan y logran muchas innovaciones interesantes en esas esferas, entre ellas las destacadas por la Sra. DiCarlo, es fundamental reconocer que esos instrumentos traen consigo cuestiones éticas, jurídicas y políticas importantes y complejas, que guardan relación con los derechos de las personas que ya se encuentran afectadas por el conflicto. Aunque puede ser tentador adoptar los marcos y la doctrina de los Estados Miembros para utilizar esos instrumentos, quisiera informar al Consejo de que las operaciones de las Naciones Unidas difieren en cuanto a sus intereses y responsabilidades al utilizar artículos sensibles en las situaciones de conflicto.

Por lo tanto, como cuarta recomendación, quisiera destacar la importancia de las formas en que las Naciones Unidas adquieren y utilizan las nuevas tecnologías para lograr la credibilidad y el posicionamiento político de las misiones sobre el terreno. La experiencia ha demostrado que la adquisición de nuevas tecnologías sensibles y las alianzas para su empleo son más eficaces cuando fortalecen la imparcialidad de las Naciones Unidas y ofrecen garantías públicas creíbles de un uso responsable.

Por lo tanto, insto a la Secretaría a que cree sus propios instrumentos, políticas y procedimientos integrales, de forma que tengan en cuenta el carácter singular de las Naciones Unidas como usuario de esas tecnologías. Ya se está llevando a cabo una preciada labor a ese respecto, en particular en el Departamento de Operaciones de Paz, que está trabajando para enriquecer sus políticas de control y vigilancia, y en los esfuerzos de todo el sistema de las Naciones Unidas, dirigidos por la iniciativa Pulso Mundial de las Naciones Unidas, para poner en marcha una política de privacidad de datos en todo el sistema. Si se hace correctamente y con total transparencia para los Estados Miembros y el público, considero que esos esfuerzos tienen un importante efecto normativo al determinar la forma en que pueden

utilizarse con responsabilidad los artículos sensibles en situaciones de conflicto con población vulnerable.

Esos esfuerzos deben reconocer con sinceridad los límites de la capacidad de las Naciones Unidas para proteger la información sensible, sobre todo la información personal, de la intrusión de actores estatales y no estatales y contar con un examen posterior de las prácticas relacionadas, por ejemplo, con la recopilación de datos biométricos en el curso de las operaciones humanitarias. En ese examen debe incluirse también la elaboración de nuevas orientaciones sobre la forma en que las Naciones Unidas comparten información con las fuerzas ajenas a ellas, en particular las fuerzas militares paralelas, las autoridades de los países receptores y los agentes internacionales del estado de derecho, en consonancia con la Política de Diligencia Debida en materia de Derechos Humanos.

Para concluir, en el debate de hoy se abordan dos conjuntos de cuestiones muy distintos, pero sumamente interrelacionados: en primer lugar, la manera en que las tecnologías digitales están cambiando el carácter de los conflictos en las situaciones en que intervienen las Naciones Unidas y, en segundo lugar, la forma en que las propias Naciones Unidas emplean las tecnologías digitales para cumplir sus mandatos. Ambos exigen un examen y un debate matizados, así como respuestas normativas y operacionales diferentes. Para que nuestras operaciones actuales y futuras sean fructíferas, es fundamental que abordemos correctamente los dos conjuntos de cuestiones. El Consejo tiene un papel fundamental que desempeñar al respecto.

La Presidenta (*habla en inglés*): Doy las gracias al Sr. Druet por su exposición informativa.

Quisiera señalar a la atención de los oradores el párrafo 22 de la nota de la Presidencia S/2017/507, en el que se alienta a todos los participantes en las sesiones del Consejo a que formulen sus declaraciones en un tiempo máximo de cinco minutos, adhiriéndose al compromiso del Consejo de hacer un uso más eficaz de las sesiones públicas.

Formularé ahora una declaración en calidad de representante de los Estados Unidos.

Doy las gracias a la Secretaria General Adjunta Di Carlo por su exposición informativa. En sus observaciones dejó claro que las nuevas tecnologías ya están desempeñando un papel fundamental en los esfuerzos de mantenimiento de la paz de las Naciones Unidas, y es esencial que se utilicen de forma constructiva. Doy las

gracias a la Sra. Nyabola por su inestimable perspectiva sobre los beneficios y los desafíos a los que se enfrentan los activistas de derechos humanos y la sociedad civil por el posible uso, así como el uso indebido, de esas tecnologías. Agradezco al Sr. Druet que haya compartido las formas en que la tecnología digital puede utilizarse para apoyar la labor de nuestro personal de mantenimiento de la paz, mientras que utilizarla indebidamente también puede socavarla. Permítaseme asegurarme de maximizar lo primero y minimizar lo segundo. Esta sesión informativa trata de una enorme oportunidad y un desafío acuciante.

El Consejo de Seguridad tiene la oportunidad de aprovechar el poder de la tecnología digital para promover la paz y la seguridad con el fin de hacer un uso responsable de esos instrumentos para que aporten un enorme beneficio en los mismos conflictos y contextos en los que están causando daño. Al fin y al cabo, esas tecnologías tienen enormes posibilidades de contribuir al buen hacer del sistema de las Naciones Unidas en todo el mundo. Los instrumentos de los medios sociales y las aplicaciones de mensajería pueden facilitar el acceso a información que puede salvar vidas durante los conflictos y antes de que estallen. Los datos de los satélites pueden identificar los riesgos del cambio climático, proporcionar información crítica al personal de mantenimiento de la paz y mejorar las comunicaciones de emergencia durante los conflictos y los desastres naturales. Podemos identificar y evitar las hambrunas antes de que empiecen. Podemos encontrar viviendas, alojamiento y empleos para los refugiados. Podemos proteger mejor a nuestro personal de mantenimiento de la paz y a las personas a las que tienen el mandato de servir.

Sin embargo, también debemos abordar un desafío acuciante, que es el modo en que las tecnologías digitales se están utilizando indebidamente para restringir los derechos humanos y alimentar los conflictos. En manos de agentes estatales y, en algunos casos, de agentes no estatales, esas tecnologías se están utilizando para cortar el acceso a la información, suprimir la libertad de expresión y difundir desinformación, con lo que se intensifican los conflictos, socavando los valores fundamentales de la Carta de las Naciones Unidas que se nos ha encomendado defender.

En la República Centroafricana y en Malí, la desinformación dirigida a las misiones de las Naciones Unidas para el mantenimiento de la paz ha amenazado la seguridad del personal de mantenimiento de la paz y ha socavado la capacidad de las misiones para proteger a los civiles. En Etiopía, las autoridades han cortado el

acceso a Internet en la región de Tigré desde noviembre de 2020 al estallar el conflicto entre las Fuerzas Nacionales de Defensa de Etiopía y las fuerzas regionales de Tigré. Esas acciones obstaculizan la capacidad de los civiles para acceder a los servicios sanitarios, retrasan la documentación de las atrocidades y los abusos contra los derechos humanos, interrumpen los servicios financieros y restringen la conexión virtual de los familiares con sus seres queridos.

Hay países sentados en esta misma mesa que también están utilizando la tecnología para acosar, vigilar arbitrariamente y censurar y reprimir a la sociedad civil y a los medios de comunicación independientes como nunca antes. En ningún lugar es más evidente que en la guerra que ha decidido librar Rusia contra Ucrania. El Gobierno ruso sigue cerrando, restringiendo y degradando la conectividad a Internet, censurando contenidos, difundiendo desinformación en línea e intimidando y deteniendo a periodistas por informar de la verdad sobre su invasión. Esas prácticas son tan erróneas como generalizadas. Como ya informó la Sra. Nyabola al Consejo, la organización no gubernamental Access Now estima que en 2021 se produjeron 182 cortes de Internet en 34 países. Hay algo más preocupante, con frecuencia oímos decir que esas acciones se llevan a cabo en nombre de la protección de la paz y la seguridad. Nada más lejos de la realidad.

También seguimos viendo cómo los agentes no estatales, incluidos los terroristas y los extremistas violentos, utilizan las plataformas de comunicación en línea para reclutar, radicalizar y movilizar en favor de la violencia. Todos los que estamos decididos a abordar y prevenir los conflictos en todo el mundo debemos hacer lo que nos corresponde con miras a garantizar que las tecnologías sirvan de fuerza para el cambio positivo, y no como un instrumento mal utilizado para perpetrar abusos contra los derechos humanos, alimentar el odio y exacerbar los conflictos.

Por ello, los Estados Unidos están trabajando con la sociedad civil, el sector privado y otras partes interesadas para lograr progresos en este esfuerzo mundial. Por nuestra parte, denunciamos el uso de cierres parciales y totales de Internet, la censura y otras tácticas para evitar el ejercicio de la libertad de expresión en línea. Tras la Cumbre para la Democracia, seguimos uniendo fuerzas con nuestros asociados de la Coalición para la Libertad en Línea con miras a proteger la libertad en Internet y garantizar que todos los ecosistemas digitales respeten los marcos internacionales de derechos humanos.

Sabemos que los instrumentos de vigilancia y otras tecnologías de doble uso pueden utilizarse indebidamente para amenazar a los defensores de los derechos humanos y a otras personas. Por eso utilizamos el control de las exportaciones para hacer rendir cuentas a las empresas que desarrollan, utilizan o trafican con programas espía y otras tecnologías que permiten esas actividades maliciosas.

Estamos trabajando a través de las Naciones Unidas y otros foros con miras a defender el marco de la conducta responsable de los Estados en el ciberespacio, en el que se expresa claramente que el derecho internacional se aplica a las actividades cibernéticas de los Estados y se establece un conjunto de normas voluntarias para orientar su comportamiento en tiempos de paz. Asimismo, estamos colaborando con países de todo el mundo para responder a las actividades cibernéticas maliciosas y protegernos de estas. En todo el mundo, las formas de acoso y abuso en línea, incluidas las campañas de desinformación contra las mujeres dirigentes, están perturbando la participación igualitaria de las mujeres en la toma de decisiones sobre cuestiones de paz y seguridad.

Tenemos que trabajar de consuno para combatir la información errónea y la desinformación a nivel mundial. Las Naciones Unidas ya están desempeñando un papel clave en la elaboración de información transparente y de fácil acceso y en la defensa de los periodistas que están en primera línea.

También debemos aprovechar las oportunidades para liberar el potencial latente de las tecnologías a la hora de promover la paz y la seguridad. Por ello, el mes pasado, un grupo de 60 asociados mundiales presentó la Declaración para el Futuro de Internet con el fin de revitalizar una visión democrática de Internet en el plano mundial. Invitamos a todas las autoridades competentes y a los Estados Miembros de las Naciones Unidas que se han comprometido a defender el principio de la Declaración a que se sumen a nosotros.

A fin de mantener eficazmente la paz y la seguridad en el siglo XXI, tenemos que responder a las amenazas del siglo XXI y valernos de los instrumentos del siglo XXI. Ha llegado el momento de que las Naciones Unidas aprovechen responsablemente el poder de la tecnología digital para afrontar nuestros desafíos más acuciantes y promover la paz y la seguridad en todo el mundo.

Vuelvo a asumir ahora mis funciones de Presidenta del Consejo.

Sr. Hoxha (Albania) (*habla en inglés*): Agradecemos a los Estados Unidos que haya organizado de esta oportuna sesión para tratar esta cuestión tan compleja como relevante. También damos las gracias a la Secretaria General Adjunta DiCarlo por sus siempre perspicaces reflexiones.

Nos complace que la sociedad civil ocupe un lugar destacado en esta sesión, y por una buena razón, como hemos podido comprobar con la amplitud de sus aportes y las recomendaciones que han formulado. Por tanto, doy las gracias a la Sra. Nyabola y al Sr. Druet.

La rápida evolución de la tecnología ha cambiado el funcionamiento del mundo, lo que ha afectado a todos los aspectos de la vida moderna. Se ha arraigado tanto en nuestra vida cotidiana que es difícil recordar cómo era el mundo antes.

Es innegable que la tecnología moderna aporta una serie de ventajas en múltiples sectores. Los particulares, los Estados, los Gobiernos, la industria, la sanidad, los sistemas financieros, las organizaciones regionales e internacionales y las misiones de mantenimiento de la paz se aprovechan de la rápida expansión de las tecnologías digitales. Ayudan a las personas a ser más productivas y a las empresas y entidades a ser más innovadoras, más flexibles y a tener una mayor capacidad de adaptación que nunca.

Hemos abrazado de buen grado la interconectividad de los dispositivos y sistemas, lo que ha facilitado visiblemente nuestra vida y nuestro trabajo, pero eso viene acompañado del inevitable costo de la exposición a una amplia gama de amenazas por parte de fuerzas maliciosas. El nexo “nueva tecnología, nuevas amenazas” no necesita explicación.

Como hemos escuchado hoy, existe un entendimiento común sobre los inmensos riesgos que entrañan las actividades maliciosas de agentes tanto estatales como no estatales. La utilización indebida de las tecnologías de la información y las comunicaciones tiene un efecto directo en la paz y la seguridad internacionales, ya que socava la integridad, la seguridad, el crecimiento económico y la estabilidad de la comunidad mundial, dando lugar a controversias y conflictos.

Habida cuenta de la preocupación cada vez mayor por el carácter de doble uso de la tecnología y sus consecuencias para el mantenimiento de la paz y la seguridad internacionales, es muy importante que el Consejo de Seguridad asuma un papel de liderazgo en la evaluación de dichos riesgos y consecuencias. Por lo tanto, acojo con gran agrado la celebración de la sesión de hoy.

