



Asamblea General

Distr. limitada
19 de enero de 2021
Español
Original: inglés

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

Proyecto de informe sustantivo (borrador preliminar)*

A. Introducción

1. Pese a las transformaciones radicales que el mundo ha vivido desde la fundación de las Naciones Unidas hace 75 años, su propósito y sus ideales atemporales siguen teniendo la misma importancia que cuando se fundaron. A la par del compromiso de promover el respeto de los derechos humanos y las libertades fundamentales, fomentar el adelanto económico y social de todos los pueblos y establecer condiciones para mantener el respeto del derecho internacional, los Estados resolvieron unir sus fuerzas para garantizar la paz y la seguridad internacionales.
2. Los avances en las tecnologías de la información y las comunicaciones tienen repercusiones en los tres pilares de la labor de las Naciones Unidas: la paz y la seguridad, los derechos humanos y el desarrollo sostenible. Las tecnologías de la información y las comunicaciones y la conectividad mundial han catalizado el progreso y el desarrollo humanos, han transformado las sociedades y las economías y han ampliado las oportunidades de cooperación por el bien común de la humanidad.
3. La necesidad de consolidar y mantener la confianza y la seguridad en el entorno digital nunca ha sido tan evidente como ahora. Algunas tendencias negativas en el ámbito digital podrían menoscabar la seguridad y estabilidad internacionales, someter a grandes presiones el crecimiento económico y el desarrollo sostenible e impedir el pleno disfrute de los derechos humanos y las libertades fundamentales. Una de estas tendencias es la explotación cada vez mayor de las tecnologías de la información y las comunicaciones con fines malintencionados.
4. La actual crisis sanitaria mundial ha puesto de relieve los beneficios fundamentales de las tecnologías de la información y las comunicaciones y nuestra dependencia de ellas, entre otras cosas para prestar servicios gubernamentales vitales, transmitir mensajes de seguridad pública esenciales, desarrollar soluciones innovadoras para garantizar la continuidad de las operaciones, acelerar la investigación y ayudar a mantener la cohesión social por medios virtuales. En este momento de incertidumbre, los Estados, el sector privado, los científicos y otros

* La versión original del presente documento no fue objeto de revisión editorial oficial.



interlocutores han aprovechado la tecnología digital para mantener a las personas y las sociedades conectadas y sanas. Al mismo tiempo, la pandemia de COVID-19 ha demostrado los riesgos y las consecuencias de las actividades malintencionadas con las que se trata de explotar las vulnerabilidades en épocas en que las sociedades soportan una enorme presión y ha puesto de manifiesto la necesidad de reducir las brechas digitales, fomentar la resiliencia de todas las sociedades y los sectores y mantener un enfoque centrado en el ser humano.

5. Dado que las tecnologías de la información y las comunicaciones pueden usarse con fines incompatibles con el mantenimiento de la paz, la estabilidad y la seguridad internacionales, la Asamblea General ha reconocido¹ que la difusión y el uso de estas tecnologías afectan a los intereses de toda la comunidad mundial y que mediante una amplia cooperación mundial se lograrían las respuestas más eficaces.

6. Habida cuenta de esto, el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, establecido en virtud de la resolución [73/27](#) de la Asamblea General, brindó la oportunidad de impulsar el examen de esta cuestión fundamental ya que ofreció una plataforma inclusiva para que todos los Estados participaran, expresaran sus opiniones y ofrecieran su cooperación sobre la dimensión de seguridad internacional de las tecnologías de la información y las comunicaciones. La participación activa de los miembros de las Naciones Unidas y la colaboración de otras partes interesadas pertinentes demuestran la aspiración compartida y el interés colectivo de la comunidad internacional en lograr un entorno pacífico y seguro para todos en la esfera de la tecnología de la información y las comunicaciones y su resolución de cooperar para lograrlo.

7. El Grupo de Trabajo representa el hito más reciente en la cooperación internacional hacia el logro de un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. Desde 2003 se han establecido grupos de expertos gubernamentales en seis ocasiones para estudiar amenazas reales y potenciales en el ámbito de la seguridad de la información y posibles medidas de cooperación para encararlas². A través de sus tres informes aprobados por consenso (2010, 2013 y 2015³), de carácter acumulativo, estos grupos han reafirmado que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad en el entorno de la tecnología de la información y las comunicaciones, han recomendado 11 normas de carácter voluntario y no vinculante de comportamiento responsable de los Estados y han reconocido que podrían elaborarse más normas progresivamente. Además, estos grupos recomendaron medidas específicas de fomento de la confianza, desarrollo de la capacidad y la cooperación. En la resolución [70/237](#) de la Asamblea General, los Estados Miembros acordaron por consenso guiarse por el informe de 2015 del Grupo de Expertos Gubernamentales en su uso de las tecnologías de la información y las comunicaciones, consolidando así un marco inicial para el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones.

8. Sobre esta base, el Grupo de Trabajo ha tratado de llegar a un terreno común y un entendimiento mutuo entre todos los Estados Miembros de las Naciones Unidas sobre un tema de importancia mundial, y en sus debates se ha guiado por los principios de inclusividad y transparencia a fin de fomentar el consenso para promover y sostener la confianza. De acuerdo con su mandato, el Grupo de Trabajo deliberó sobre amenazas reales y potenciales en el ámbito de la seguridad de la información y

¹ Véase, por ejemplo, [A/RES/53/70](#), pág. 6.

² [A/RES/58/32](#), [A/RES/60/45](#), [A/RES/66/24](#), [A/RES/68/243](#), [A/RES/70/237](#), [A/RES/73/266](#).

³ [A/65/201](#), [A/68/98*](#) y [A/70/174](#).

posibles medidas de cooperación para afrontarlas; el desarrollo ulterior de reglas, normas y principios sobre el comportamiento responsable de los Estados; la aplicación del derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados; las medidas de fomento de la confianza; el desarrollo de la capacidad; y la posibilidad de establecer un diálogo institucional periódico con una participación amplia bajo los auspicios de las Naciones Unidas.

9. Si bien los Estados son responsables del mantenimiento de la paz y la seguridad internacionales, todas las partes interesadas tienen la responsabilidad de utilizar las tecnologías de la información y las comunicaciones de forma que no se ponga en peligro la paz y la seguridad. Dado que la dimensión de seguridad internacional de las tecnologías de la información y las comunicaciones abarca múltiples ámbitos y disciplinas, el Grupo de Trabajo ha aprovechado los conocimientos especializados, el saber y la experiencia que han compartido con él los representantes de las organizaciones intergubernamentales, las organizaciones regionales, la sociedad civil, el sector privado, los círculos académicos y la comunidad técnica. La reunión consultiva oficiosa de tres días del Grupo de Trabajo, celebrada en diciembre de 2019, dio lugar a un rico debate entre los Estados y una amplia gama de partes interesadas⁴. Además, estas partes interesadas han aportado propuestas y ejemplos concretos de buenas prácticas mediante contribuciones escritas e intercambios oficiosos con el Grupo de Trabajo. Algunas delegaciones también han celebrado consultas con múltiples partes interesadas *motu proprio* para basar en ellas sus contribuciones al Grupo de Trabajo.

10. El Grupo de Trabajo, consciente de las distintas situaciones, capacidades y prioridades de los Estados y las regiones, reconoce que los Estados tienen responsabilidades individuales y compartidas en el ámbito digital y los beneficios de las tecnologías digitales no están distribuidos equitativamente, y que reducir las brechas digitales, entre otras cosas ampliando el acceso a las tecnologías de la información y las comunicaciones y la conectividad, sigue siendo una prioridad urgente para la comunidad internacional.

11. El Grupo de Trabajo acoge con agrado el alto grado de participación de las delegadas en sus períodos de sesiones y la prominencia de las perspectivas de género en sus debates, y subraya la importancia de reducir la brecha digital de género y promover la participación eficaz y significativa y el liderazgo de las mujeres en los procesos de toma de decisiones vinculados al uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

12. El Grupo de Trabajo reconoce la importancia y complementariedad de los debates especializados en otros órganos y foros de las Naciones Unidas sobre aspectos de las tecnologías digitales, entre ellos las cuestiones relativas al desarrollo sostenible, los derechos humanos (incluidas la protección y privacidad de los datos, la libertad de expresión y la libertad de información), la cooperación digital, la gobernanza de Internet, la ciberdelincuencia y el uso de Internet con fines terroristas.

13. El Grupo de Trabajo subraya que los distintos elementos de que se compone su mandato están interrelacionados y se refuerzan mutuamente, y juntos fomentan un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. El derecho internacional constituye un marco para las acciones de los Estados y las normas definen más claramente las expectativas sobre el comportamiento responsable de los Estados. Las medidas que fomentan la

⁴ Véase el resumen de la Presidencia de la reunión consultiva oficiosa entre períodos de sesiones 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, disponible en <https://www.un.org/disarmament/open-ended-working-group/>.

confianza y la capacidad refuerzan el cumplimiento del derecho internacional, alientan la aplicación de normas, ofrecen oportunidades de aumentar la cooperación entre los Estados y permiten a todos los Estados cosechar los beneficios de las tecnologías de la información y las comunicaciones en beneficio de sus sociedades y economías.

14. Habida cuenta de estas sinergias, las siguientes secciones del informe son complementarias e interdependientes. Cada una de las siguientes secciones (B a G) comienza con una reflexión sobre las opiniones expresadas durante los debates sustantivos del Grupo de Trabajo, seguida de ámbitos de acuerdo y recomendaciones específicas.

B. Amenazas reales y potenciales

15. En sus debates celebrados en el Grupo de Trabajo, los Estados plantearon una amplia gama de amenazas reales y potenciales, lo que puso de manifiesto que estos pueden percibir de formas distintas las amenazas procedentes del ámbito digital. El formato inclusivo del Grupo de Trabajo ofreció a los Estados la oportunidad de profundizar su comprensión sobre el modo en que otros perciben las acciones y los comportamientos en el entorno de la tecnología de la información y las comunicaciones y atender a lo que otros consideran las amenazas y los riesgos más significativos.

Deliberaciones

16. Algunos Estados se mostraron preocupados por el desarrollo o el uso de las capacidades de las tecnologías de la información y las comunicaciones con fines militares de manera incompatible con los objetivos del mantenimiento de la paz y la seguridad internacionales, y algunos expresaron su preocupación por la posibilidad de que las características del entorno de las tecnologías de la información y las comunicaciones pudieran alentar la adopción de medidas unilaterales en lugar del arreglo pacífico de controversias. También se expresó inquietud por la acumulación de vulnerabilidades y la falta de transparencia y de procesos definidos para comunicarlas, la explotación de funciones ocultas dañinas, la integridad de las cadenas de suministro mundiales de tecnología de la información y las comunicaciones y la garantía de la seguridad de los datos. Algunos Estados expresaron preocupación por la posibilidad de que las tecnologías de la información y las comunicaciones se pudieran utilizar para interferir en sus asuntos internos, entre otras cosas mediante operaciones de información y campañas de desinformación. Se expresó especial preocupación por los esfuerzos encaminados a aumentar la automatización y la autonomía en las operaciones de tecnología de la información y las comunicaciones y por las actividades que pudieran dar lugar a una reducción o interrupción de la conectividad, a una intensificación no deseada de la tensión o a repercusiones negativas para terceros. Algunos Estados también indicaron la falta de claridad sobre las responsabilidades del sector privado como un motivo de preocupación en sí mismo.

17. Se subrayó que las medidas para promover un comportamiento responsable de los Estados deben seguir siendo tecnológicamente neutrales y que lo que resultaba preocupante era el uso indebido de las tecnologías y no las tecnologías en sí mismas. Se reconoció que, si bien los avances tecnológicos y las nuevas aplicaciones pueden ofrecer oportunidades de desarrollo, también pueden ampliar los ámbitos de ataque, aumentar las vulnerabilidades en el entorno de la tecnología de la información y las comunicaciones o utilizarse para realizar nuevas actividades malintencionadas. En este sentido, se destacaron determinadas tendencias y avances tecnológicos, como el

progreso en el aprendizaje automático y la informática cuántica, la ubicuidad de los dispositivos conectados (“la Internet de las cosas”), los nuevos modos de almacenar y acceder a los datos mediante los registros descentralizados y la computación en la nube, y la ampliación de los macrodatos y los datos personales digitalizados.

Conclusiones

18. Los Estados coincidieron en que les preocupaban cada vez más las repercusiones del uso malintencionado de las tecnologías de la información y las comunicaciones en el mantenimiento de la paz y la seguridad internacionales, y, por consiguiente, en los derechos humanos y el desarrollo. Los incidentes dañinos vinculados a la tecnología de la información y las comunicaciones son cada vez más frecuentes, precisos y sofisticados, y evolucionan y se diversifican constantemente. La conectividad y la dependencia cada vez mayores de las tecnologías de la información y las comunicaciones pueden traer consigo riesgos imprevistos y hacer a las sociedades más vulnerables frente a las actividades malintencionadas en la esfera de la tecnología de la información y las comunicaciones. Pese a los incalculables beneficios que suponen las tecnologías de la información y las comunicaciones para la humanidad, su uso malintencionado puede tener repercusiones negativas de gran alcance.

19. Los Estados coincidieron en que el continuo aumento de los incidentes de uso malintencionado de las tecnologías de la información y las comunicaciones por agentes estatales y no estatales, incluidos los intermediarios, era una tendencia perturbadora. Algunos agentes no estatales han demostrado capacidades de tecnología de la información y las comunicaciones que anteriormente solo estaban al alcance de los Estados, y se expresó preocupación por la posibilidad de que estas capacidades se utilizaran con fines terroristas o criminales.

20. Los Estados también coincidieron en que cualquier uso de las tecnologías de la información y las comunicaciones por los Estados de forma incompatible con su compromiso de convivir en paz como buenos vecinos, adquirido en virtud de la Carta de las Naciones Unidas, y con el resto de sus obligaciones en virtud del derecho internacional menoscaba la confianza y la estabilidad entre los Estados, lo que puede aumentar el riesgo de percepciones erróneas y la probabilidad de futuros conflictos entre los Estados.

21. Los Estados coincidieron en que los ataques contra la infraestructura crítica y la infraestructura de información crítica en que se sustentan servicios esenciales para el público como las instalaciones médicas, la energía, el agua, el transporte y el saneamiento, pueden tener consecuencias humanitarias devastadoras. También son motivo de preocupación real, y cada vez mayor, los ataques a estas dos infraestructuras que menoscaban la confianza en los procesos políticos y electorales y las instituciones públicas o que afectan al sistema financiero. Es posible que esta infraestructura sea propiedad del sector privado o que este la gestione o la maneje, o puede que se comparta o se transmita en red con otro Estado o esté gestionada por distintos Estados, y por ello puede ser necesaria la cooperación entre Estados o entre los sectores público y privado para proteger su integridad, funcionamiento y disponibilidad.

22. Los Estados también coincidieron en que el uso de las tecnologías de la información y las comunicaciones para alterar, dañar o destruir la infraestructura crítica y la infraestructura de información crítica suponía una amenaza no solo para la seguridad, sino también para el desarrollo económico y los medios de subsistencia, y en última instancia para la seguridad y el bienestar de las personas.

23. Los Estados coincidieron en que el desconocimiento y la falta de capacidades suficientes para detectar las actividades malintencionadas de tecnología de la información y las comunicaciones, defenderse contra ellas o responder a ellas constituía un desafío, ya que todos los países dependen cada vez más de las tecnologías digitales. Como se ha observado en la actual emergencia sanitaria mundial, las vulnerabilidades ya existentes pueden agravarse en épocas de crisis.

24. Los Estados coincidieron en que las amenazas podían afectar de distinto modo a los Estados en función de sus niveles de capacidad, de seguridad y resiliencia en materia de tecnología de la información y las comunicaciones, de infraestructura y de desarrollo. Las amenazas también pueden repercutir de forma distinta a distintos grupos y entidades, como la juventud, las personas de edad, las mujeres y los hombres, los grupos de población vulnerables, algunas profesiones específicas, las pequeñas y medianas empresas y otros.

25. Habida cuenta de la situación cada vez más preocupante de las amenazas digitales y reconociendo que ningún Estado está a salvo de ellas, los Estados coincidieron en la urgencia de implantar y seguir desarrollando, a través de foros multilaterales, medidas de cooperación para abordar estas amenazas, y afirmaron que actuando unidos y de forma inclusiva, siempre que fuera posible, se lograrían resultados más eficaces y de mayor alcance. En este sentido, se destacó también la importancia de seguir reforzando la colaboración con la sociedad civil, el sector privado, el mundo académico y la comunidad técnica, cuando procediera.