La inteligencia artificial está haciendo milagros en muchos sectores, como la agricultura y la medicina, a saber, salvando vidas, aumentando la producción de alimentos, mejorando las fuentes de energía y gestionando los procesos de producción. No obstante, si no se utiliza correctamente y, sobre todo, si no se respeta la ética, puede dar lugar a graves violaciones de los derechos humanos, como la vigilancia indebida dirigida a grupos y comunidades específicos. Dado que la tecnología suele desarrollarse más rápido de lo que los Estados pueden captar su repercusión total, debemos asegurarnos de que los principios y valores fundamentales, como la equidad, la igualdad, la inclusividad, la responsabilidad, la transparencia y la rendición de cuentas, se preserven de los efectos negativos.

Por desgracia, el potencial de la tecnología para afectar de manera drástica a la cohesión social y, naturalmente, a la paz y la seguridad internacionales, a causa de una utilización indebida por parte de agentes estatales o no estatales, está creciendo de manera significativa. Algunos países siguen intentando proporcionar información engañosa de manera deliberada, tergiversar los hechos, interferir en los procesos democráticos de otros, difundir el odio, promover la discriminación e incitar a la violencia o a los conflictos mediante la utilización indebida de las tecnologías digitales. Del mismo modo, vemos con preocupación los cortes de Internet y la restricción o negación de los derechos humanos y las libertades al hacer uso de este. Los ponentes expusieron ejemplos concretos. Deberíamos redoblar los esfuerzos para mitigar el daño que pueden causar, como se indica en el informe del Secretario General sobre una hoja de ruta para la cooperación digital (A/74/821), y examinar detenidamente sus recomendaciones.

Quiero destacar la firme posición de Albania a favor de un ciberespacio mundial, abierto, libre, estable y seguro, donde se aplique plenamente el derecho internacional, incluido el respeto de los derechos humanos y las libertades fundamentales, en aras del desarrollo social, político y económico.

Estamos sumamente preocupados por el aumento de las actividades cibernéticas y digitales maliciosas en los últimos meses. Sabemos que las medidas de Rusia causaron cortes de la comunicación, incluso contra infraestructura crítica, no solo en Ucrania sino también en otras partes de Europa, al atacar deliberadamente el satélite de Viasat el 24 de febrero de 2022, justo una hora antes de la invasión no provocada e injustificada de Rusia a Ucrania.

Los ciberataques supuestamente originados en Rusia también han intentado interferir en las elecciones ucranianas, atacando su red de suministro eléctrico, sustituyendo los sitios web de su Gobierno y propagando programas maliciosos en sus sistemas, lo que ha tenido efectos destructivos. Los Balcanes Occidentales, de donde soy, están siendo objeto de campañas sistemáticas de injerencia y manipulación informativa para provocar de manera intencionada inestabilidad política y socavar sus aspiraciones euroatlánticas. No lo permitiremos y opondremos resistencia.

Otros ejemplos notorios son las reiteradas actividades maliciosas del régimen de la República Popular Democrática de Corea, que intenta recopilar información de inteligencia, cometer ciberataques y generar ingresos ilícitos que, entre otras cosas, sirvan para financiar su militarización y proliferación, lo que contraviene el derecho internacional y las resoluciones del Consejo de Seguridad. Añadimos a esa lista los cortes de Internet en Myanmar, que también se han mencionado hoy. Pedimos que se ponga fin a esas actividades y se respeten las normas vigentes y el orden internacional basado en normas en el ciberespacio. Internet no es ni debe convertirse en un arma, sino seguir siendo un bien público.

Acogemos con agrado los informes del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A través de ellos, los Estados Miembros han acordado un marco sustancial de las Naciones Unidas, que incluye el derecho internacional vigente, 11 normas voluntarias no vinculantes, medidas de fomento de la confianza, la creación de capacidades y los conocimientos especializados de la comunidad de múltiples partes interesadas.

Permítaseme terminar con esta reflexión: a lo largo de la historia, los nuevos desafíos han abierto nuevas oportunidades de cooperación. Hoy en día sigue siendo así, aunque los desafíos que se plantean son muy complejos, evolucionan rápidamente y surgen en medio de una creciente sensación de conflicto y crisis. Sin embargo, no hay alternativa al diálogo significativo, a la cooperación a través de un comportamiento responsable, primero, y a los marcos normativos, después, sobre cómo los avances tecnológicos están afectando a las personas, a los Estados y a las sociedades, y sobre los usos y aplicaciones de la tecnología que generan más trastornos, especialmente los que suponen una amenaza directa a la paz y la seguridad. Con respecto a muchos

otros aspectos, nos corresponde decidir si compartimos los enormes beneficios o asumimos los ingentes costos.

Sr. De Rivière (Francia) (*habla en francés*): Doy las gracias a la Sra. DiCarlo, a la Sra. Nyabola y al Sr. Druet por sus exposiciones informativas.

Me centraré en tres observaciones.

Ante todo, las tecnologías digitales son una oportunidad para la paz y la seguridad internacionales. Las operaciones de mantenimiento de la paz han estado a la vanguardia de esos esfuerzos. En la declaración de la Presidencia, aprobada en agosto (S/PRST/2021/17) a iniciativa de la India, se hizo un balance de la situación. Estas tecnologías contribuyen a la seguridad del personal de mantenimiento de la paz y a la realización de las operaciones, sobre todo con vistas a mejorar la protección de los civiles. Están revolucionando las comunicaciones estratégicas para el mantenimiento de la paz. Por ello, Francia seguirá apoyando todas esas innovaciones.

La tecnología también es un factor impulsor para movilizar e incluir a la sociedad civil. La Misión de las Naciones Unidas en el Sudán llevó a cabo una consulta en línea en el país, que permitió a toda la sociedad civil expresar su opinión, incluido en las regiones. Al facilitar la circulación de la información, las tecnologías también contribuyen a la lucha contra la impunidad, como lo demuestran la cobertura mediática y la inteligencia de fuentes abiertas en el contexto del conflicto en Ucrania.

Sin embargo, los usos maliciosos de las tecnologías están proliferando y pueden constituir una amenaza para la paz y la seguridad internacionales. Esa es mi segunda observación.

Eso es lo que ocurre con el desarrollo de las ciberamenazas, como demuestra una vez más el conflicto en Ucrania. Francia y la Unión Europea, así como varios asociados, han condenado los ciberataques cometidos por Rusia contra una red de satélites una hora antes de la invasión de Ucrania, con el objetivo de facilitar su agresión. El derecho internacional se aplica en su totalidad al ciberespacio. También condenamos las actividades cibernéticas maliciosas de Corea del Norte, que incluyen robar información sensible y criptomonedas para contribuir a sus programas nucleares y balísticos. También nos preocupa el uso cada vez mayor de criptomonedas para la financiación del terrorismo. Condenamos el aumento de los ataques contra los agentes humanitarios y las organizaciones no gubernamentales.

Las tecnologías digitales también facilitan la guerra de la información. Condenamos las campañas

masivas de desinformación que se están llevando a cabo en la República Centroafricana y en Malí, así como las que apoyan la guerra de Rusia contra Ucrania. En Malí, Francia frustró hace poco un intento de manipulación de la información por parte de los mercenarios del Grupo Wagner. Ese ejemplo demuestra la amenaza que suponen las estrategias híbridas que pretenden difuminar la línea entre los agentes estatales y no estatales.

Los cortes de Internet constituyen una violación de los derechos humanos. Lamentamos la continua interrupción de las telecomunicaciones en el norte de Etiopía. Esta ha dificultado la obtención de pruebas de las violaciones de los derechos humanos, que no deben quedar impunes. En Oriente Medio, los cortes de Internet se utilizan para debilitar los movimientos de protesta, y algunos defensores de los derechos son sometidos a vigilancia y acoso en las redes sociales.

Ante esas amenazas que se multiplican, los Gobiernos deben responder mediante la cooperación y la ley. Esa es mi tercera observación.

Las Naciones Unidas ofrecen un marco insustituible para lograrlo. Francia seguirá contribuyendo a ello, entre otras cosas velando por que en las resoluciones del Consejo de Seguridad se tengan en cuenta esos desafíos. Junto con un grupo de 60 países, estamos promoviendo el establecimiento en las Naciones Unidas de un programa de acción para aumentar la capacidad de los Estados a la hora de aplicar las normas convenidas en la esfera del ciberespacio y fortalecer la resiliencia de las redes.

Sr. Tirumurti (India) (*habla en inglés*): Celebro la iniciativa de los Estados Unidos de organizar la importante sesión informativa de hoy. Agradezco las valiosas aportaciones de la Secretaria General Adjunta, Sra. Rosemary DiCarlo, y de los demás ponentes, la Sra. Nyabola y el Sr. Druet.

El creciente uso de las tecnologías digitales ha acelerado el desarrollo económico, ha mejorado la prestación de servicios a los ciudadanos, ha generado una mayor conciencia social y ha puesto la información y el conocimiento al alcance de las personas. Las tecnologías digitales han hecho que la gobernanza sea más inclusiva, centrada en el ciudadano y transparente. En esta era digital, la mayoría de las actividades —políticas, sociales, económicas, humanitarias y de desarrollo— se realizan sistemáticamente en el ciberespacio o están conectadas a él. Sin embargo, habida cuenta de su naturaleza de doble uso y su susceptibilidad a usos perjudiciales por parte de agentes tanto estatales como

no estatales, también pueden tener un efecto negativo en la paz y la seguridad internacionales.

La naturaleza de los conflictos y sus herramientas subyacentes han cambiado enormemente a lo largo de los decenios. Mientras continúan los conflictos interestatales, asistimos a un aumento de las amenazas por parte de agentes no estatales, incluidos los grupos terroristas. Del mismo modo, los teatros de guerra y conflicto también se han ampliado. Además de los conflictos territoriales, el mundo se enfrenta a nuevos conflictos en los mares y el espacio, y por espacio me refiero tanto al espacio ultraterrestre como al ciberespacio. La tecnología se ha convertido en el denominador común subyacente y en un factor de cambio de estos conflictos. Por lo tanto, nuestro enfoque convencional de la seguridad a los niveles nacional e internacional necesita un reajuste.

Quisiera someter a la consideración del Consejo de Seguridad las cinco cuestiones siguientes. En primer lugar, es necesario abordar la cuestión del abuso de las tecnologías digitales por parte de grupos terroristas para difundir sus ideologías, radicalizar, incitar a la violencia y reclutar a la próxima generación de terroristas aprovechando el aumento de la presencia en línea de los jóvenes. Los grupos terroristas están aprovechando las herramientas en línea para crear redes, reclutar nuevos miembros, conseguir armas y asegurar el apoyo logístico. Los métodos de comunicación digital utilizados por estos grupos son organizados y sofisticados. Se han vuelto expertos en el uso de las salas de chat de los juegos, la web oscura y otros sitios de acceso restringido y espacio en línea no regulado para difundir propaganda e incitar a la violencia. Ha habido casos de terroristas que han transmitido en directo sus atentados en las principales plataformas para publicitarse y obtener un impacto máximo. La gran capacidad de divulgación del espacio en línea ha permitido a los grupos terroristas aprovecharse de la apertura de las sociedades democráticas pluralistas, como la nuestra, alimentando las divisiones sociales y el odio sectario y apoyando los movimientos antidemocráticos y las ideologías radicales destinadas a desestabilizar los Gobiernos y las instituciones del Estado.

La destreza de los terroristas para conectarse, comunicarse y compartir información a través de las plataformas digitales no hace sino subrayar la creciente necesidad de regular estos contenidos incendiarios en línea. También es necesario adoptar medidas respecto de los problemas jurídicos para llevar a los autores de estos delitos ante la justicia, en particular habida cuenta

del carácter remoto de su implicación en las actividades terroristas. Estamos acostumbrados a considerar el terrorismo como un ataque físico directo por parte de sus autores, pero en el ámbito digital, los autores que incitan a cometer actos terroristas sirviéndose de contenidos de odio e ideologías radicales pueden encontrarse lejos de los autores materiales del acto terrorista. También se debe responsabilizar a los instigadores de esos actos de terror. No pueden ser menos culpables que quienes cometen los actos de terror. Esto es esencial cuando consideramos el terrorismo en el ciberdominio.

La aparición de nuevas tecnologías financieras, como los nuevos métodos de pago, las monedas virtuales y los métodos de recaudación de fondos en línea, incluidas las donaciones directas, los tokens no fungibles y las plataformas de financiación colectiva, con la facilidad de acceso, el anonimato y la insolubilidad que ofrecen, han permitido a las entidades terroristas recaudar y transferir fondos eludiendo las estructuras de vigilancia y aplicación de la ley. Algunos nuevos métodos de pago, como las tarjetas telefónicas de prepago, los servicios de pago en línea y el dinero virtual, han permitido a los grupos terroristas canjearlos por oro, plata y otros metales y, más recientemente, por pagos con teléfonos móviles, y financiar actividades terroristas. Las tarjetas de prepago se utilizan a menudo como alternativa al dinero en efectivo. El uso de bitcoins para financiar actividades terroristas también está bien establecido. Además, el uso indebido de la inteligencia artificial y la impresión 3D con fines terroristas, que tienen un alcance mundial, también exige nuestra atención inmediata.