C. El derecho internacional

26. Los Estados, guiados por el mandato del Grupo y con miras a promover una comprensión común del modo en que se aplica el derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados, mantuvieron un intercambio de opiniones sobre cómo se aplica el derecho internacional (principios generales del derecho, tratados y derecho internacional consuetudinario) a la dimensión de seguridad internacional de las tecnologías de la información y las comunicaciones.

Deliberaciones

27. En sus debates celebrados en el Grupo de Trabajo, los Estados recordaron que el derecho internacional, y en particular la Carta de las Naciones Unidas en su integridad, era aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. Asimismo, se destacó la necesidad de comprender mejor cómo se aplica el derecho internacional al uso de la tecnología de la información y las comunicaciones por parte de los Estados.

28. Entre los principios específicos de la Carta de las Naciones Unidas que se destacaron en las deliberaciones estaban la soberanía de los Estados; la igualdad soberana; la solución de controversias internacionales por medios pacíficos de modo que no se pongan en peligro ni la paz ni la seguridad internacionales ni la justicia; la renuncia a recurrir, en las relaciones internacionales, a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas; el respeto de los derechos humanos y las libertades fundamentales; y la no intervención en los asuntos internos de otros Estados⁵.

⁵ A/RES/73/27, decimosexto párr. del preámbulo.

29. Se recordó que el derecho internacional era la base de la estabilidad y la previsibilidad en las relaciones entre los Estados. En particular, el derecho internacional humanitario reduce los riesgos y los posibles daños para los civiles, los objetos civiles y los combatientes en el contexto de los conflictos armados. Por otra parte, los Estados pusieron de relieve que el derecho internacional humanitario no alentaba la militarización ni legitima el recurso al conflicto en ningún ámbito.

30. También se observó que en virtud del derecho internacional consuetudinario, las responsabilidades de los Estados con respecto a los hechos internacionalmente ilícitos se extienden a su uso de las tecnologías de la información y las comunicaciones. Se recordó también que los Estados no deben recurrir a intermediarios para cometer actos internacionalmente ilícitos utilizando las tecnologías de la información y las comunicaciones, y deben tratar de que ningún agente no estatal, siguiendo instrucciones de un Estado o bajo su control, utilice su territorio para cometer esos actos. También se aludió a la responsabilidad de los Estados con respecto a las entidades que son propiedad de otro Estado o están bajo el control de este.

31. Se recordó que es posible que el indicio de que una actividad de tecnología de la información y las comunicaciones se ha iniciado o tiene su origen en el territorio o la infraestructura de tecnología de la información y las comunicaciones de un Estado sea insuficiente, en sí mismo, para atribuir la actividad a ese Estado, y que las acusaciones de organizar y llevar a cabo hechos ilícitos formuladas contra los Estados deben fundamentarse.

32. Algunos Estados expresaron la opinión de que el derecho internacional vigente, complementado por las normas voluntarias no vinculantes que reflejan el consenso entre los Estados, es suficiente, actualmente, para abordar el uso de las tecnologías de la información y las comunicaciones por los Estados. También se propuso que los esfuerzos se centraran en alcanzar una comprensión común del modo en que se aplica el marco normativo convenido mediante el desarrollo de orientación adicional y el modo en que puede ponerse en práctica mediante una mejora de la aplicación por todos los Estados. Al mismo tiempo, algunos Estados opinaron que, debido a los rápidos cambios en las amenazas y a la gravedad del riesgo, se necesita un marco jurídicamente vinculante en la esfera de las tecnologías de la información y las comunicaciones. También se sugirió que con un marco vinculante de este tipo sería posible lograr una aplicación mundial más eficaz de los compromisos y establecer una base más firme para que los interlocutores rindieran cuentas de sus actos.

33. Se destacó que, si bien los instrumentos de derecho internacional actuales no contienen referencias específicas al uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, el derecho internacional puede desarrollarse progresivamente, entre otras cosas mediante la *opinio iuris* y la práctica de los Estados. Se mencionó la posibilidad de desarrollar paulatinamente medidas complementarias vinculantes de forma simultánea a la aplicación de normas. Asimismo, se propuso un compromiso político como camino a seguir.

34. Si bien se recordó que el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable al uso de las tecnologías de la información y las comunicaciones, se destacó que todavía no se han aclarado del todo algunas cuestiones sobre el modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones, por ejemplo, el tipo de actividad vinculada a las tecnologías de la información y las comunicaciones que otros Estados podrían interpretar como amenaza o uso de la fuerza (Art. 2, párr. 4, de la Carta) o que podrían constituir motivos para que un Estado invocara su derecho intrínseco de legítima defensa (Art. 51 de la Carta), así como el modo en que algunos principios del derecho internacional humanitario, como los de humanidad, necesidad, proporcionalidad, distinción y precaución se aplican a las operaciones de tecnología

de la información y las comunicaciones. En este sentido, algunos Estados observaron que debían abordarse con prudencia los debates sobre la aplicabilidad del derecho internacional humanitario al uso de las tecnologías de la información y las comunicaciones por parte de los Estados.

35. Por otra parte, en cuanto al camino a seguir, se propuso, como primer paso clave para aclarar y seguir desarrollando entendimientos comunes, que los Estados aumentaran sus intercambios y sus debates a fondo sobre el modo en que se aplica el derecho internacional, y observaron que estos intercambios podían servir, en sí mismos, como una importante medida de fomento de la confianza. Además, se propusieron varias formas de compartir voluntariamente sus posturas nacionales sobre la cuestión del derecho internacional, en particular utilizando el informe anual del Secretario General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional o proporcionando una encuesta sobre la práctica nacional en la aplicación del derecho internacional. También se destacó el progreso alcanzado en los acuerdos regionales y de otra índole para intercambiar opiniones y desarrollar percepciones comunes sobre el modo de aplicar el derecho internacional.

36. Desde la óptica del mantenimiento de la paz y la prevención de los conflictos, se observó que también debería prestarse mayor atención al arreglo pacífico de controversias y a los modos de evitar la amenaza o el uso de la fuerza. En este contexto, se recordaron los órganos, mecanismos e instrumentos que existen para la prevención y el arreglo pacífico de controversias, y algunos Estados sugirieron que la elaboración de un enfoque y un entendimiento comunes y universalmente aceptados, a nivel técnico, en torno a las causas de los incidentes vinculados a la tecnología de la información y las comunicaciones, bajo los auspicios de las Naciones Unidas y mediante el intercambio de buenas prácticas, teniendo en cuenta el respeto al principio de la soberanía de los Estados, podría aumentar la rendición de cuentas y la transparencia y contribuir a apoyar el recurso jurídico para las personas perjudicadas por los actos maliciosos.

Conclusiones y recomendaciones

37. En virtud de la resolución [73/27](#) de la Asamblea General, por la que se estableció el Grupo de Trabajo, los Estados afirmaron que el derecho internacional, y en particular la Carta de las Naciones Unidas, era aplicable y esencial para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. Los Estados también convinieron en que debían desarrollarse más entendimientos comunes del modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones por los Estados.

38. Los Estados también reafirmaron la importancia del arreglo pacífico de controversias por medios pacíficos como la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial y el recurso a organismos o acuerdos regionales.

39. Los Estados convinieron en que pueden fomentarse entendimientos comunes sobre el modo en que el derecho internacional es aplicable al uso que hacen los Estados de las tecnologías de la información y las comunicaciones alentando el intercambio de opiniones al respecto entre los Estados y designando temas de derecho internacional específicos para mantener más debates en profundidad.

40. A fin de que todos los Estados desarrollen sus propias percepciones acerca del modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones por parte de los Estados, y con miras a contribuir

a fomentar el consenso en la comunidad internacional, los Estados convinieron en que había una gran necesidad de realizar más esfuerzos neutrales y objetivos para desarrollar la capacidad en las esferas del derecho internacional y la legislación y las políticas nacionales.

El Grupo de Trabajo recomienda:

41. Que los Estados sigan informando, de forma voluntaria, al Secretario General sobre sus opiniones y prácticas nacionales con respecto al modo en que el derecho internacional puede aplicarse a su uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, a fin de que incluya esta información en su informe anual sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

42. Que los Estados presenten, de forma voluntaria, opiniones y prácticas nacionales sobre el modo en que se aplica el derecho internacional al uso por los Estados de las tecnologías de la información y las comunicaciones, para incluirlas en el Cyber Policy Portal del Instituto de las Naciones Unidas de Investigación sobre el Desarme.