La necesidad de que los Estados Miembros aborden y atajen de forma amplia y más estratégica las implicaciones de la explotación terrorista de las tecnologías digitales nunca ha sido más acuciante. A este respecto, me complace informar al Consejo de Seguridad de que hemos propuesto la celebración dentro de poco en la India de una reunión especial del Comité contra el Terrorismo, que se centrará exclusivamente en esta cuestión y servirá para presentar propuestas de cara al futuro.

En segundo lugar, algunos Estados están aprovechando su experiencia en el ámbito digital para lograr sus objetivos políticos y de seguridad, y se entregan a formas contemporáneas de terrorismo transfronterizo y atentados contra infraestructuras nacionales críticas, incluidas instalaciones sanitarias y energéticas, y perturban la armonía social promoviendo la radicalización a través del espacio en línea. Las sociedades abiertas han sido especialmente vulnerables a esas amenazas y a

las campañas de desinformación. Las tecnologías digitales emergentes, como el uso del aprendizaje automático y los macrodatos, tienen el potencial de aumentar la letalidad de esos actos, lo que supone una amenaza considerable para la paz y la seguridad internacionales. La comunidad internacional no puede adoptar un enfoque selectivo y debe evitar los dobles raseros a la hora de abordar estas amenazas.

En tercer lugar, la naturaleza interconectada del dominio digital hace que las soluciones a los problemas y amenazas complejos que emanan de este dominio no puedan solucionarse de forma aislada. Existe una necesidad subyacente de adoptar un enfoque basado en normas de colaboración y de trabajar para garantizar su apertura, estabilidad y seguridad. Fomentar el acceso equitativo a las tecnologías digitales y sus beneficios también debe ser un componente importante de este enfoque. El aumento de la brecha digital, la brecha digital de género y las lagunas de conocimientos digitales crea un entorno insostenible en el ciberdominio. La creciente dependencia digital en la era posterior a la enfermedad por coronavirus ha exacerbado los riesgos y ha dejado al descubierto estas fisuras de las desigualdades digitales. Esas lagunas deben colmarse con creación de capacidades y transferencia de tecnología.

En cuarto lugar, las misiones de mantenimiento de la paz de las Naciones Unidas deben dotarse de las últimas tecnologías digitales para contrarrestar las empleadas por los grupos armados. Proteger a quienes protegen debe ser nuestra prioridad en la misma medida que lo es proteger a los civiles. A este respecto, durante nuestra Presidencia del Consejo en agosto de 2021 pusimos en marcha, en colaboración con las Naciones Unidas, la plataforma Unite Aware. Este programa tecnológico proporciona al personal de mantenimiento de la paz una evaluación de las amenazas en tiempo real, y debe ampliarse a todas las misiones de mantenimiento de la paz de las Naciones Unidas. Agradezco a la representación de Francia su referencia a la declaración de la Presidencia sobre tecnología y mantenimiento de la paz (S/PRST/2021/17), aprobada durante nuestra Presidencia en 2021.

En quinto lugar, el mantenimiento de la paz y la seguridad internacionales en el ciberespacio también depende del intercambio de información entre países sobre el uso indebido de las tecnologías digitales para cometer delitos. Esta cooperación debe ser eficaz y en tiempo real para disuadir, interrumpir y mitigar el uso indebido de esas tecnologías. Por lo tanto, la creación 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 es un paso en la dirección correcta.

Por último, permítaseme reiterar que la comunidad mundial debe aprovechar las tecnologías digitales en beneficio de toda la humanidad, no solo de unos pocos. Nuestro objetivo general debe ser aprovechar estas tecnologías para el desarrollo, la prosperidad y el empoderamiento de todos los pueblos, y para promover la paz y la seguridad internacionales. La India está dispuesta a compartir sus conocimientos especializados y su experiencia en este empeño común.

Sr. Zhang Jun (China) (*habla en chino*): El rápido desarrollo de la ciencia y la tecnología ha venido acompañado de nuevas oportunidades y nuevos retos. En mayo de 2021, China, Kenya, México y los Emiratos Árabes Unidos convocaron una reunión con arreglo a la fórmula Arria para intercambiar opiniones en profundidad sobre la repercusión de las tecnologías emergentes para la paz y la seguridad internacionales. China acoge con satisfacción la oportunidad de proseguir las deliberaciones sobre tecnología y seguridad en el Consejo de Seguridad. Para desarrollar y utilizar mejor la ciencia y la tecnología en beneficio de la humanidad, China desea proponer lo siguiente.

En primer lugar, debemos defender enérgicamente la innovación científica y tecnológica. La innovación es el principal motor del desarrollo. Todas y cada una de las revoluciones científicas, tecnológicas e industriales de la historia de la humanidad han transformado profundamente nuestro modo de producción y estilo de vida y han promovido enormemente el progreso y el bienestar de la humanidad.

El mundo actual se enfrenta a desafíos complejos y sin precedentes. La rápida evolución de la tecnología digital, la inteligencia artificial y la biotecnología, entre otras cosas, ha desempeñado un papel importante en los ámbitos de la prevención y el control de pandemias, el cambio climático, la seguridad alimentaria y la seguridad energética, entre otros. Ya sea como un nuevo impulso para el crecimiento económico mundial o como una nueva forma y un medio para solucionar problemas complejos de gran envergadura, la innovación en la ciencia y la tecnología es sencillamente indispensable.

Puesto que la economía mundial es sumamente interdependiente y las cadenas industriales y de suministro mundiales están profundamente entrelazadas, todos los países deben considerar los intercambios y la cooperación internacionales en materia de ciencia y tecnología con una mentalidad abierta y promoverlos utilizando las

medidas pertinentes para crear entre todos un entorno abierto, equitativo, justo y no discriminatorio a este respecto, llevando a cabo actividades conjuntas de investigación y desarrollo orientadas a fomentar el progreso gracias a los esfuerzos concertados.

En segundo lugar, los logros de la ciencia y la tecnología deben utilizarse en beneficio de todos. La tecnología no conoce fronteras y forma parte de la riqueza común de la humanidad. Estos logros no deben convertirse en tesoros escondidos en cuevas. En la actualidad, la creciente brecha tecnológica entre los países desarrollados y los países en desarrollo —en particular la brecha digital— está agravando las nuevas formas de desigualdad.

Hay que permitir que plataformas multilaterales como las Naciones Unidas desempeñen plenamente su papel de apoyo a las capacidades de investigación y desarrollo de los países en desarrollo; aceleren la transferencia de tecnologías; estimulen la comercialización de los logros científicos; compartan los dividendos del progreso científico y tecnológico con los países en desarrollo; subsanen las carencias de desarrollo reduciendo la brecha digital; y aceleren la implementación de la Agenda 2030 para el Desarrollo Sostenible.

Se debe prestar apoyo a los países en desarrollo para utilizar las últimas tecnologías y los microdatos con el fin de mejorar la gobernanza social y prevenir y combatir eficazmente los delitos.

En el mantenimiento y la consolidación de la paz, el Consejo también debe utilizar activamente las nuevas tecnologías para reforzar sus capacidades de recopilación de información, alerta temprana, respuesta de emergencia y rescate.

En tercer lugar, la colaboración es imprescindible para gestionar y controlar los riesgos que plantea la tecnología. Los avances tecnológicos pueden ser una fuente de riesgo en cuanto a normas conflictivas, riesgos sociales y desafíos éticos. La comunidad internacional debe defender el concepto de ciencia y tecnología en beneficio de la humanidad; permitir que las Naciones Unidas cumplan su función de canal principal para el diálogo activo, los intercambios y la cooperación; adherirse a la participación multilateral y de múltiples partes interesadas; gestionar conjuntamente los riesgos del desarrollo tecnológico; y formular y mejorar reglas y normas aceptadas universalmente.

Es necesario frenar el abuso de las tecnologías de la información, oponerse a la cibervigilancia y los ataques y oponerse a una carrera armamentista en el

cibespacio. Es fundamental impedir que los terroristas utilicen Internet para reclutar, financiar u organizar atentados terroristas, así como evitar que Internet se convierta en un semillero de discursos de odio, racismo, pornografía y violencia. Los Gobiernos deben reforzar las medidas de supervisión y control de acuerdo con la ley, normalizar la aplicación de la tecnología y salvaguardar mejor los intereses públicos. Los proveedores de plataformas tecnológicas y de servicios de Internet deben normalizar sus prácticas y reforzar la autodisciplina para cumplir con sus responsabilidades sociales.

En cuarto lugar, nos oponemos a la politización de las cuestiones de carácter tecnológico. El mundo de la ciencia no es un campo de batalla de suma cero. No debe haber un único paladín de la innovación tecnológica. Sin embargo, resulta preocupante que, desde hace algún tiempo, algunos Gobiernos politicen cuestiones de carácter científico y tecnológico. Han generalizado el concepto de seguridad nacional, han abusado del poder del Estado y han intensificado gratuitamente la eliminación de empresas de alta tecnología de otros países. Para mantener su monopolio en los ámbitos de la ciencia y la tecnología, esos Gobiernos han establecido círculos y clubes exclusivos en el contexto de sus denominadas estrategias o marcos. Han impuesto bloqueos tecnológicos a otros países y han incurrido en prácticas de intimidación en el ámbito de la ciencia y la tecnología. Han obstruido e interferido con la cooperación económica, comercial, científica y tecnológica entre otros países.

Este enfoque, con su mentalidad obsoleta de guerra fría, es contrario al espíritu de cooperación internacional y a las tendencias de nuestro tiempo. Perjudica los intereses colectivos de todos los países y está condenado al fracaso. Instamos a ciertos Gobiernos a que adopten un enfoque racional y abierto; consideren los avances científicos y tecnológicos y la cooperación internacional desde la perspectiva adecuada; y pongan fin a los ataques y restricciones infundadas a las empresas de alta tecnología de otros países.

El camino correcto para hacer frente a los problemas mundiales es el de la solidaridad y la cooperación. China pide a los países concernidos que dejen de crear divisiones en todo el mundo, incluida la región de Asia y el Pacífico; pongan fin a los enfrentamientos geográficos; dejen de trazar líneas basadas en la ideología y de utilizar medidas coercitivas para obligar a otros países a tomar partido; se abstengan de desvincular la economía de la ciencia y la tecnología; y detengan sus prácticas destructivas que afectan a la estabilidad de las cadenas de suministro y a la recuperación económica mundiales.

China concede gran importancia a la innovación científica y tecnológica y previene los riesgos tecnológicos de manera responsable. Hemos trabajado activamente para promover el consenso y la cooperación internacionales. En 2020, China puso en marcha una iniciativa de seguridad de datos a nivel mundial, en la que pedía apertura, seguridad y estabilidad en las cadenas mundiales de suministro, al tiempo que se oponía a la práctica de utilizar las tecnologías de la información para destruir infraestructuras críticas o llevar a cabo una vigilancia a gran escala. También abogaba por el respeto de la soberanía y jurisdicción nacionales y el derecho de los Estados a gestionar sus propios datos. La iniciativa ofrece un proyecto de normas internacionales sobre seguridad digital, que esperamos atraiga la participación de Gobiernos, organizaciones internacionales y múltiples partes interesadas.

Ante los formidables cambios que ha ocasionado la inteligencia artificial y sobre la base de los resultados de años de deliberaciones en las Naciones Unidas, a finales del año pasado, China presentó un documento de posición sobre la regulación de la aplicación militar de la inteligencia artificial. En ese documento se presenta un marco viable para que la comunidad internacional analice la repercusión de las aplicaciones militares de la inteligencia artificial en las normas y la ética de la gobernanza de la seguridad estratégica.

En julio, científicos de más de 20 países formularon las Directrices de Tianjin sobre Biocustodia para la Elaboración de Códigos de Conducta Científicos, que abogan por la investigación y el desarrollo responsables en el campo de la biotecnología, que es la aspiración común de la comunidad científica internacional. China se congratula de la adopción voluntaria y la promoción de las Directrices de Bioseguridad de Tianjin por todos los países y las partes interesadas pertinentes con el fin de evitar el uso indebido o el abuso de la biotecnología, reducir los riesgos asociados a la bioseguridad y promover el uso de la biotecnología en beneficio de la humanidad.

El uso de la ciencia y la tecnología con fines pacíficos y la cooperación a nivel internacional a ese respecto constituyen un derecho inalienable de todos los Estados en virtud del derecho internacional. En su septuagésimo sexto período de sesiones, la Asamblea General aprobó una resolución titulada “Promoción de la cooperación internacional para los usos pacíficos en el contexto de la seguridad internacional” (resolución 76/234). China y otros 26 países copatrocinaron esa resolución, en la que se insta a todos los países a levantar las restricciones poco razonables al derecho de los países en desarrollo

a los usos pacíficos de la ciencia y la tecnología, cumpliendo al mismo tiempo sus obligaciones internacionales en materia de no proliferación.

China se congratula de que continúe el diálogo inclusivo en el marco de la Asamblea General con el fin de mejorar la confianza mutua, crear consenso y garantizar que los países en desarrollo disfruten plenamente de su derecho al uso pacífico de la ciencia y la tecnología. De esa manera, se contribuirá a mejorar el cumplimiento de los Objetivos de Desarrollo Sostenible y a mantener la paz y la seguridad internacionales.

Sr. Kiboino (Kenya) (*habla en inglés*): Doy las gracias a la Secretaria General Adjunta DiCarlo; a mi compatriota, la Sra. Nyabola; y al Sr. Druet por sus opiniones y recomendaciones sobre el tema que nos ocupa hoy.

Cuando pensamos en el formidable papel que la tecnología digital ha desempeñado en este mismo decenio y en las repercusiones sin precedentes que la revolución digital ha tenido para la paz y la seguridad en nuestra época —y teniendo en cuenta el carácter omnipresente, trascendental y en gran medida no regulado de las tecnologías digitales—, se hace patente la necesidad de contar con una comunidad de interlocutores y agentes, entre ellos el Consejo de Seguridad, que exploren el delicado equilibrio entre, por un lado, lograr la innovación digital y, por otro lado, hacer frente a su uso malintencionado por parte de agentes estatales y no estatales en los asuntos relativos a la paz y la seguridad.

Kenya ha dado pasos importantes para garantizar la accesibilidad de Internet y proteger al máximo al país y a los ciudadanos frente a situaciones y amenazas inesperadas y perturbadoras en el ámbito digital. Sin embargo, reconocemos que la ciberseguridad no es ni puede ser el resultado de la labor de un solo país. En efecto, en estos momentos, la búsqueda tradicional de la paz y la seguridad internacionales por parte del sistema multilateral debe tener lugar también en la ciberesfera.

En ese sentido, subrayaré cinco cuestiones importantes para su consideración. La primera tiene que ver con la necesidad de reconocer que las Naciones Unidas deben apoyar a los países para hacer frente a las repercusiones de la revolución digital en la ciudadanía y en la estabilidad nacional, teniendo en cuenta, entre otras cosas, los usos indebidos de la inteligencia artificial, los macrodatos, los medios sociales y otras tecnologías digitales de vanguardia. El Consejo de Seguridad tiene la responsabilidad de velar por que las Naciones Unidas tengan la capacidad y la experiencia necesarias para desempeñar esta función.

La segunda cuestión tiene que ver con el nexo entre las tecnologías digitales y la paz, sobre todo en las etapas de transición política. Los procesos electorales conllevan una promesa democrática, pero, a menudo, conllevan más vulnerabilidades en materia de seguridad en las plataformas digitales, lo que tiene implicaciones para la cohesión ciudadana y la gestión de las crisis en los respectivos países. El 28 de octubre de 2021, cuando presidíamos el Consejo de Seguridad, Kenya convocó una reunión con arreglo a la fórmula Arria para abordar y contrarrestar el discurso de odio y evitar la incitación a la discriminación, la hostilidad y la violencia en los medios sociales. Es evidente que los formuladores de políticas se enfrentan a menudo a un dilema en su búsqueda de un equilibrio entre la libertad de expresión y la lucha contra el discurso de odio y entre la obligación democrática de rendir cuentas y la salvaguardia de la información privada y reservada. Abogamos por que se dediquen más atención e inversiones para apoyar a los Gobiernos de los países a la hora de abordar el nexo entre la ciberseguridad y la seguridad electoral, sobre todo en las situaciones de conflicto.

En tercer lugar, en cuanto a las alianzas entre el sector privado y las entidades reguladoras, en la mencionada reunión con arreglo a la fórmula Arria participaron representantes de las principales compañías tecnológicas, como Facebook, Twitter, TikTok y Google, y de la sociedad civil, quienes demostraron que dichas alianzas son posibles. Una mayor colaboración entre las empresas tecnológicas, las entidades reguladoras y las Naciones Unidas permitirá establecer mecanismos y normativas eficaces para asegurar una conducta responsable en el ciberespacio, sobre la base de principios que tengan en cuenta el bien común, de manera que se puedan tender puentes de paz entre grupos diversos y superar los temas que generan división.

Mi cuarta observación se refiere a la relación entre las tecnologías digitales y el terrorismo. Si bien las tecnologías emergentes son beneficiosas, su carácter omnipresente, programable y basado en datos ha abierto la puerta a su uso indebido por parte de grupos armados y terroristas, que aprovechan los sistemas con interfaces de usuario simplificadas para su labor de reclutamiento, radicalización, movilización de recursos, planificación y ejecución de actos terroristas. Es necesario velar por que los Estados dispongan de las capacidades necesarias para paliar la amenaza terrorista en Internet, ampliar las capacidades de investigación y colaborar en la reducción de los niveles de radicalización en línea y de los flujos financieros ilícitos, así como en la detección y eliminación de contenidos extremistas en línea.

Mi quinta observación tiene que ver con la inclusión y con la protección de la participación. Creemos que la responsabilidad gubernamental de asegurar el acceso a Internet comporta, además, la protección de quienes accedan a las plataformas digitales, incluidas las redes sociales. En concreto, sigue siendo crucial proteger las mujeres que participen en los procesos de paz y seguridad. Por ello, los Estados deben impulsar la rendición de cuentas y el enjuiciamiento de los autores de ataques en línea y de actos de intimidación, publicación de soportes privados o violencia física contra las mujeres participantes en la búsqueda de la paz. Además, en el contexto de la preservación de los pilares de protección y participación de la agenda sobre las mujeres y la paz y la seguridad, el Consejo de Seguridad debe tomar medidas específicas, en especial para que se sancione con más peso cualquier tipo de intimidación en línea contra las mujeres que intervengan como ponentes ante el Consejo.

Sr. Gómez Robledo Verduzco (México): Sra. Presidenta: Deseo, en primer lugar, agradecerle por haber convocado a esta sesión sobre un tema de dimensiones cuasi infinitas y que nos invita a reflexionar, entre otros aspectos, sobre cómo adaptar el trabajo de las Naciones Unidas frente a los desafíos que plantea el uso de la tecnología digital para el mantenimiento de la paz y la seguridad internacionales. Agradecemos, igualmente, a los ponentes de esta mañana —la Secretaria General Adjunta DiCarlo, la Directora de Advox y el profesor Druet, de la Universidad McGill— por sus excelentes análisis y las propuestas que hicieron.

Si queremos ver las cosas de frente, debemos partir del principio de que el uso de la tecnología digital debe nutrirse, en primerísimo lugar, de la defensa de la democracia y los derechos humanos. Son dos aspectos inseparables. En ese sentido, México reafirma su compromiso, que ha mantenido a lo largo de los años, con un ciberespacio libre, abierto, estable y seguro, en el cual es plenamente aplicable el derecho internacional, incluyendo el derecho internacional de los derechos humanos, el derecho internacional humanitario, el derecho penal internacional y otras fuentes jurisprudenciales que establecen, por ejemplo, el derecho a la privacidad. Recordamos los acuerdos que, a nivel intergubernamental, ya hemos alcanzado en los procesos que están en curso, particularmente en materia de ciberseguridad, mediante los informes del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y del grupo de

trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. De igual forma, debemos tener presentes otros procesos también en curso, como el 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.

Ahora bien, es necesario ir más lejos y buscar soluciones innovadoras a los retos actuales para el mantenimiento de la paz, en particular, a través del fortalecimiento de las capacidades tecnológicas digitales en las operaciones de paz y misiones políticas especiales, como ya se mencionó en las intervenciones de esta mañana. El uso de la tecnología puede contribuir de manera muy positiva a mejorar la alerta temprana para la detección de amenazas emergentes y la prevención de las crisis humanitarias y las violaciones de los derechos humanos, así como para fortalecer las medidas de protección y asistencia a la población y la infraestructura civiles, incluyendo la lucha contra el tráfico ilícito de armas y la realización de acciones de desminado.

Las nuevas tecnologías son particularmente prometedoras en ámbitos como la asistencia médica, incluyendo la provisión de asistencia oportuna en materia de salud mental y psicosocial, de manera rutinaria y también en los casos de emergencia. Tanto el personal de las misiones de paz como la población civil afectada por crisis humanitarias pueden beneficiarse de la flexibilidad y las oportunidades que ofrece la telemedicina. Por otra parte, hemos constatado que el uso de tecnologías de energía renovable puede aumentar la seguridad y la protección del personal de las Naciones Unidas, la eficiencia de las misiones y su sostenibilidad. Frente a un entorno creciente de desinformación, como ya ha sido subrayado esta mañana, el uso de las redes sociales es un elemento central para fortalecer las relaciones entre las misiones de paz y las comunidades en las que operan estas misiones. Por ello, las disposiciones de la resolución 2589 (2021) y la declaración de la Presidencia S/PRST/2021/17, con las que este Consejo de Seguridad reconoció que la tecnología puede contribuir a que las misiones de mantenimiento de la paz comprendan mejor los entornos en los que operan, son absolutamente indispensables y deben permitirnos una mejor recopilación, análisis y difusión de los datos.

Igualmente, tomamos nota de la Estrategia del Secretario General para la Transformación Digital del Mantenimiento de la Paz de las Naciones Unidas en materia de nuevas tecnologías y de datos, en seguimiento

a la iniciativa Acción por el Mantenimiento de la Paz Plus. La plena instrumentación de la Estrategia mencionada requiere de una mayor coordinación entre el sistema de las Naciones Unidas y los actores en el terreno, así como la cooperación con organizaciones regionales, el sector privado, la sociedad civil y, por supuesto también, el sector académico.

En la pasada Conferencia Ministerial de las Naciones Unidas sobre el Mantenimiento de la Paz, México suscribió la iniciativa impulsada por la República de Corea sobre tecnología y creación de capacidad médica en el mantenimiento de la paz, la cual tiene entre sus objetivos maximizar el uso de las tecnologías disponibles para la mejora del conocimiento de la situación y la alerta temprana, responder a la desinformación en situaciones de conflicto, mejorar la inteligencia en ciberseguridad y promover el avance en las capacidades para el análisis de datos e información.

En última instancia, la resolución 75/316, promovida por México en la Asamblea General, subrayó el impacto que tiene el cambio tecnológico rápido en la consecución de la Agenda 2030 para el Desarrollo Sostenible y, por tanto, en la paz y la estabilidad internacionales. Subrayamos la importancia de la Hoja de Ruta para la Cooperación Digital y los elementos presentes en el informe “Nuestra Agenda Común” (A/75/982).

Sr. Agyeman (Ghana) (*habla en inglés*): Para empezar, me gustaría dar las gracias a los Estados Unidos por haber organizado la sesión informativa de hoy sobre el uso de las tecnologías digitales en el mantenimiento de la paz y la seguridad internacionales.

También doy las gracias a la Secretaria General Adjunta Rosemary DiCarlo por su esclarecedora presentación informativa, así como a la Directora del proyecto Advox de Global Voices sobre derechos digitales, Sra. Nanjala Nyabola, y al Profesor Adjunto del departamento de estudios sobre la paz y la seguridad internacionales de la Universidad McGill, Sr. Dirk Druet, por la información adicional que han proporcionado.

Al reconocer el carácter omnipresente de las tecnologías digitales en todo el mundo, Ghana comparte la opinión de que dichas tecnologías pueden desempeñar un papel importante en el mantenimiento de la paz internacional y, por tanto, se deben aprovechar para mejorar nuestra seguridad colectiva. Creemos que, desde el respeto de los imperativos de la soberanía nacional y la integridad territorial, las tecnologías digitales, que trascienden los límites territoriales, pueden emplearse para reforzar los objetivos de la diplomacia preventiva,

a través de la mejora de la conciencia situacional, en la activación de la alerta temprana, la detección de las amenazas emergentes y la superación de las diferencias sociales, ya que se movilizan puntos de vista y posiciones dispares hacia un conjunto constructivo y coherente con objeto de reforzar los objetivos de paz.

En situaciones de gestión de conflictos, también conocemos los beneficios que pueden aportar las tecnologías digitales en el análisis de riesgos, la mejora de los plazos necesarios para proteger a la población civil y la infraestructura civil y el rigor que aportan para mejorar el cumplimiento de los mandatos de las operaciones de paz y mejorar la seguridad del personal uniformado y de otro tipo. Las tecnologías digitales también pueden apoyar firmemente los esfuerzos en pro de la consolidación de la paz y la reconstrucción de las sociedades fracturadas por la guerra.

Ghana cree que los beneficios infinitos que las tecnologías digitales pueden aportar para potenciar los esfuerzos en pro del mantenimiento de la paz y la seguridad internacionales solo pueden aprovecharse mejor si existe un entendimiento común del marco normativo que sustenta ese enfoque mejorado y complementario para aprovechar las herramientas modernas disponibles en pro de la pacificación de nuestro mundo. Así, somos conscientes de que, no obstante la naturaleza benigna de las tecnologías digitales, estas también pueden exacerbar la inseguridad mundial si no se emplean de forma responsable. Pueden profundizar la desconfianza si persiste, en sociedades tensas y frágiles, la percepción de que fuerzas exógenas están manipulando la voluntad de la población inculcando valores que pueden ser ajenos a esas sociedades.

También observamos el uso malicioso que se ha hecho de las tecnologías digitales, en algunos casos por parte de agentes estatales y no estatales, para desinformar y manipular a la población, amenazar y acosar a determinados activistas y periodistas y alimentar la discriminación de forma que se socavan la unidad y la cohesión nacionales. También suscita una gran preocupación la forma en que esas tecnologías se han empleado para reclutar y radicalizar a personas en grupos terroristas, organizar atentados terroristas y financiar actividades terroristas.