43. Que los Estados que estén en condiciones de hacerlo sigan apoyando, de forma neutral y objetiva, más iniciativas para aumentar la capacidad, de acuerdo con los principios incluidos en el párrafo 85 del presente informe, en las esferas del derecho internacional y la legislación y las políticas nacionales, a fin de que todos los Estados desarrollen su propia comprensión del modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones por los Estados y para contribuir a fomentar el consenso en la comunidad internacional.

44. Que los Estados sigan manteniendo debates a nivel multilateral para fomentar entendimientos comunes del modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional y sigan examinando otras alternativas en este sentido.

D. Normas, reglas y principios de comportamiento responsable de los Estados

45. Las normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados contribuyen notablemente a aumentar la previsibilidad y reducir los riesgos de percepciones erróneas y, de este modo, contribuyen a la prevención de los conflictos. Se destacó que estas normas reflejan las expectativas de la comunidad internacional y fijan normas sobre el comportamiento de los Estados en su uso de las tecnologías de la información y las comunicaciones.

Deliberaciones

46. En sus debates celebrados en el Grupo de Trabajo, los Estados recordaron que las normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados deben considerarse compatibles con el derecho internacional y con los propósitos y principios de las Naciones Unidas, en particular el mantenimiento de la paz y la seguridad internacionales y la promoción de los derechos humanos. Los Estados también recordaron la resolución 2131 (XX) de la Asamblea General, de 1965, titulada “Declaración sobre la Inadmisibilidad de la Intervención en los Asuntos Internos de los Estados y Protección de su Independencia y Soberanía”.

47. Se recordó que en la resolución 70/237, aprobada por consenso, se exhorta a los Estados a que, en su uso de las tecnologías de la información y las comunicaciones,

se guíen por el informe de 2015 del Grupo de Expertos Gubernamentales sobre la Verificación del Desarme Nuclear, que incluye 11 normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados. Algunos Estados destacaron que estas 11 normas acordadas formaban la base de la labor del Grupo de Trabajo, y otros recordaron que la resolución 73/27 de la Asamblea General incluye un conjunto de 13 normas, reglas y principios de comportamiento responsable de los Estados. Se reconoció que los Estados tenían la prerrogativa de aplicar progresivamente normas voluntarias en función de sus prioridades y capacidades nacionales.

48. Se subrayó la necesidad de dar a conocer las normas vigentes y apoyar su puesta en práctica paralelamente al desarrollo paulatino de nuevas normas. Los Estados destacaron también la necesidad de orientación sobre el modo de poner en práctica las normas y, en este sentido, pidieron que se compartieran y difundieran buenas prácticas y lecciones aprendidas sobre la aplicación de normas. Se propusieron distintos enfoques de cooperación, como una hoja de ruta elaborada por los Estados, para contribuir a sus actividades de aplicación, así como encuestas voluntarias para compartir lecciones y buenas prácticas.

49. Se reconoció que las normas podían ayudar a evitar el conflicto en el entorno de la tecnología de la información y las comunicaciones y contribuir a su uso pacífico y su realización plena a fin de aumentar el desarrollo social y económico mundial. Los Estados destacaron que la aplicación de normas no debía dar lugar a restricciones indebidas de la cooperación internacional y la transferencia de tecnología ni impedir la innovación con fines pacíficos y el desarrollo económico de los Estados en un entorno justo y no discriminatorio. Los Estados también subrayaron los vínculos entre las normas, el fomento de la confianza y el desarrollo de la capacidad, así como la necesidad de incorporar las perspectivas de género en la aplicación de normas.

50. En las deliberaciones, se formularon propuestas de seguir desarrollando las normas vigentes. Se reiteró la importancia de la protección de la infraestructura crítica, que debería abarcar las instalaciones médicas y sanitarias, y se señaló la importancia de cooperar para proteger la infraestructura crítica que trasciende fronteras o jurisdicciones, así como la importancia de asegurar la disponibilidad general y la integridad de Internet. Además, se recordó la resolución 64/211 de la Asamblea General, titulada “Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales”⁶. Además, los Estados también propusieron que se siguiera velando por la integridad de la cadena de suministro de las TIC, expresando su preocupación por la creación de funciones ocultas perjudiciales en los productos de las TIC y la responsabilidad de notificar a los usuarios cuando se detecten vulnerabilidades importantes.

51. Atendiendo a lo expuesto en el párrafo anterior, se recopiló en un documento oficioso que se publicará en línea⁷ una lista de las propuestas escritas formuladas por los Estados en el Grupo de Trabajo sobre la elaboración de las normas existentes, la orientación sobre su aplicación y las normas nuevas.

52. También se señaló la propuesta, formulada en 2015, de crear un código de conducta internacional para la seguridad de la información⁸.

53. Se reconoció la necesidad de alentar y apoyar más iniciativas regionales y alianzas con otras partes interesadas, como el sector privado y la comunidad técnica, sobre la aplicación de normas. Estas alianzas podrían establecerse, por ejemplo, con

⁶ Esta resolución tiene como anexo un instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales.

⁷ <https://www.un.org/disarmament/open-ended-working-group/>.

⁸ A/69/723, al que se hace referencia en A/70/174, párr. 12.

miras a garantizar iniciativas sostenibles de desarrollo de la capacidad para reducir las diferencias en las capacidades de aplicación. Podría instarse a los Estados a adoptar las medidas de divulgación y cooperación necesarias para que las distintas partes interesadas, incluidos los sectores público y privado y la sociedad civil, cumplan sus responsabilidades en el uso de las tecnologías de la información y las comunicaciones.

Conclusiones y recomendaciones

54. Los Estados convinieron en que las normas no sustituyen ni alteran las obligaciones de los Estados en virtud del derecho internacional, que son vinculantes, sino que proporcionan una orientación específica adicional sobre lo que constituye un comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones.

55. Los Estados convinieron también en que la pandemia de COVID-19 acentuó la importancia de proteger la infraestructura sanitaria, incluidos los servicios y las instalaciones médicas, como parte de las normas relativas a la infraestructura crítica.

56. Los Estados coincidieron en la importancia de apoyar e impulsar los esfuerzos para aplicar normas en los planos mundial, regional y nacional.

57. Dadas las características particulares de las tecnologías de la información y las comunicaciones, los Estados reafirmaron que, teniendo en cuenta las propuestas sobre normas formuladas en el Grupo de Trabajo, podrían seguir desarrollándose progresivamente nuevas normas. Los Estados también coincidieron en que seguir desarrollando normas y aplicar las ya existentes no eran actividades mutuamente excluyentes, sino que podían ocurrir en paralelo.

El Grupo de Trabajo recomienda:

58. Que los Estados examinen voluntariamente sus esfuerzos a nivel nacional por aplicar normas y sigan informando al Secretario General de estos exámenes nacionales para que pueda incluirlos en su informe anual sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. Los Estados también solicitaron a la Secretaría de las Naciones Unidas que recopilara información de estos exámenes en apoyo de las actividades de desarrollo de la capacidad.

59. Que los Estados, en asociación con las organizaciones pertinentes, incluidas las Naciones Unidas, elaboren más orientación voluntaria relativa a la aplicación de normas sobre el comportamiento responsable de los Estados y la difundan ampliamente en los planos nacional, regional, interregional y mundial. Debe alentarse a los Estados que estén en condiciones de hacerlo a aportar su experiencia o sus recursos para elaborar y difundir esta orientación.

60. Que los Estados, teniendo en cuenta las resoluciones 70/237 y 73/27 así como, cuando proceda, el texto oficioso en que figuran las propuestas formuladas por los Estados en este Grupo de Trabajo y a las que se hace referencia en el párrafo 51, sigan examinando las reglas, las normas y los principios internacionales acerca del comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, incluida su aplicación, y celebrando debates a nivel multilateral sobre ellos.

E. Medidas de fomento de la confianza

61. Las medidas de fomento de la confianza, que incluyen medidas de transparencia, cooperación y estabilidad, pueden contribuir a prevenir los conflictos, evitar las percepciones erróneas y los malentendidos y servir como “válvula de seguridad” para reducir las tensiones, y constituyen una expresión concreta de la cooperación internacional. Con los recursos, la capacidad y la colaboración necesarios, las medidas de fomento de la confianza pueden reforzar la seguridad, la resiliencia y el uso pacífico de las tecnologías de la información y las comunicaciones en general. Estas medidas también pueden favorecer la aplicación de normas sobre el comportamiento responsable de los Estados, ya que fomentan la confianza y garantizan una mayor claridad, previsibilidad y estabilidad en el uso de las tecnologías de la información y las comunicaciones por parte de los Estados. Junto con los demás pilares del marco para el comportamiento responsable de los Estados, las medidas de fomento de la confianza pueden contribuir también a fomentar entendimientos comunes entre los Estados y contribuir así a lograr un entorno internacional más pacífico.

62. Dado que las medidas de fomento de la confianza son compromisos voluntarios que se asumen progresivamente, pueden servir como primer paso para reducir la desconfianza entre los Estados estableciendo vías de comunicación, tendiendo puentes e iniciando una cooperación en pos de un objetivo compartido de interés mutuo. Por tanto, estas medidas pueden sentar las bases para ampliar o estructurar mejor las disposiciones y los acuerdos y establecer otros nuevos.

Deliberaciones

63. En sus debates en el Grupo de Trabajo, los Estados observaron que las medidas de fomento de la confianza recomendadas en los informes del Grupo de Expertos Gubernamentales aprobados por consenso seguían siendo pertinentes, y destacaron varias de ellas que requerían atención prioritaria, como el diálogo y los intercambios de información voluntarios de carácter periódico sobre las amenazas actuales y emergentes, la política o la doctrina nacional, las opiniones nacionales sobre el modo en que el derecho internacional es aplicable al uso de las tecnologías de la información y las comunicaciones por parte de los Estados y los enfoques nacionales a la hora de definir la infraestructura crítica y categorizar los incidentes vinculados a la tecnología de la información y las comunicaciones. El intercambio de buenas prácticas en los enfoques de la ciencia forense digital y la investigación de los ciberincidentes malintencionados podrían contribuir a aumentar la cooperación y desarrollar la capacidad. También se destacó la importancia de desarrollar una percepción común de los conceptos y la terminología como medida práctica para impulsar la cooperación internacional y fomentar la confianza. Entre otras medidas de este tipo figuraban el desarrollo de orientación sobre la aplicación de las medidas de fomento de la confianza, la capacitación del cuerpo diplomático, el intercambio de lecciones aprendidas sobre el establecimiento y el ejercicio de vías de comunicación seguras para las crisis, los intercambios de personal, los ejercicios basados en situaciones en el ámbito de las políticas y los ejercicios operacionales en el plano técnico entre los equipos informáticos de respuesta de emergencia o los equipos de respuesta a incidentes de ciberseguridad. Las medidas nacionales de transparencia, como la de compartir voluntariamente las respuestas a una encuesta sobre la aplicación o la emisión de declaraciones nacionales de adhesión al marco para el comportamiento responsable de los Estados son otras vías para fomentar la confianza con respecto a las intenciones y los compromisos de los Estados.

64. Teniendo en cuenta las experiencias de los órganos regionales en el establecimiento y mantenimiento de redes de puntos de contacto, y sobre la base de

las redes ya existentes, se debatió la viabilidad de establecer un directorio mundial central de puntos de contacto. Al mismo tiempo, se observó que la seguridad de este directorio, así como sus modalidades operacionales, serían fundamentales para su eficacia, al igual que evitar que los acuerdos se duplicaran o fueran excesivamente detallados. Asimismo, se destacó la importancia de realizar ejercicios periódicos entre una red de puntos de contacto, ya que puede ayudar a mantener la preparación y la capacidad de respuesta y garantizar que los directorios de puntos de contacto se mantengan al día.

65. Dado que las medidas de fomento de la confianza pueden llevarse a cabo en los planos bilateral, regional o multilateral, los Estados también debatieron la idoneidad y viabilidad de establecer un repositorio mundial de estas medidas, bajo los auspicios de las Naciones Unidas, a fin de compartir políticas, buenas prácticas, experiencias y evaluaciones respecto de la aplicación de estas medidas y alentar el aprendizaje entre pares y la inversión en el fomento de la capacidad. Este repositorio también podría ayudar a los Estados a determinar otras medidas de fomento de la confianza adecuadas a sus contextos nacionales y regionales y ofrecer posibles modelos para su adaptación en otros ámbitos. Se observó que cualquier nuevo repositorio mundial debía evitar duplicar los acuerdos ya existentes y que deberían seguir debatiéndose las modalidades operacionales.

66. También se señalaron las funciones y responsabilidades de otros agentes, incluidos la sociedad civil, el sector privado, el mundo académico y la comunidad técnica, a la hora de contribuir a fomentar la confianza en el uso de las tecnologías de la información y las comunicaciones en los planos nacional, regional y mundial. Además, se observó la diversidad de iniciativas de múltiples partes interesadas que, mediante el desarrollo de principios y compromisos, han establecido nuevas redes para el intercambio, la colaboración y la cooperación. Asimismo, las iniciativas para sectores o ámbitos específicos han demostrado una conciencia cada vez mayor acerca de las funciones y responsabilidades de otros interlocutores y las contribuciones particulares que estos pueden realizar a la seguridad de la tecnología de la información y las comunicaciones mediante compromisos, códigos profesionales y normas de carácter voluntario.

Conclusiones y recomendaciones

67. Los Estados coincidieron en que el diálogo dentro del Grupo de Trabajo era, en sí mismo, una medida de fomento de la confianza, ya que estimula un intercambio de opiniones abierto y transparente sobre las percepciones de las amenazas y las vulnerabilidades, el comportamiento responsable de los Estados y otros agentes y buenas prácticas, lo que en última instancia contribuye al desarrollo y la aplicación colectivos del marco para el comportamiento responsable de los Estados en su uso de las tecnologías de la información y las comunicaciones.

68. Además, los Estados coincidieron en que las Naciones Unidas ejercían un papel fundamental en la elaboración y el apoyo a la aplicación de medidas mundiales de fomento de la confianza. En todos los informes del Grupo de Expertos aprobados por consenso se han recomendado medidas prácticas de fomento de la confianza. Además de estas recomendaciones orientadas específicamente a las tecnologías de la información y las comunicaciones, en la resolución 43/78 (H), aprobada por consenso, la Asamblea General hizo suyas las Directrices para las Medidas de Fomento de la Confianza elaboradas en la Comisión de Desarme de las Naciones Unidas, en las que se definían principios, objetivos y características de gran valor para las medidas de fomento de la confianza que pueden tenerse en cuenta al elaborar nuevas medidas orientadas específicamente a las tecnologías de la información y las comunicaciones.

69. Sobre la base de sus activos esenciales de la confianza y las relaciones que han establecido, los Estados coincidieron en que las organizaciones regionales y subregionales han realizado grandes esfuerzos por elaborar medidas de fomento de la confianza y adaptarlas a sus contextos y prioridades específicas, concienciar al público e intercambiar información entre sus miembros. Además, los intercambios regionales, interregionales e interinstitucionales pueden establecer nuevas vías de colaboración, cooperación y aprendizaje mutuo. Dado que no todos los Estados son miembros de una organización regional y no todas las organizaciones regionales aplican medidas de fomento de la confianza, se señaló que estas medidas eran complementarias de la labor de las Naciones Unidas y otras organizaciones para promover las medidas de fomento de la confianza.

70. Sobre la base de las lecciones y prácticas compartidas en el Grupo de Trabajo, los Estados coincidieron en que la existencia previa de mecanismos y estructuras nacionales y regionales, así como el desarrollo de recursos y capacidades adecuadas, como los equipos informáticos de respuesta de emergencia de ámbito nacional, eran fundamentales para que las medidas de fomento de la confianza cumplieran su objetivo previsto.

71. Como medida específica, los Estados coincidieron en que establecer puntos de contacto nacionales era una medida de fomento de la confianza en sí misma, pero también un requisito previo para la aplicación de otras muchas medidas de fomento de la confianza, y un elemento de valor incalculable en tiempos de crisis. A los Estados puede resultarles útil tener puntos de contacto, por ejemplo, para los intercambios diplomáticos, normativos, jurídicos y técnicos, así como para la notificación de incidentes y la respuesta a ellos.

El Grupo de Trabajo recomienda:

72. Que los Estados sigan informando al Secretario General, de forma voluntaria, sobre sus opiniones y evaluaciones, a fin de que pueda incluirlas en su informe anual sobre los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, e incluyan información adicional sobre las lecciones aprendidas y las buenas prácticas en relación con las medidas de fomento de la confianza pertinentes en los planos bilateral, regional o multilateral.