Con el telón de fondo del gran potencial que albergan las tecnologías digitales en el refuerzo de las herramientas disponibles para el mantenimiento de la paz y la seguridad internacionales, pero conscientes de sus consecuencias negativas, quisiéramos formular

algunas observaciones adicionales. Como se ha indicado anteriormente, el uso de las tecnologías digitales para el mantenimiento de la paz y la seguridad internacionales debe partir de una convergencia y estar basado en principios que respeten la soberanía nacional y promuevan valores universales. A ese respecto, creemos que las Naciones Unidas tienen un papel indispensable que desempeñar para potenciar el efecto positivo de las tecnologías digitales en la paz mundial. Por ejemplo, si se aprovechan los compromisos asumidos en el marco de la Estrategia del Secretario General para la Transformación Digital del Mantenimiento de la Paz de las Naciones Unidas, cuyo objetivo radica en aprovechar las oportunidades que ofrecen las tecnologías digitales, las misiones se podrían adaptar a la dinámica cambiante de los conflictos y aprovechar las mejoras en la eficiencia. Además, las enseñanzas extraídas por el Departamento de Asuntos Políticos y de Consolidación de la Paz en los esfuerzos de mediación durante la pandemia de enfermedad por coronavirus a través del uso de las tecnologías digitales pueden servir como una vía aceptable para el establecimiento de marcos duraderos para colaboraciones de esa índole con poblaciones más amplias en pro de la causa de la paz.

En segundo lugar, la capacidad de los Gobiernos nacionales para mejorar su ciberseguridad debe tener un papel central en el desarrollo de un marco sólido para el uso de las tecnologías digitales. El uso malintencionado de las tecnologías digitales por parte de terroristas y grupos extremistas y la tendencia a la realización de ciber guerras hacen necesario que los países vulnerables, como algunos de África donde existen fragilidades, obtengan el apoyo necesario para reforzar su capacidad digital, en línea con la Estrategia de Transformación Digital para África (2020-2030) de la Unión Africana. Esos esfuerzos de creación de capacidades deben comprender la recopilación, el procesamiento, el uso y el análisis de las nuevas tecnologías y de su repercusión en la seguridad. A ese respecto, el papel de apoyo de la Dirección Ejecutiva del Comité contra el Terrorismo es encomiable, y acogemos con satisfacción más esfuerzos de este tipo.

En tercer lugar, los Estados también tienen un papel fundamental que desempeñar a la hora de concebir políticas en las que se impida el uso indebido del ciberespacio a través de elementos que, entre otras cosas, fomenten las inversiones en la infraestructura nacionales esencial, promuevan el contenido responsable de los medios de comunicación y faciliten la detección temprana, la investigación y el enjuiciamiento de los

delincuentes. Los Estados deben cumplir su determinación de defender la Carta de las Naciones Unidas respetando el derecho internacional de los derechos humanos de manera que se garantice que, cuando se recojan, almacenen, procesen, utilicen, transfieran y divulguen datos personales, se respete y proteja la privacidad de las personas. Además, acogemos con satisfacción las medidas por las que se anima a las empresas a respetar el derecho internacional de los derechos humanos y las normas empresariales, sobre la base de los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos.

En cuarto lugar, conscientes de la eficacia de los acuerdos regionales en la prevención de conflictos a través de mecanismos de alerta temprana y en la consolidación de la paz en situaciones de posconflicto, instamos firmemente a que se fortalezcan las asociaciones de tecnología digital entre los sistemas multilaterales globales y los organismos regionales. Animamos a que se apoye la aplicación de los tratados existentes, como el Convenio sobre la Ciberdelincuencia y el Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales, también conocido como Convenio de Malabo, y creemos que cabe profundizar aún más los mecanismos de alerta temprana, como los de la Comunidad Económica de los Estados de África Occidental y la Unión Africana, a través de un sólido apoyo mundial.

Asimismo, mediante el apoyo a las plataformas regionales de inteligencia y de intercambio de información se podría mejorar la detección temprana de los planes expansionistas de las redes terroristas, especialmente en África Occidental y en relación con sus actividades en línea. Por otra parte, es preciso mantener y potenciar la acción para cercenar la financiación del terrorismo, particularmente en la economía sumergida, donde las criptomonedas se han convertido en la vía preferida para financiar actividades terroristas. Si bien la colaboración entre el Grupo Intergubernamental de Acción contra el Blanqueo de Dinero en África Occidental y los centros nacionales de inteligencia financiera de África Occidental ha permitido lograr resultados importantes, sería necesario seguir profundizando en su acción.

Antes de concluir, quisiera mencionar el empeño de Ghana de potenciar el uso de las tecnologías con fines pacíficos gracias a las medidas que se han adoptado para fortalecer el ecosistema nacional de las tecnologías de la información y las comunicaciones. Además de la institucionalización de un mes nacional de sensibilización sobre la ciberseguridad, destinado a mejorar la conciencia que

tiene toda la sociedad sobre las amenazas cibernéticas, la puesta en marcha de equipos sectoriales de respuesta a emergencias informáticas en instituciones clave, como la Autoridad Nacional de Comunicaciones, el Banco Central y la Agencia Nacional de Tecnologías de la Información, han mejorado la resiliencia del ciberecosistema en los servicios en línea, el sector financiero y las empresas del Gobierno. Por lo tanto, abogamos por un enfoque de toda la sociedad para desarrollar la resiliencia en cuanto al nexo entre la paz y la seguridad, incluidas las asociaciones con el sector privado, las organizaciones de la sociedad civil y los gigantes de la tecnología, cuyo papel cada vez más importante debe ponerse al servicio del bien público. Asimismo, las mujeres y los jóvenes son agentes críticos del cambio y seguirán siendo cruciales para potenciar la incidencia positiva de las tecnologías en la seguridad mundial.

Obligada al objetivo colectivo de potenciar todas las herramientas disponibles, Ghana estima que las iniciativas multilaterales y regionales pueden aprovechar eficazmente las tecnologías en pro de los objetivos de la paz y la seguridad mundiales.

Sr. Nebenzia (Federación de Rusia) (*habla en ruso*): Queremos dar las gracias a nuestros ponentes por sus exposiciones informativas.

Las tecnologías digitales han transformado el mundo y se han convertido en parte integrante de sus procesos económicos, políticos y sociales. Había esperanzas de que se convirtieran en un motor de progreso económico y social y que simplificarían la comunicación y ayudarían a la humanidad a hacer la transición hacia una nueva etapa de desarrollo digital.

Durante la pandemia de enfermedad por coronavirus, fue gracias a las tecnologías de la información y las comunicaciones (TIC) que se preservaron los puestos de trabajo y la unidad del mundo dividido por la cuarentena. Los servicios públicos prestados por el Gobierno, incluida la labor de los hospitales, los bancos y el sector financiero en general, las escuelas y otras instituciones fundamentales para la sociedad, pasaron a verse casi totalmente vinculados a las TIC. No es exagerado decir que la humanidad es hoy mucho más dependiente de las TIC que en cualquier otro momento de su historia.

Sin embargo, las esperanzas de que las TIC fueran una fuerza inequívoca para el bien no se han cumplido. El culpable no es la tecnología, sino el hecho de que esta se haya utilizado para alcanzar objetivos geopolíticos y para imponer la hegemonía. Eso es así no solo en el entorno físico, sino también en el entorno en línea.

En los últimos años, la manipulación de la información ha adquirido proporciones amenazantes. Ha surgido todo un ejército de pseudoinvestigadores de organizaciones no gubernamentales que, a instancias de los Gobiernos occidentales, están produciendo grandes cantidades de lo que llaman investigaciones y que, en realidad, generan y difunden numerosas mentiras e información no verificada de fuentes de dominio público para empañar la reputación de los países incómodos para Occidente. Un ejemplo tristemente célebre de ello son los Cascos Blancos y Bellingcat. Se han distinguido por sus burdas fabricaciones en interés de la propaganda occidental sobre el expediente químico sirio, la historia del vuelo MH-17 de Malaysia Airlines y otros muchos asuntos de relieve. Los expertos los han pillado repetidamente con las manos en la masa, por así decir, y han señalado las incoherencias de sus conclusiones, que no tienen nada que ver con el periodismo de investigación profesional e independiente y a las que llegan en violación todos los principios más básicos.

Nos sentimos profundamente preocupados por una nueva tendencia: se está librando una guerra de información que no solo se aparta completamente de la realidad, sino que, además, tiene el objetivo de falsearla y sustituirla por completo. La verdad se ve suplantada por un intenso flujo de información y correo basura de carácter ideológico, para no conceder a la audiencia la más mínima oportunidad de tener acceso a información objetiva.

Un ejemplo destacado de ello es la información que desatan los medios de comunicación occidentales, bajo la dirección de sus Gobiernos, en relación con la muerte de civiles en Bucha, en cuyo caso se culpó a los militares rusos. Todos los hechos y pruebas objetivas se ocultaron bajo la mesa y, en su lugar, se difundieron falsificaciones descaradas. Bajo la presión de los hechos, incluso los medios de comunicación occidentales se vieron finalmente obligados a admitir que muchos residentes pacíficos de Bucha no murieron por heridas de bala, como afirmaba Ucrania, sino por proyectiles de artillería obsoletos que habían sido utilizados por las fuerzas armadas ucranianas cuando bombardearon esa ciudad. Ahora lanzan nuevas acusaciones falsas para desviar la atención de la responsabilidad evidente de las fuerzas armadas de Ucrania por el acto de provocación. Del mismo modo, también guardan silencio sobre los ataques contra Kramatorsk, después de que una investigación revelara pruebas que muestran claramente la participación de las fuerzas armadas ucranianas.

En los últimos meses, la labor colectiva del Ministerio de la Verdad occidental, o más bien, del Ministerio

de la Mentira, ha alcanzado su cenit. Se ha desatado una campaña de desinformación y manipulación de la opinión pública sin precedentes en su alcance e intensidad contra Rusia. Los medios de comunicación occidentales, no conocidos ya por su objetividad, se han convertido finalmente en portavoces de la burda propaganda del Estado, así como en fábricas de noticias falsas.

Los gigantes de las TIC, que han monopolizado el ámbito de las redes sociales y los sitios de emisión de vídeos, no se están comportando mejor. Las plataformas digitales se han quitado por fin sus máscaras y ya no intentan ocultar su sesgo político. Están bloqueando toda cuenta cuyo contenido no se ajuste a la agenda que dictan las élites occidentales. La corporación Meta ha permitido explícitamente el discurso de odio y los llamamientos a la violencia contra los rusos y los rusoparlantes en sus plataformas.

Los Estados que se autodenominan “comunidad de democracias” están diseñando de hecho un verdadero cibertotalitarismo. Quieren crear un mundo en el que ellos —y solo ellos— tengan el control total de los flujos de información y determinen lo que es verdad y lo que la audiencia necesita leer y ver. Todo punto de vista alternativo es inmediatamente estigmatizado como desinformación y propaganda, y los hechos incómodos se dejan de lado. Se cierran canales de televisión rusos, se expulsa a periodistas rusos y se bloquea el acceso a sitios web rusos. ¿Es eso la llamada libertad de acceso a la información? Esperamos que eso sea lo que los organizadores de la sesión de hoy entendían por abuso de las restricciones de acceso a los recursos de Internet con el pretexto de garantizar la seguridad nacional.

El ataque informativo rusóphobo ha sido dirigido por sus iniciadores contra diversas esferas de actividad, incluidas las que no tienen ninguna relación con la política, como la educación, la cultura y el deporte. Se trata de una violación flagrante del principio básico de la inadmisibilidad de la discriminación por motivos étnicos. Además de la agresión informativa dirigida contra la mente de la población, se ha orquestado una campaña para socavar la propia infraestructura de las TIC mediante la organización de ataques informáticos. En Kiev se anunció recientemente la creación de un ciberejército y se reconoció abiertamente la existencia de esos ciberataques contra objetivos rusos y bielorrusos. Además, los patrocinadores occidentales del régimen de Kiev no solo no trataron de impedirlo, sino que cultivaron deliberadamente ese ejército de *hackers* sin pensar en las consecuencias. Como sabemos, la Organización del Tratado del Atlántico Norte promovió recientemente las tareas correspondientes, en

el marco del ejercicio de ciberseguridad Locked Shields (Escudos Bloqueados) en el que actualmente participan las fuerzas armadas ucranianas.

En abril, Washington anunció una recompensa de 10 millones de dólares para quien pudiera justificar la teoría de que la inteligencia rusa estaba supuestamente implicada en los ciberataques contra los Estados Unidos. Se ha hecho caso omiso de nuestros llamamientos reiterados a abordar las cuestiones a través de los organismos competentes.

Los Gobiernos occidentales recurren deliberadamente a grupos de *hackers*, y, a menudo, a usuarios corrientes, para la realización de ciberataques. Se suben al dominio público herramientas e instrucciones detalladas para la preparación de ataques informáticos y en las redes sociales se lleva a cabo una labor masiva de agitación en relación con la organización de ataques de *hackers* contra infraestructura rusa.

En ese contexto, no nos sorprendió la designación, el pasado 27 de abril, de Nina Yankovic, nacida en el oeste de Ucrania y conocida por haber liderado la campaña de blanqueo del neonazismo en Ucrania y por haber difundido información sobre el *Russiagate* (que nunca existió), al frente de la denominada Junta de Gobernanza de la Desinformación, en el Departamento de Seguridad Nacional de los Estados Unidos. Hace poco quedó claro que Nina Yankovic recibía instrucciones directas de la que fue rival de Trump en las elecciones, Hillary Clinton. Incluso en los Estados Unidos, este acto de cinismo descarado ha ocasionado un escándalo. Yankovic ha tenido que dimitir, y el proyecto se ha suspendido por el momento. No obstante, estamos seguros de que se reactivará de un modo u otro, ya que, aparte de promover las noticias falsas y la desinformación, nuestros colegas occidentales ya casi no tienen medios diplomáticos a su disposición.

Además de la inyección de armas convencionales en Ucrania por parte de Occidente, existe una distribución paralela e incontrolada de ciberarmas y otras técnicas disponibles para su uso. Un gran número de personas están adquiriendo conocimientos prácticos. Según Zelenskyy, hay más de 300.000 combatientes en su denominado “ejército informático”.

Se está creando un ciberejército incontrolable. Tras desarrollar sus capacidades bajo el mando de Estados Miembros en Ucrania al tiempo que ataca a Rusia, no se detendrá aquí. No se trata de un ejército normal. Los especialistas saben bien lo difícil que resulta rastrear las actividades de los *hackers*, localizar su origen

y suprimirlas. La movilización de *hackers* por parte de Estados Miembros se extenderá por todo el mundo, lo que supondrá, entre otras cosas, una amenaza para los ciudadanos de los países occidentales.

La militarización del espacio digital que está llevando a cabo Occidente aumenta en grado sumo la amenaza de un enfrentamiento militar directo, sobre todo porque el régimen de Kiev maneja activamente las provocaciones en el espacio de la información según técnicas occidentales. Sin embargo, sus consecuencias podrían ser aún más terribles. Los ataques informáticos contra infraestructura crítica pueden desembocar en bajas humanas reales a gran escala, por no hablar del riesgo de identificar erróneamente a los autores cuando se produzcan ataques de bandera falsa, mucho más fáciles de organizar en el espacio virtual que en la vida real. En tal caso, se multiplicarían los riesgos de una escalada involuntaria y de un intercambio mutuo de ciberagresiones.

Las acciones temerarias del régimen de Kiev podrían conducir a un enfrentamiento a gran escala en el ciberespacio que involucraría a otros países. La OTAN ya ha extendido al espacio de la información el derecho de legítima defensa colectiva, en virtud del artículo 5. La responsabilidad de tal escalada recaerá por completo en los países occidentales, que están alentando la temeridad de los dirigentes de Kiev.

Ante esa amenaza, no cabe duda de que lucharemos contra cualquier intento de socavar la seguridad de la información de Rusia. Ahora bien, insto una vez más a los miembros del Consejo a que piensen en el peligro que supone arrastrar al mundo a una confrontación en el ciberespacio, lo cual no es menos peligroso que el empleo de armas de destrucción masiva. Llevamos más de dos decenios tratando de evitar esta posibilidad.

Permítaseme recordar que Rusia fue la primera en plantear la cuestión de la seguridad de la información internacional en las Naciones Unidas, en 1998, y en lograr que figurase de manera permanente entre los temas de los que se ocupa la Organización. También insistimos en que las Naciones Unidas crearan plataformas de negociación, inicialmente entre expertos y, después, abiertas a todos los Estados Miembros. En todos esos momentos, tuvimos que afrontar la firme oposición de nuestros colegas occidentales, quienes aseguraban que podían arreglárselas sin las Naciones Unidas. El mundo sabe bien cómo se las arreglan sin ellas.

Lo que buscamos es un compromiso internacional por el que todos los Estados se propongan no utilizar las TIC con fines militares. Reclamamos la

desmilitarización del espacio informativo. Durante todos estos años, hemos venido proponiendo proyectos de instrumentos internacionales específicos, como un concepto universal para garantizar la seguridad de la información internacional y, en nombre de la Organización de Cooperación de Shanghái, un proyecto de código de conducta responsable en este ámbito.

¿Qué decir de nuestros colegas occidentales? Durante todos estos años, han estado desarrollando abiertamente su ciberpotencial ofensivo y elaborando normas para su uso. Basta recordar el cínico *Manual de Tallin sobre el derecho internacional aplicable a la ciberguerra*, que regula en detalle la manera presuntamente humana de librar la guerra informática.

Así pues, ¿quién de nosotros se ha estado preparando para la ciberguerra durante todos estos años? ¿Rusia, que reclamó una prohibición del uso de las TIC con fines políticos y militares y que está dispuesta a asumir las obligaciones correspondientes, o los países occidentales, que rechazaron repetidamente todas esas iniciativas para mantener su completo libre albedrío en el espacio de la información?

No se debe permitir que la esfera digital se convierta en un ámbito de confrontación geopolítica. Se trata de una cuestión existencial para la humanidad. Ahora, más que nunca, es necesario un discurso responsable, que tenga por objeto la búsqueda de soluciones prácticas. Es nuestro deber apoyarlo, independientemente del clima político. Abogamos por que se hable de manera despolitizada sobre todos los aspectos de la labor de garantizar la seguridad de la información internacional, en un foro especializado y bajo los auspicios de la Asamblea General: el Grupo de trabajo de composición abierta. Creemos que nuestra sesión de hoy no es, de ningún modo, un sustituto de las actividades de ese grupo.

Sra. Nusseibeh (Emiratos Árabes Unidos) (*habla en inglés*): Los Emiratos Árabes Unidos desean dar las gracias a los Estados Unidos por haber organizado esta sesión dedicada a una cuestión de creciente importancia, que el Consejo de Seguridad, por derecho propio y en opinión de los Emiratos Árabes Unidos, debería afrontar de manera conjunta, más allá de conflictos específicos. Damos las gracias también a la Secretaria General Adjunta DiCarlo, la Sra. Nyabola y el Sr. Druet por sus esclarecedoras exposiciones informativas de hoy.

Las tecnologías digitales avanzan a una velocidad vertiginosa. Pensemos en 1989, cuando se creó la *world wide web*. A finales del decenio siguiente, Larry Page y Sergey Brin habían inventado Google. Poco sabíamos,

por entonces, que esa nueva idea, originada en un garaje de California, iba a cambiar nuestras vidas para siempre. Un decenio más tarde, Google estaba en los teléfonos inteligentes de todos y se había convertido en un elemento indispensable del trabajo y de la vida, lo que comportó avances y cambios enormes.

Imaginemos ahora que, tal como hemos escuchado, el lado perverso de la tecnología avanza hoy a esa misma velocidad vertiginosa frente a nuestros ojos. Por ejemplo, el avance constante de las tecnologías digitales está multiplicando lo que se puede hacer con dispositivos como las aeronaves no tripuladas. En un futuro próximo, existirá la posibilidad de que enjambres de aeronaves no tripuladas, en manos de grupos terroristas, lleven a cabo ataques transfronterizos, utilizando la tecnología de reconocimiento facial y otras opciones habilitadas por la inteligencia artificial, sin que se pueda atribuir su autoría a ninguna entidad, ya sea estatal o no estatal. ¿Cómo responderán los Estados, incluidos los que están sentados en torno a esta mesa, ante ese tipo de ataques en el futuro, de manera legal y de conformidad con el derecho internacional humanitario?

Para evitar ese futuro distópico, debemos adoptar medidas urgentes ahora, en las Naciones Unidas, en el Consejo de Seguridad y en otros foros. Lo que es evidente es que no podemos esperar que surjan respuestas significativas en debates políticos y éticos que perduran desde hace más de dos decenios y que no están a la altura de tecnologías que se han vuelto omnipresentes y que tienen potencial para ser utilizadas de esas maneras tan destructivas.

No hay duda de que las tecnologías digitales conllevan su parte de riesgos y desafíos, sobre todo porque pueden servir como multiplicador de fuerza para los grupos terroristas. Ahora bien, como también hemos escuchado, esa no es la historia completa.

Como se ha dicho hoy, las tecnologías digitales pueden ser también un factor facilitador de la paz. Por ejemplo, los sistemas de alerta ante catástrofes naturales, basados en las tecnologías y los datos más recientes, nos permiten anticipar fenómenos meteorológicos extremos, como sequías, huracanes e inundaciones, y posicionar la ayuda en consecuencia. Los sucesivos programas de medidas anticipatorias en Somalia han ayudado a las comunidades a hacer frente a situaciones devastadoras de escasez de agua y de sequía. Gracias a esas tecnologías, la Oficina de Coordinación de Asuntos Humanitarios y otros asociados han podido mitigar la pérdida de medios de subsistencia y la disminución

del consumo de alimentos, garantizar el acceso al agua y lograr que los niños sigan yendo a la escuela, como les corresponde. Con una información adecuada, la comunidad internacional está en mejores condiciones para responder a las amenazas a la seguridad climática. Gracias a ella, se salvan vidas y se ayuda a evitar que la fragilidad se convierta en un factor de inestabilidad.

Teniendo en cuenta la doble naturaleza de las tecnologías digitales, ha llegado el momento de que el Consejo vaya más allá de contemplar el problema y discuta las formas concretas en que puede aprovechar las innovaciones tecnológicas para contribuir a la paz y la seguridad sostenibles. Hoy, los Emiratos Árabes Unidos desean abordar cinco cuestiones concretas.

En primer lugar, como han mencionado otros, no se debe permitir que grupos terroristas y extremistas como Dáesh, Al-Qaida y muchos otros utilicen Internet para propagar sus ideas y manipular las redes sociales y a sus miles de millones de usuarios. Las empresas tecnológicas invierten cada vez más en herramientas de detección basadas en la inteligencia artificial y en equipos de moderación humana para eliminar estos contenidos de sus plataformas. Sin embargo, los Gobiernos tienen claro desde hace tiempo que no basta con seguir como hasta ahora, porque los terroristas y extremistas siguen radicalizándose y reclutando en línea. Este problema no se limita en absoluto a los países en desarrollo. Los autores de varios delitos de odio recientes de gran repercusión cometidos contra minorías religiosas y étnicas en gran parte de Europa y los Estados Unidos se han radicalizado a través de estas plataformas en línea, al igual que innumerables reclutas de Dáesh de todo el mundo. Por ello, aunque en los últimos años hemos visto avances en el fortalecimiento de los marcos normativos y legislativos para proteger a los usuarios de los contenidos terroristas y extremistas, es evidente que debemos acelerar estas medidas, ya que el marco normativo internacional no se está poniendo al día. Se trata de una tarea que no solo incumbe a las empresas tecnológicas, sino también a los Gobiernos.

En segundo lugar, debemos hacer frente a los efectos perniciosos de las campañas de desinformación e información engañosa en línea que se sirven de las plataformas de las redes sociales, incluso en relación con las operaciones de paz y las actividades humanitarias. Hay que salvaguardarlas. Hemos visto casos en los que el personal de mantenimiento de la paz y humanitario, que ya pone en peligro su vida para proteger a los civiles, se ve aún más amenazado por la difusión de información errónea y desinformación contra ellos. Se

necesitan respuestas eficaces para luchar contra la desinformación a diversos niveles, por ejemplo, mediante la regulación del sector privado, la verificación de datos, el etiquetado de la información y campañas de alfabetización mediática. Deberíamos acoger de buen grado las sugerencias que han hecho hoy los ponentes de que las Naciones Unidas deberían aumentar su capacidad y sus habilidades en este sentido.

En tercer lugar, debemos aprovechar las tecnologías digitales para aumentar la protección de los civiles. Por ejemplo, en el mundo físico, los médicos y ciertos agentes humanitarios utilizan los emblemas de la cruz roja o la media luna roja para señalar que están protegidos en virtud del derecho internacional humanitario. Dado que estos agentes se enfrentan a nuevas amenazas digitales por los ataques contra sus redes troncales digitales, deberíamos empezar a plantearnos si se podría crear un emblema digital para señalar claramente que los agentes médicos y humanitarios nunca deben ser objeto de ataques, ni en el mundo virtual ni en el real. El emblema no solo debería resaltar la idea de que dichas redes deben ser protegidas, sino también que hay que rendir cuentas por cualquier violación y que el derecho internacional es aplicable aquí.

En cuarto lugar, la innovación digital está teniendo repercusiones en el mundo físico, ya que se están multiplicando las posibilidades de lo que pueden hacer dispositivos tales como los drones. Lo he mencionado al principio de mi intervención. Ahora los drones disponibles en el mercado pueden volar más rápido, viajar más lejos, transportar cargas mayores y aprovechar la inteligencia artificial y otras herramientas para operar sin control manual. Y los drones no solo operan en el aire. El 3 de marzo de 2020, como informé al Consejo, el grupo terrorista huzí utilizó una embarcación teledirigida cargada de explosivos para atacar un petrolero frente a la costa del Yemen. De haber salido bien, el ataque habría tenido consecuencias devastadoras, no solo para el petrolero y su tripulación, sino para el medio ambiente, las rutas de abastecimiento mundiales y las comunidades locales de la costa yemení que dependen del mar para su subsistencia. Nos encontramos en un estado de naturaleza hobbesiano en lo que respecta al uso de la tecnología por parte de actores no estatales con superpoderes. La inacción no es una opción porque cuando no hay regulación, solo estamos fomentando la proliferación.

Hoy en día está claro, por las pruebas y otros informes que lo demuestran, que los grupos terroristas y los actores no estatales tienen cada vez más acceso a

estas tecnologías. Condenamos enérgicamente su uso para llevar a cabo ataques transfronterizos, dirigidos contra civiles o infraestructuras civiles, infringiendo el derecho internacional. Pero esta amenaza no hará más que aumentar a medida que avance la tecnología, y debe abordarse en las Naciones Unidas. Los Gobiernos deben mejorar la coordinación, apoyar las medidas de creación de capacidades e intercambiar buenas prácticas y orientaciones para contrarrestar esa amenaza.

Por último, hemos hablado de la importancia de las tecnologías digitales para proteger a los agentes humanitarios. Hablemos ahora de su función a la hora de ampliar la acción humanitaria. Innovaciones digitales como la inteligencia artificial, el análisis predictivo, las transferencias digitales de efectivo y la tecnología de cadenas de bloques pueden mejorar las operaciones humanitarias. Estas tecnologías emergentes no solo ayudan a los agentes humanitarios a prever las crisis y prepararse para ellas, sino que también les permiten actuar con mayor rapidez y eficacia cuando estas se producen.