73. Que los Estados determinen y examinen voluntariamente las medidas de fomento de la confianza adecuadas para sus contextos específicos y cooperen con otros Estados en su aplicación.

74. Que, como medida de fomento de la confianza, los Estados reafirmen públicamente su compromiso de guiarse en su uso de las tecnologías de la información y las comunicaciones por el informe de 2015 del Grupo de Expertos Gubernamentales⁹.

75. Que los Estados apliquen voluntariamente medidas de transparencia compartiendo información y lecciones pertinentes en el formato y los foros que elijan, según corresponda, en particular a través del Cyber Policy Portal del Instituto de las Naciones Unidas de Investigación sobre el Desarme.

76. Que los Estados que aún no lo hayan hecho nombren a un punto de contacto nacional en los planos técnico, diplomático y de políticas, teniendo en cuenta las diferencias en la capacidad. Se alienta también a los Estados a seguir examinando las modalidades para establecer un directorio de estos puntos de contacto a nivel mundial.

⁹ [A/70/174](#), véase también [A/RES/70/237](#).

77. Que los Estados exploren mecanismos para mantener intercambios interregionales periódicos de lecciones aprendidas y buenas prácticas con respecto a las medidas de fomento de la confianza, teniendo en cuenta las diferencias en los contextos regionales y las estructuras de las organizaciones pertinentes.

78. Que los Estados sigan estudiando la posibilidad de adoptar medidas de fomento de la confianza en los planos bilateral, regional y multilateral y fomenten las oportunidades para el ejercicio cooperativo de estas medidas.

F. Desarrollo de la capacidad

79. La capacidad de la comunidad internacional para prevenir o atenuar las repercusiones de las actividades maliciosas en la esfera de la tecnología de la información y las comunicaciones depende de la capacidad que tenga cada Estado para prepararse y responder a ellas. El desarrollo de la capacidad ayuda a desarrollar las aptitudes, los recursos humanos, las políticas y las instituciones necesarias para aumentar la resiliencia y la seguridad de los Estados a fin de que puedan gozar plenamente de los beneficios de las tecnologías digitales. El desarrollo de la capacidad es un aspecto importante de la cooperación internacional y un acto voluntario del donante y del beneficiario, y es importante a la hora de promover el cumplimiento del derecho internacional y la aplicación de normas sobre el comportamiento responsable de los Estados y de apoyar la aplicación de medidas de fomento de la confianza. En un mundo digitalmente interdependiente, los beneficios del desarrollo de la capacidad se extienden más allá de los beneficiarios iniciales y contribuyen a crear un entorno más seguro y estable para todos en la esfera de la tecnología de la información y las comunicaciones.

Deliberaciones

80. En sus debates celebrados en el Grupo de Trabajo, los Estados pusieron de relieve la importancia que podía tener el desarrollo de la capacidad a la hora de permitir a todos los Estados y a otros agentes pertinentes participar plenamente en las deliberaciones internacionales sobre el marco para el comportamiento responsable de los Estados y, al mismo tiempo, contribuir a alcanzar compromisos comunes, como la Agenda 2030 para el Desarrollo Sostenible¹⁰. En este sentido, los Estados destacaron la necesidad de asignar suficientes recursos financieros y humanos a los programas de desarrollo de la capacidad.

81. Se destacó la importante labor que han realizado otros interlocutores, incluidas las organizaciones internacionales, los órganos regionales y subregionales, la sociedad civil, el sector privado, el mundo académico y los órganos técnicos especializados, para desarrollar la capacidad en materia de tecnologías de la información y las comunicaciones, y recomendaron que se reflexionara sobre el modo de fomentar la cooperación, la sostenibilidad, la eficacia y la reducción de la duplicación entre estas actividades.

82. Las Naciones Unidas pueden contribuir de modo fundamental a ayudar a los Estados a dar más visibilidad al desarrollo de la capacidad y pueden aprovechar su poder de convocatoria para fomentar una mayor coordinación de los diversos agentes

¹⁰ Algunos ejemplos de objetivos y metas pertinentes en relación con los Objetivos de Desarrollo Sostenible son aumentar significativamente el acceso a la tecnología de la información y las comunicaciones (9.C), mejorar la cooperación regional e internacional Norte-Sur, Sur-Sur y triangular en materia de ciencia, tecnología e innovación y el acceso a estas (17.6) y aumentar el apoyo internacional a la realización de actividades de creación de capacidad eficaces y específicas (17.9).

que participan en el desarrollo de la capacidad. Los Estados sugirieron que las plataformas que existen dentro de las Naciones Unidas, sus organismos especializados y la comunidad internacional en general podrían utilizarse para reforzar la coordinación ya establecida. Estas plataformas podrían usarse para compartir perspectivas nacionales acerca de las necesidades de desarrollo de la capacidad, alentar el intercambio de lecciones y experiencias, tanto de quienes reciben apoyo como de quienes lo proporcionan, y facilitar el acceso a información sobre el desarrollo de la capacidad y a programas de asistencia técnica. Estas plataformas también podrían apoyar la movilización de recursos o contribuir a destinar los recursos disponibles a atender las solicitudes de apoyo en el desarrollo de la capacidad y de asistencia técnica. Se sugirió que el desarrollo de un programa de desarrollo de la capacidad cibernética a nivel mundial bajo los auspicios de las Naciones Unidas podía contribuir a aumentar la coherencia en las actividades de desarrollo de la capacidad y que la realización de encuestas voluntarias de autoevaluación podía ayudar a los Estados a determinar y establecer prioridades en sus necesidades de desarrollo de la capacidad o su capacidad para proporcionar apoyo.

83. Si bien se recordó la responsabilidad primordial de los Estados de mantener un entorno seguro y de confianza en la esfera de la tecnología de la información y las comunicaciones, también se hizo hincapié en la importancia de adoptar un enfoque de múltiples interesados que aborde las brechas técnicas y normativas en todos los sectores pertinentes de la sociedad. Los Estados indicaron, en particular, que la sostenibilidad en el desarrollo de la capacidad podía mejorarse mediante un enfoque que implique la colaboración y las alianzas con la sociedad civil local, la comunidad técnica, las instituciones académicas y los agentes del sector privado, así como mediante la creación de grupos y centros de expertos. A este respecto, se destacó también que los enfoques nacionales en materia de seguridad de la tecnología de la información y las comunicaciones podrían mejorar si se adoptara un enfoque intersectorial, holístico y multidisciplinario del desarrollo de la capacidad, entre otras cosas mejorando los órganos de coordinación nacionales con la participación de las partes interesadas pertinentes a fin de evaluar la eficacia de los programas. Este enfoque también puede ayudar a afrontar los desafíos que representan las nuevas tecnologías emergentes.

84. Se señaló la brecha digital de género y se pidieron medidas específicas en los planos nacional e internacional para abordar las cuestiones de la igualdad de género y la participación significativa de las mujeres en los debates y los programas de desarrollo de la capacidad internacionales relativos a las tecnologías de la información y las comunicaciones y la seguridad internacional, en particular recopilando datos desglosados por género. Se reconocieron los programas que han facilitado la participación de las mujeres en debates multilaterales sobre la seguridad de la tecnología de la información y las comunicaciones. Asimismo, se hizo hincapié en la necesidad de reforzar los vínculos entre este tema y la agenda de las Naciones Unidas sobre las mujeres, la paz y la seguridad.

85. Se señaló que había muchos obstáculos que impedían el desarrollo de la capacidad o reducen su eficacia, e indicaron como aspectos especialmente preocupantes la coordinación y complementariedad insuficientes a la hora de determinar y ejecutar las actividades de desarrollo de la capacidad. También se expresaron preocupaciones prácticas en lo relativo a la determinación de las necesidades de desarrollo de la capacidad, la rapidez de la respuesta a las solicitudes de asistencia para el desarrollo de la capacidad y el diseño, la ejecución, la sostenibilidad y la accesibilidad de las actividades de desarrollo de la capacidad, así como la falta de criterios específicos para medir su repercusión. En muchos contextos, la falta de recursos humanos, financieros y técnicos suficientes impide las actividades de creación de capacidad y el progreso necesarios para reducir la brecha digital. Una

vez que se ha desarrollado la capacidad, algunos países se enfrentan al reto de retener el talento en un mercado competitivo para los profesionales de las tecnologías de la información y las comunicaciones. Los Estados mencionaron que otra dificultad era la falta de acceso a las tecnologías vinculadas a la seguridad de la tecnología de la información y las comunicaciones.