A la hora de hablar de la innovación digital, no debemos olvidar la brecha digital. Se calcula que el 37 % de la población mundial —casi 3.000 millones de personas— no ha utilizado nunca Internet. La brecha sigue siendo grande y afecta de manera desproporcionada a las mujeres y las niñas. Solo el 19 % de las mujeres de los países menos adelantados utilizan Internet, un 12 % menos que los hombres. La desigualdad en el mundo físico se reproduce claramente en el mundo digital. Ahora que estamos reflexionando sobre cómo puede ayudarnos la innovación a mejorar la eficacia de nuestra labor, demos prioridad a los que aún no han visto los dividendos de los avances tecnológicos que ahora son comunes en otras partes del mundo.

Los Emiratos Árabes Unidos, uno de los primeros defensores de las tecnologías de vanguardia, están aprovechando sus ventajas tanto en su territorio como en el extranjero. Por eso, hace cuatro años, defendimos la creación por parte del Secretario General del Panel de Alto Nivel sobre la Cooperación Digital, ya que reflejaba nuestra convicción de que las tecnologías digitales pueden contribuir de forma positiva a la paz y la seguridad mundiales. Apoyamos activamente las iniciativas para su aplicación y nos alienta ver que en el informe “Nuestra Agenda Común” (A/75/982) del Secretario General se menciona la idea de establecer un pacto digital global. Todos tenemos que seguir defendiendo esta labor multilateral.

Los Emiratos Árabes Unidos seguirán trabajando con todos los reunidos aquí y con todas las partes

interesadas para velar por que el mundo se beneficie de las tecnologías digitales como elemento clave para lograr sociedades más resilientes, equitativas e inclusivas.

Sr. De Oliveira Marques (Brasil) (*habla en inglés*): El Brasil agradece a la Presidencia de los Estados Unidos la organización de la sesión informativa de hoy sobre las repercusiones de las tecnologías digitales para el mantenimiento de la paz y la seguridad internacionales. También expresamos nuestro agradecimiento a la Secretaria General Adjunta DiCarlo, a la Sra. Nyabola y al Sr. Druet por sus interesantes presentaciones.

El proceso de transformación digital conlleva grandes beneficios y oportunidades para la humanidad, incluso para construir la paz y el entendimiento y para empoderar a los grupos infrarrepresentados y vulnerables.

La pandemia de enfermedad por coronavirus ha mostrado a la sociedad las grandes ventajas de las tecnologías digitales, que han demostrado ser instrumentos eficaces para poder seguir con la vida cotidiana, tras las restricciones impuestas por la amenaza del virus. Los sistemas educativos, comerciales y bancarios, entre otros muchos, han sido capaces de adaptar las tecnologías existentes a la nueva y repentina realidad. El Consejo y el sistema de las Naciones Unidas dependen de ellas para seguir celebrando reuniones, y hoy en día incluso nos hemos acostumbrado a escuchar a los ponentes que no pueden asistir a una reunión en persona. Por supuesto, esas ventajas no se han disfrutado por igual en todas partes, debido a las desigualdades persistentes en el acceso a las tecnologías de la información y la comunicación. Abordar esa brecha digital sigue siendo una importante tarea de la comunidad internacional.

Como bien sabemos, las mismas tecnologías digitales que han revolucionado nuestras vidas al permitir la generación, el almacenamiento, la difusión y el acceso a enormes cantidades de información, muchas veces han sido mal utilizadas por Gobiernos y agentes no estatales. En las deliberaciones de hoy se han abordado algunos de esos problemas, que son de índole diversa y, por tanto, requieren diferentes modalidades de respuesta por parte de los Estados.

La Asamblea General ha reconocido que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable a las actividades de los Estados en el ciberespacio y es esencial para mantener la paz y la estabilidad, respetar los derechos humanos y promover un entorno digital público, seguro, pacífico y accesible. Hay que respetar el derecho internacional de los

derechos humanos y el derecho internacional humanitario. También subrayamos la importancia de adherirse a las normas voluntarias y no vinculantes para el comportamiento responsable de los Estados en el ciberespacio aprobadas por la Asamblea General, entre otras cosas, protegiendo la infraestructura de información crucial que permite prestar servicios esenciales para el público.

Para hacer frente al reto de la desinformación, los Gobiernos y las sociedades deben adoptar estrategias amplias. Las campañas educativas y los debates abiertos para sensibilizar a la población, así como la cooperación entre agentes públicos y privados, como las empresas de redes sociales, pueden ayudar a atajar el uso indebido de las plataformas digitales con fines de incitación a la violencia y el terrorismo.

La cooperación internacional en el uso de la tecnología digital ha mejorado enormemente nuestra capacidad para detectar amenazas comunes, entre ellas, las procedentes de agentes no estatales, como son los grupos terroristas. A medida que evolucionan las tecnologías, también podemos utilizarlas más eficazmente para mejorar la transparencia y la agilidad del Consejo de Seguridad. Debemos fomentar el uso de las nuevas tecnologías para que las mujeres, los jóvenes y la sociedad civil tengan más acceso a los procesos de paz y a las iniciativas de consolidación y mantenimiento de la paz.

Las operaciones de las Naciones Unidas para el mantenimiento de la paz deberían aprovechar al máximo las tecnologías digitales existentes para mejorar la ejecución de su mandato. Me gustaría destacar la importancia de las nuevas tecnologías para las comunicaciones estratégicas en las misiones de mantenimiento de la paz. Las comunicaciones estratégicas actúan como facilitadores y tienen un efecto multiplicador en todos los ámbitos del mandato, especialmente en relación con la protección de los civiles y la agenda sobre las mujeres y la paz y la seguridad. Además, son cruciales para combatir la información engañosa y la desinformación que pueden dificultar la ejecución del mandato y amenazar la seguridad del personal de mantenimiento de la paz.

Sr. Biang (Gabón) (*habla en francés*): Sra. Presidenta: Le doy las gracias por haber tenido la iniciativa de convocar esta sesión, que nos brinda la oportunidad de estudiar las repercusiones que tienen las tecnologías digitales en el mantenimiento de la paz y la seguridad internacionales. En los últimos tiempos, la cuestión ha ido cobrando cada vez más importancia para la agenda para la paz y la seguridad internacionales. Me gustaría dar las gracias a la Secretaria General Adjunta,

Sra. DiCarlo, así como a la Sra. Nyabola y al Sr. Druet, por sus esclarecedoras exposiciones.

El tema central de nuestras deliberaciones de hoy nos recuerda más que nunca que el progreso tecnológico ha hecho retroceder los límites de nuestro mundo físico hasta la infinidad de lo digital y lo cibernético. Esto implica, por un lado, un aumento de nuestras posibilidades a todos los niveles, incluido el mantenimiento de la paz y la seguridad internacionales, pero, por otro lado, una reconfiguración y recalibración de las amenazas que pesan sobre ellas.

El mantenimiento de la paz depende más que nunca de un sólido ecosistema de tecnología e innovación que no solo refuerce los instrumentos de gestión y prevención de conflictos, sino que también promueva un mejor conocimiento de la situación, mejore el apoyo a las misiones y facilite una mejor aplicación de los mandatos de mantenimiento de la paz de las Naciones Unidas, a menudo en entornos complejos.

Los avances tecnológicos también contribuyen a reforzar la seguridad del personal de mantenimiento de la paz y de la población civil y permiten mejorar las medidas preventivas, especialmente en el ámbito humanitario. El uso de vehículos aéreos no tripulados y de sistemas de análisis de puntos se está convirtiendo cada vez más en el medio preferido para observar y prever los movimientos en zonas de difícil acceso, como los campos de batalla, a fin de disponer de información fiable para reaccionar oportunamente y con más eficacia.

Está claro que el mundo se encuentra en un punto de inflexión en su camino hacia la robotización y digitalización de nuestra sociedad, de nuestra gobernanza —tanto nacional como mundial— y, sobre todo, de nuestros derechos y obligaciones. Desgraciadamente, esa mutación tecnológica no es exclusivamente ventajosa. Viene acompañada de consecuencias y motivos de preocupación, como toda ciencia que no esté revestida de un manto de conciencia.

Considerado a menudo como un multiplicador de fuerzas, el progreso tecnológico se revela también como un factor de exacerbación en situaciones de conflicto. En efecto, el discurso de odio, la radicalización, la incitación a la discriminación y la violencia en todas sus formas, difundidas a través de Internet y de las redes sociales y de las que las mujeres y los jóvenes son los principales objetivos vulnerables, se han convertido hoy en día en los vehículos preferidos del terror, el miedo y la perpetuación de las crisis.

La fabricación de armas más potentes y sofisticadas, perfeccionadas por el progreso tecnológico, conlleva una mayor capacidad de molestia y deshumanización, que debe someterse a un estricto marco jurídico y deontológico a riesgo de ser un verdadero peligro para la humanidad. El triste espectáculo de los grupos armados y terroristas que adquieren libremente armas cada vez más sofisticadas y nuevas tecnologías para reforzar su poder de desestabilización en varias regiones de África recuerda la necesidad de que el personal de mantenimiento de la paz, así como las fuerzas regulares de los países afectados, tengan también acceso a las últimas tecnologías.

Lo que está en juego es la viabilidad de los Estados que se encuentran en las garras de esas fuerzas negativas y la supervivencia de la población afectada, acorralada entre la impotencia de los Estados cuya autoridad está en decadencia y los suplicios infligidos por grupos armados decididos a sembrar el terror y caos. Es crucial que las fuerzas de mantenimiento de la paz tengan acceso a un equipamiento tecnológico acorde con la magnitud de las nuevas amenazas y adaptado a los retos que deben afrontar, especialmente en los conflictos armados asimétricos contra grupos terroristas.

Compartimos la convicción de que es necesario fomentar la innovación y el progreso tecnológico sobre el terreno; aprovechar al máximo el potencial de las tecnologías existentes y nuevas para mejorar la capacidad de nuestras misiones de mantenimiento de la paz para cumplir eficazmente sus mandatos; permitir a las operaciones de paz detectar, analizar y hacer frente de manera oportuna e integral a las amenazas que pesan sobre los civiles, el personal de mantenimiento de la paz y las misiones humanitarias y políticas. y, por último, velar por que las operaciones de paz hagan un uso más responsable de las tecnologías digitales, respetando los derechos humanos allí donde estén en peligro.

Mi país apoya la Estrategia para la Transformación Digital del Mantenimiento de la Paz de las Naciones Unidas, así como la Estrategia y Plan de Acción de las Naciones Unidas para la Lucha contra el Discurso de Odio.

El Gabón sigue defendiendo firmemente el uso pacífico y responsable de la tecnología para el mantenimiento de la paz y la seguridad internacionales y pide que se refuerce la cooperación triangular, que es esencial, entre otras cosas, para la aplicación de la resolución 2518 (2020), relativa a la seguridad del personal de mantenimiento de la paz.

Para concluir, quisiera subrayar la importancia de movilizarse a nivel internacional, regional y nacional para lograr una gobernanza óptima del espacio digital y del progreso tecnológico, y para convertirlo en un auténtico catalizador de los mandatos de las misiones de paz de las Naciones Unidas y de los principales instrumentos para la paz y la seguridad internacionales.

Sra. Juul (Noruega) (*habla en inglés*): Deseo dar las gracias a los ponentes por sus interesantes declaraciones. Agradezco también a los Estados Unidos que haya facilitado esta importante discusión en el Consejo de Seguridad.

A lo largo del último año, el Consejo ha participado, en diferentes formatos, en deliberaciones sobre tecnología y seguridad, desde la reunión celebrada con arreglo la fórmula Arria sobre nuevas tecnologías y seguridad, celebrada en mayo de 2021 por la Misión Permanente de China, hasta el debate abierto de junio, en el que Estonia incluyó por primera vez la ciberseguridad en el orden del día del Consejo (véase S/2021/621). Esta es una continuación oportuna de esos debates.

Las tecnologías digitales emergentes y en evolución presentan grandes oportunidades en varios ámbitos. De hecho, sin la tecnología digital, el propio Consejo de Seguridad no habría podido funcionar durante las fases iniciales de la pandemia de enfermedad por coronavirus. Al mismo tiempo, las tecnologías digitales también pueden plantear problemas y desafíos. Cuando se utilizan con fines maliciosos, no cabe duda de que pueden suponer una amenaza para la paz y la seguridad internacionales. Por lo tanto, el debate de hoy gira en torno a una cuestión central del mandato y la responsabilidad del Consejo.

Las tecnologías digitales no solo las aportan y utilizan los Estados, de ahí la importancia de la cooperación entre los Estados y otras partes interesadas. Tenemos que colaborar con todos los que desarrollan y utilizan las tecnologías, incluso con el mundo académico y las organizaciones no gubernamentales. Solo si trabajamos juntos podremos conseguir que las nuevas tecnologías nos ayuden a avanzar en una dirección que sea beneficiosa para todos. Las Naciones Unidas constituyen una importante plataforma mundial para esta interacción.