Conclusiones y recomendaciones

86. Garantizar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones es una responsabilidad común pero diferenciada que requiere una cooperación eficaz entre los Estados para reducir los riesgos para la paz y la seguridad internacionales. El desarrollo de la capacidad es un elemento crucial de esta cooperación. Teniendo en cuenta y elaborando más a fondo algunos principios ampliamente aceptados, los Estados coincidieron en que el desarrollo de la capacidad en relación con el uso de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional debe guiarse por los siguientes principios:

Proceso y finalidad

- El desarrollo de la capacidad debe ser un proceso sostenible y compuesto de actividades específicas realizadas por distintos agentes y destinadas a distintos agentes.
- Determinadas actividades deben tener un objetivo claro y centrarse en el logro de resultados y, al mismo tiempo, apoyar el objetivo común de establecer un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones.
- Las actividades de desarrollo de la capacidad deben contar con una base empírica y ser políticamente neutrales, transparentes, responsables e incondicionales.
- El desarrollo de la capacidad debe llevarse a cabo respetando plenamente el principio de la soberanía estatal.
- Es posible que deba facilitarse el acceso a las tecnologías pertinentes.

Alianzas

- Es preciso que el desarrollo de la capacidad se base en la confianza mutua y en la demanda, corresponda a unas necesidades y prioridades determinadas a nivel nacional y se lleve a cabo reconociendo plenamente la implicación nacional. Los asociados en el desarrollo de la capacidad deben participar en él voluntariamente.
- Dado que las actividades de desarrollo de la capacidad deben adaptarse a necesidades y contextos específicos, todas las partes son asociados activos en ellas, con responsabilidades compartidas pero diferenciadas, en particular las de colaborar en el diseño, la ejecución, el seguimiento y la evaluación de dichas actividades.
- Todos los asociados deben proteger y respetar la confidencialidad de las políticas y los planes nacionales.

Las personas

- El desarrollo de la capacidad debe respetar los derechos humanos y las libertades fundamentales, tener en cuenta las cuestiones de género y ser inclusivo, universal y no discriminatorio.

- Debe garantizarse la confidencialidad de la información sensible.

87. Los Estados coincidieron en que el desarrollo de la capacidad era una responsabilidad compartida y un proyecto recíproco, una “calle de dos vías” en que los participantes aprenden unos de otros y todas las partes se benefician de la mejora general de la seguridad de la tecnología de la información y las comunicaciones a nivel mundial. Asimismo, se recordó el valor de la cooperación Sur-Sur, Sur-Norte y triangular y de la cooperación centrada en el ámbito regional.

88. Los Estados coincidieron en que el desarrollo de la capacidad podía contribuir a que se comprendan y aborden los riesgos sistémicos y de otra índole que conllevan la falta de seguridad de la tecnología de la información y las comunicaciones, la falta de coordinación suficiente entre las capacidades técnicas y normativas en el plano nacional y los desafíos conexos de las desigualdades y las brechas digitales. Se consideró de especial importancia el desarrollo de la capacidad con miras a que los Estados pudieran determinar y proteger la infraestructura crítica nacional y colaborar en la protección de la infraestructura de información crítica. El intercambio de información y la coordinación en los planos nacional, regional e internacional puede hacer que las actividades de desarrollo de la capacidad sean más eficaces, estratégicas y acordes con las prioridades nacionales.

89. Además de las aptitudes técnicas, el fortalecimiento institucional y los mecanismos de cooperación, los Estados coincidieron en la necesidad urgente de fomentar conocimientos especializados en distintos ámbitos diplomáticos, jurídicos, normativos, legislativos y reglamentarios, y en este contexto se destacó la importancia de desarrollar la capacidad diplomática para participar en los procesos internacionales e intergubernamentales.

90. Los Estados recordaron la necesidad de un enfoque concreto y orientado a la acción en el desarrollo de la capacidad y convinieron en que estas medidas concretas podían incluir el apoyo en los planos normativo y técnico, por ejemplo, la elaboración de estrategias nacionales de ciberseguridad, la facilitación del acceso a las tecnologías pertinentes, el apoyo a los equipos informáticos de respuesta de emergencia o a los equipos de respuesta a incidentes de ciberseguridad y el establecimiento de formación especializada y planes de estudios adaptados, incluidos los programas de formación de formadores y la certificación profesional. Además, se reconocieron los beneficios de establecer centros de excelencia y otros mecanismos para el intercambio de información que incluyeran buenas prácticas jurídicas y administrativas.

El Grupo de Trabajo recomienda:

91. Que los Estados se guíen por los principios enunciados en el párrafo 86 en sus actividades de desarrollo de la capacidad vinculadas a las tecnologías de la información y las comunicaciones en el ámbito de la seguridad internacional.

92. Que los Estados sigan informando al Secretario General, de forma voluntaria, sobre sus opiniones y evaluaciones en relación con los avances en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional e incluyan información adicional sobre las lecciones aprendidas y las buenas prácticas con respecto a los programas y las iniciativas de desarrollo de la capacidad.

93. Que se aliente a los Estados y otros interlocutores que estén en condiciones de hacerlo a ofrecer asistencia financiera, técnica o en especie para el desarrollo de la capacidad. Debe seguir facilitándose una mayor promoción de la coordinación y la financiación de las actividades de desarrollo de la capacidad, en particular entre las organizaciones pertinentes y las Naciones Unidas.

94. Que los Estados sigan examinando el desarrollo de la capacidad en el plano multilateral, incluido el intercambio de opiniones, información y buenas prácticas.

G. Diálogo institucional periódico

95. El Grupo de Trabajo establecido en virtud de la resolución 73/27 de la Asamblea General ofreció, por primera vez bajo los auspicios de las Naciones Unidas, una plataforma específica para el diálogo abierta a todos los Estados sobre los avances en las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

96. Además de su objetivo de tratar de lograr entendimientos comunes entre todos los Estados mediante intercambios sustantivos, como se refleja en las secciones anteriores del presente informe, el Grupo de Trabajo ha fomentado redes diplomáticas y ha alentado la confianza entre sus participantes. La amplia implicación de las partes interesadas no gubernamentales ha demostrado que hay una comunidad más amplia de agentes dispuesta a aprovechar su experiencia para apoyar a los Estados en su objetivo de garantizar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. Las deliberaciones del Grupo de Trabajo fueron una afirmación de la importancia de los debates recurrentes y estructurados bajo los auspicios de las Naciones Unidas sobre el uso de las tecnologías de la información y las comunicaciones, como también se reconoce en los informes aprobados por consenso del Grupo de Expertos Gubernamentales.

Deliberaciones

97. En sus debates celebrados en el Grupo de Trabajo, los Estados recordaron el mandato del Grupo, incluido en la resolución 73/27 de la Asamblea General, de estudiar la posibilidad de establecer un diálogo institucional periódico y confirmaron que las evaluaciones y recomendaciones del Grupo de Trabajo en este sentido serían un resultado fundamental de su labor.

98. Los Estados expresaron opiniones diversas sobre los objetivos que debían ser prioritarios para el diálogo institucional periódico y sobre el formato de diálogo periódico que podía apoyar mejor estos objetivos. Algunos Estados expresaron el deseo de que el diálogo periódico dé prioridad a la aplicación de los compromisos y las recomendaciones vigentes, entre otras cosas desarrollando orientación para apoyar y supervisar su aplicación; coordinando y reforzando la eficacia del desarrollo de la capacidad; e indicando e intercambiando buenas prácticas. Otros Estados expresaron el deseo de que el diálogo periódico dé prioridad a seguir desarrollando los compromisos vigentes y a elaborar nuevos compromisos, como la negociación de un instrumento jurídicamente vinculante y las estructuras institucionales para apoyarlo.

99. Algunos Estados formularon una propuesta concreta sobre el establecimiento de un Programa de Acción que promueva un comportamiento responsable de los Estados en el ciberespacio con miras a crear un foro permanente de las Naciones Unidas para examinar el uso de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional. Se propuso que el Programa de Acción constituyera un compromiso político de los Estados con las recomendaciones, las normas y los principios convenidos, convocara reuniones ordinarias centradas en la aplicación, mejorara la cooperación y la creación de capacidad entre los Estados y celebrara conferencias de examen periódicas. En la propuesta del Programa de Acción también se previeron una participación y consultas amplias.

100. También se expresó el deseo de que la comunidad internacional regresara, en última instancia, a un único proceso basado en el consenso y el apoyo mundial desde

el principio a fin de garantizar la identificación colectiva con el proceso, y en este sentido observaron que los distintos formatos propuestos para el diálogo no eran necesariamente excluyentes entre sí. Se sugirió que distintos formatos podían ser complementarios o fusionarse para aprovechar las características particulares de cada uno y reducir la duplicación de esfuerzos, y se propuso que el Grupo de Trabajo elaborara una hoja de ruta en la que se indicaran temas y cuestiones prioritarias y plazos para un futuro diálogo institucional periódico.

101. Además, se planteó la necesidad de seguir examinando la duración y sostenibilidad del diálogo futuro, si debía ser en forma de deliberaciones u orientado a la acción, el momento y los posibles lugares para celebrarlo y las consideraciones presupuestarias pertinentes.

102. El examen de los avances en las tecnologías de la información y las comunicaciones y la seguridad internacional en las Naciones Unidas se centra en sus dimensiones de paz, estabilidad y prevención de conflictos a nivel internacional y, por tanto, se ha llevado a cabo en el marco de la Primera Comisión de la Asamblea General. Otros órganos de las Naciones Unidas tienen el mandato de examinar las dimensiones digitales de otras cuestiones, como el terrorismo, la delincuencia, el desarrollo y los derechos humanos, así como la gobernanza de Internet. Se sugirió que un mayor intercambio entre estos foros y los procesos establecidos por la Primera Comisión podría contribuir a reforzar las sinergias y mejorar la coherencia, respetando al mismo tiempo el carácter o el mandato especializados de cada órgano.

103. Si bien los Estados reconocieron su función y responsabilidad particulares en relación con la seguridad nacional e internacional, también subrayaron la importante contribución que realizaba el comportamiento responsable de otros interlocutores al logro de un entorno abierto, seguro, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones. Aumentar la cooperación y las alianzas entre múltiples partes interesadas puede facilitar la creación de un entorno más resiliente y seguro para estas tecnologías.

Conclusiones y recomendaciones

104. Los Estados coincidieron en que, dada la dependencia cada vez mayor de las tecnologías de la información y las comunicaciones y el alcance de las amenazas que se derivan de su uso indebido, era urgente lograr más entendimientos comunes, fomentar la confianza e intensificar la cooperación internacional.

105. Los Estados coincidieron también en que un diálogo periódico contribuía a los objetivos compartidos de reforzar la paz internacional, la estabilidad y la prevención de los conflictos en el entorno de la tecnología de la información y las comunicaciones.

106. Como principales responsables de la seguridad nacional, la seguridad pública y el estado de derecho, los Estados coincidieron en la importancia de mantener un diálogo intergubernamental periódico y recalcaron asimismo la importancia de decidir cuáles eran los mecanismos adecuados para la colaboración con otros grupos de partes interesadas en los procesos futuros.

107. Los Estados coincidieron en que el diálogo institucional periódico establecido a través de la Primera Comisión debía seguir centrándose en la paz y la seguridad internacionales a fin de no duplicar los mandatos, los esfuerzos y las actividades ya existentes de las Naciones Unidas centrados en las dimensiones digitales de otras

cuestiones, incluidos el terrorismo, la delincuencia, el desarrollo, los derechos humanos y la gobernanza de Internet¹¹.

108. Los Estados coincidieron en que el diálogo futuro sobre la cooperación internacional en torno a las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional debía, entre otras cosas, fomentar la confianza y alentar más estudios y debates sobre esferas en que aún no se ha logrado un entendimiento común.

109. Los Estados coincidieron en que el diálogo institucional periódico bajo los auspicios de las Naciones Unidas debía ser un proceso orientado a la acción que persiguiera objetivos específicos y se basara en los resultados anteriores, y que fuera inclusivo, transparente, centrado en el consenso y basado en los resultados.

110. Tras examinar los aspectos sustantivos de su mandato, que figuran en las secciones B a F del presente informe, los Estados recomendaron para cada sección una lista de acciones y medidas de cooperación concretas a fin de abordar las amenazas que entrañan las tecnologías de la información y las comunicaciones y promover un entorno abierto, seguro, estable, accesible y pacífico en relación con estas tecnologías. Los Estados también coincidieron en la necesidad de un mayor diálogo que incluyera el intercambio de opiniones o buenas prácticas nacionales sobre cuestiones relativas al modo en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones; la aplicación de normas y su ulterior desarrollo progresivo; y el desarrollo y la aplicación de medidas de fomento de la confianza y de desarrollo de la capacidad.

El Grupo de Trabajo recomienda:

111. Que los Estados consideren las conclusiones y recomendaciones del presente informe en todo proceso futuro de diálogo institucional periódico bajo los auspicios de las Naciones Unidas.

112. Que los Estados establezcan un programa para seguir impulsando los acuerdos y compromisos vigentes en su uso de las tecnologías de la información y las comunicaciones, según lo establecido en las resoluciones pertinentes de la Asamblea General, en particular la resolución [70/237](#), así como las conclusiones y recomendaciones de este Grupo de Trabajo. Estos debates se llevarían a cabo en el marco de la Primera Comisión de la Asamblea General de las Naciones Unidas en forma de un Programa de Acción para promover un comportamiento responsable de los Estados en el ciberespacio.

113. Que los Estados sigan participando activamente en un diálogo institucional periódico bajo los auspicios de las Naciones Unidas.

114. Que los Estados que estén en condiciones de hacerlo estudien la posibilidad de establecer o apoyar programas de patrocinio y otros mecanismos para garantizar una participación amplia en los procesos mencionados de las Naciones Unidas.

H. Observaciones finales

115. El Grupo de Trabajo supuso una oportunidad histórica de que todos los Estados mantuvieran largos debates, bajo los auspicios de las Naciones Unidas, centrados

¹¹ Véase el documento de antecedentes publicado por la Presidencia del Grupo de Trabajo, “An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme”, diciembre de 2019, disponible en <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf>.

específicamente en asuntos relativos a las tecnologías de la información y las comunicaciones y la seguridad internacional. Además de los muchos ámbitos de acuerdo reflejados en el presente informe, mediante sus debates inclusivos y transparentes, el Grupo de Trabajo ha servido como una valiosa medida para fomentar la confianza y los entendimientos entre los Estados y ha ayudado a establecer una red diplomática mundial de expertos nacionales. La participación activa y amplia de todas las delegaciones ha demostrado la determinación de los Estados de seguir abordando unidos esta cuestión de importancia fundamental para todos.

116. Los períodos de sesiones oficiales, oficiosos y virtuales del Grupo de Trabajo se caracterizaron por intercambios interactivos sustantivos entre los Estados, así como con la sociedad civil, el sector privado, el mundo académico y la comunidad técnica. El compromiso demostrado por los Estados y otras partes interesadas durante toda la labor del Grupo de Trabajo, con su participación cada vez mayor, incluso cuando algunas de sus reuniones pasaron a adoptar un formato virtual, es muestra innegable de la importancia cada vez más universal de los temas que examina, así como del reconocimiento cada vez mayor de la necesidad urgente de afrontar colectivamente las amenazas que representa para la seguridad internacional el uso malintencionado de las tecnologías de la información y las comunicaciones.

117. El Grupo de Trabajo ha demostrado la firme voluntad colectiva de la comunidad internacional de seguir trabajando unida para lograr un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones que beneficie a todos los Estados y pueblos. A lo largo de todas sus deliberaciones en el Grupo de Trabajo, los Estados subrayaron los vínculos y las sinergias entre cada uno de los elementos de su mandato: las normas voluntarias no vinculantes refuerzan y complementan las obligaciones vigentes en virtud del derecho internacional. Estos dos elementos definen las expectativas sobre el comportamiento en relación con los usos de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional y, de este modo, también contribuyen a fomentar la confianza, aumentando la transparencia y la cooperación entre los Estados, y a reducir el riesgo de conflicto. A su vez, el desarrollo de la capacidad permite que todos los Estados contribuyan a aumentar la estabilidad y la seguridad a nivel mundial. Conjuntamente, estos elementos constituyen un marco mundial de medidas de cooperación para hacer frente a amenazas reales o potenciales en el ámbito de las tecnologías de la información y las comunicaciones. Mantener un diálogo institucional periódico brindará la oportunidad de seguir desarrollando y aplicando este marco mediante el fomento de entendimientos comunes, el intercambio de las lecciones aprendidas y las buenas prácticas de aplicación, el fomento de la confianza y el aumento de la capacidad entre los Estados.