El mal uso de las tecnologías digitales puede afectar a la paz y la seguridad de todo el mundo, por ejemplo, a través de cortes de Internet o la difusión masiva de desinformación. A Noruega le preocupa que la evolución del uso indebido del ámbito digital pueda tener consecuencias que intensifiquen las tensiones y agraven

las violaciones y los abusos de los derechos humanos. Las restricciones intencionadas del acceso a Internet, en su totalidad o en parte, representan solo un tipo de uso indebido. La difusión de desinformación selectiva a través de las tecnologías digitales representa otra, que a menudo limita el acceso de las personas a información fiable en los momentos en que más se necesita.

Sin embargo, no debemos subestimar los efectos positivos de las tecnologías digitales, ya que pueden ayudar a promover la inclusión en los procesos de decisiones al permitir el acceso de grupos tradicionalmente excluidos, como las mujeres y los grupos minoritarios, por ejemplo, mediante el uso de las videoconferencias en el propio Consejo de Seguridad para facilitar la participación de más y diversos ponentes de la sociedad civil.

La desinformación también sigue siendo un problema en muchos ámbitos, e incluso supone un riesgo para nuestras propias misiones de mantenimiento de la paz de las Naciones Unidas, por ejemplo, cuando se difunde información falsa para engendrar hostilidad entre las comunidades a las que el personal de mantenimiento de la paz tiene el deber de ayudar. Sin embargo, la mejor defensa contra la desinformación es contar con un sector de los medios de comunicación libre, independiente y profesional. Es esencial que estos tengan libertad para transmitir información importante, hacer preguntas cruciales e informar sobre las violaciones y abusos de los derechos humanos. Por tanto, apoyar a los medios de comunicación independientes y pluralistas y garantizar la seguridad de los periodistas puede contribuir también a reducir las tensiones y prevenir los conflictos.

Una vez más, Sra. Presidenta, le doy las gracias por incluir esta cuestión en nuestro orden del día. Espero que este sea el comienzo de un debate continuo sobre cómo podemos evitar y combatir la desinformación y otros retos derivados del uso indebido de las tecnologías digitales, sin perder de vista los inmensos beneficios que dichas tecnologías ofrecen al mantenimiento de la paz y la seguridad internacionales.

Sr. Roscoe (Reino Unido de Gran Bretaña e Irlanda del Norte) (*habla en inglés*): Sra. Presidenta: Le doy las gracias por haber convocado este debate de hoy. Nosotros también estamos muy agradecidos a los ponentes por sus aportaciones, ya que han ilustrado que la tecnología está cambiando la forma de vigilar y comprender los conflictos y las crisis humanitarias en todo el mundo y responder a ellos.

Está claro que, en primer lugar, la tecnología puede ayudar a evitar que estalle un conflicto. Si podemos

ver los riesgos con antelación, podemos y debemos actuar antes de que se desencadene una crisis. El hecho de tomar decisiones a tiempo permite actuar pronto y de forma preventiva, que es un ámbito que creo que el Consejo de Seguridad debería explorar más, junto con la Secretaría. También es la razón por la que estamos trabajando con otros asociados y con la industria para elaborar modelos de prevención de conflictos basados en la inteligencia artificial.

En segundo lugar, durante el propio conflicto, es esencial que el personal de mantenimiento de la paz de las Naciones Unidas tenga un conocimiento preciso de la situación. Gracias a la combinación de tecnologías digitales, como la vigilancia a distancia, con la mejora de los procesos de inteligencia, vigilancia y reconocimiento, las misiones de mantenimiento de la paz y de vigilancia pueden comprender mejor las amenazas y vulnerabilidades sobre el terreno. Si conseguimos que esos drones descritos por nuestro colega de los Emiratos Árabes Unidos ayuden a las fuerzas de paz en lugar de atacar a la gente, podremos avanzar.

En tercer lugar, la tecnología también permite aumentar la rendición de cuentas. Como hemos oído hoy, e incluso han comentado nuestros brillantes ponentes, las redes sociales permiten una mayor rendición de cuentas; gracias a ellas, la gente puede contar los conflictos al mundo tal y como los viven, y el mundo puede saber lo que está ocurriendo tal cual está ocurriendo. Eso significa que quienes desean ocultar la verdad, como las pruebas de atrocidades masivas o de violaciones del derecho internacional humanitario, no pueden ocultarla.

Como también se ha dicho hoy, la tecnología está siendo utilizada por los Estados y otros agentes para suprimir los derechos humanos y difundir desinformación, y como herramienta en los conflictos. Vemos que algunos Estados intentan ocultar la verdad bloqueando el acceso a las redes sociales o a los sitios de medios de comunicación independientes. Como han señalado otros, lo vimos el año pasado cuando la junta militar cerró Internet en Myanmar. También vemos que los regímenes autoritarios utilizan la tecnología de vigilancia para controlar y perseguir a sus propios ciudadanos, negándoles sus derechos humanos. La tecnología también la pueden utilizar aquellos que quieren desestabilizar, y eso es particularmente cierto en el contexto de la invasión rusa de Ucrania, donde Rusia ha realizado ciberataques y, como hemos informado, ha utilizado una fábrica de trolls en línea para difundir desinformación y manipular la opinión pública sobre su guerra ilegal.

Afortunadamente, la tecnología también puede ayudarnos a combatir la desinformación. Rusia ha vuelto a intentar hoy afirmar que los cuerpos de las víctimas que yacen en las calles de Bucha son un montaje de Ucrania para provocar. Han sugerido que las fuerzas ucranianas realizaron ese montaje después de retomar la ciudad. Sin embargo, las imágenes por satélite demostraron que los cuerpos que yacían en las calles de Bucha llevaban allí varias semanas, lo que deja claro que fueron asesinados durante el tiempo en que las fuerzas rusas ocuparon la ciudad.

Hoy, en lugar de hablar de un montaje para provocar, nos han contado una nueva tontería sobre artillería obsoleta. Esa es otra de las tácticas rusas para intentar distraer y confundir y ofuscar. Lanzan mentiras contradictorias y opuestas para que la gente se confunda y no sepa qué creer. Pero nadie debe dejarse engañar por esto. Esperamos que la Corte Penal Internacional lleve a cabo una investigación completa para que podamos saber la verdad sobre lo que ocurrió en Bucha, basándose en pruebas reales. Esperamos que de ahí surjan autos de acusación.

La lucha contra la desinformación y la defensa de los medios de comunicación que se comprometen a informar sobre la verdad en línea son fundamentales para el buen funcionamiento del sistema internacional. Por tanto, cuando la delegación rusa se lamenta de que se le sanciona en las redes sociales o de que se bloquean sus medios de propaganda estatal, no debería hacerlo. En el espacio digital, como en todos los espacios, debemos esforzarnos por proteger la verdad de este nuevo doble lenguaje.

Para terminar, tenemos que trabajar juntos, incluso con las organizaciones de la sociedad civil, el sector privado y otras comunidades, para aprovechar las ventajas de las tecnologías digitales y contrarrestar los riesgos derivados de ellas. Esto implicará adaptar las instituciones y acatar normas estrictas relativas a los derechos humanos y los valores democráticos. El Consejo debe velar por que los marcos existentes y el derecho internacional sigan siendo nuestros principios rectores. Y si lo logramos, podremos garantizar que las tecnologías digitales sean una fuerza para el bien y una oportunidad de transformación para sostener la paz y el desarrollo.

Sr. Flynn (Irlanda) (*habla en inglés*): Doy las gracias a los ponentes de hoy.

Como se ha dicho hoy, la tecnología es positiva para el bien de nuestras vidas, pero también puede ser un arma poderosa para fomentar la violencia y el conflicto. Los ciberataques, la ciberdelincuencia y el uso

indebido de la tecnología para difundir desinformación están minando gravemente la confianza, mientras que los avances de la tecnología moderna están contribuyendo a cambiar la naturaleza de los conflictos. El discurso de odio puede difundirse y amplificarse en cuestión de minutos, polarizando así a las comunidades, socavando la democracia y alimentando la intolerancia y la violencia en todo el mundo.

Existen innumerables ejemplos de tales riesgos. Los medios de comunicación controlados por el Estado ruso han sembrado discursos de desinformación en un intento de excusar su guerra ilegal e injustificada en Ucrania. A medida que la guerra continúa, también lo hacen los esfuerzos de la Federación de Rusia por distorsionar la realidad y negar su brutal agresión sobre el terreno.

En Myanmar, como se ha mencionado en otras intervenciones, la restricción del acceso a Internet antes del golpe de Estado fue un preludio de la posterior erosión de las libertades fundamentales, la represión, la vigilancia y la violencia brutal. Hemos visto que en Etiopía las tecnologías se han usado indebidamente para oprimir a los defensores de los derechos humanos, vigilar a los activistas, difundir discursos de odio y atizar las tensiones a través de las redes sociales. En muchos otros casos, las nuevas tecnologías se utilizan indebidamente para amenazar la seguridad e integridad de los Estados, atacar infraestructuras críticas, injerir en los procesos democráticos y restringir los derechos humanos.

Aunque la proliferación de las tecnologías digitales plantea nuevos riesgos y desafíos, también alberga el potencial de desempeñar un papel vital en apoyo de la paz. Desde Colombia hasta Libia, hemos visto cómo las tecnologías digitales han apoyado una mayor inclusión, promovido la participación en los procesos de paz y complementado las interacciones cara a cara. Esas tecnologías pueden y deben facilitar y ampliar la participación de las mujeres, los jóvenes y las minorías. Irlanda acoge con satisfacción la labor que realizan la Dependencia de Apoyo a la Mediación y la Célula de Innovación del Departamento de Asuntos Políticos y de Consolidación de la Paz a ese respecto. Sin embargo, en esos esfuerzos deben tener en cuenta los riesgos particulares a los que se enfrentan estos grupos en el ciberespacio, así como la brecha digital de género en todo el mundo.

Alentamos a todos los presentes en la mesa a mostrarse más abiertos al papel positivo que la tecnología puede desempeñar en la prevención de conflictos y en la solución de retos globales como el cambio climático. La creación de capacidades y las medidas e iniciativas de

fomento de la confianza, incluido el programa de acción para avanzar en el comportamiento responsable de los Estados en el ciberespacio, que Irlanda se enorgulleció de copatrocinar, son fundamentales en el contexto de esos esfuerzos.

La tecnología también puede actuar como una multiplicadora de fuerzas en las misiones de mantenimiento de la paz, brindando a nuestro personal de mantenimiento de la paz una mayor conciencia de la situación y una mejor capacidad de análisis de datos. Esos habilitadores de importancia crítica mejoran la seguridad y la eficacia operativa, con lo que se refuerza la ejecución de los mandatos. Esa es la razón por la que la aplicación de la Estrategia para la Transformación Digital del Mantenimiento de la Paz de las Naciones Unidas reviste tanta importancia.

Es precisamente en tiempos de conflicto armado cuando debemos defender resueltamente el derecho a la libertad de expresión, tanto en la red como fuera de ella, y el acceso a la información, libertades esenciales para promover una paz duradera, comprender la naturaleza del conflicto y garantizar la rendición de cuentas. Hoy rindo homenaje a los ciudadanos, periodistas y defensores de los derechos humanos de Ucrania que emplean las tecnologías digitales para compartir historias desgarradoras del frente, a menudo asumiendo un enorme riesgo personal. Trabajan incansablemente para recopilar, verificar y conservar las pruebas digitales de los atentados, con la esperanza de que sirvan para exigir responsabilidades a los autores.

Es indiscutible que el derecho internacional, incluido el derecho internacional humanitario y de los derechos humanos, se aplica en el ciberespacio. Nuestros planteamientos sobre las tecnologías digitales deben basarse en los derechos humanos, el estado de derecho y los valores democráticos.

Irlanda apoya un ciberespacio libre, seguro, inclusivo y accesible. Sabemos que las tecnologías digitales no existen en un vacío. Está claro que los agentes no estatales desempeñan un papel destacado en el impulso de la innovación tecnológica. La participación activa y significativa de la sociedad civil, incluidos los defensores de los derechos humanos, los grupos de mujeres, los expertos técnicos, el mundo académico y el sector privado, reviste una importancia crucial en nuestra labor para identificar soluciones a los retos compartidos. Irlanda también alienta encarecidamente a la Comisión de Consolidación de la Paz a que tenga en cuenta la repercusión de las tecnologías digitales, tanto las positivas como las negativas, en sus debates y su asesoramiento.

Para concluir, la inversión en el potencial de las tecnologías digitales implica invertir en la paz. En lo que respecta al uso de la tecnología digital, Irlanda cree firmemente que el multilateralismo, el comportamiento responsable de los Estados, la transparencia y la responsabilidad humana son fundamentales para generar y mantener la confianza en la que se sustentan la paz y la seguridad internacionales.

La Presidenta (*habla en inglés*): A continuación formularé una nueva declaración en calidad de representante de los Estados Unidos.

Permítaseme, para empezar, dar las gracias a todos mis colegas por haber entablado hoy un diálogo sumamente constructivo sobre el papel que desempeñan las tecnologías digitales en la promoción de la paz y la

seguridad internacionales. Desgraciadamente, Rusia optó por ser poco constructiva vertiendo ataques infundados para difundir intencionadamente el mismo tipo de desinformación para cuya prevención y solución, en parte, nos hemos reunido hoy.

No ahondaré en las teorías conspirativas de Rusia. Por el contrario, trabajaremos juntos en el futuro con otros miembros del Consejo para continuar estas importantes conversaciones en las próximas semanas y meses. Quisiera dar nuevamente las gracias a los ponentes por sus contribuciones de hoy. También me gustaría dar las gracias a todos mis colegas.

Vuelvo a asumir mis funciones como Presidenta del Consejo.

Se levanta la sesión a las 12.35 horas.