Naciones Unidas A/70/174

Asamblea General

Distr. general
22 de julio de 2015
Español
Original: inglés

Septuagésimo período de sesiones
Tema 93 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Nota del Secretario General

El Secretario General tiene el honor de remitir adjunto el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. El Grupo fue creado en cumplimiento de lo dispuesto en el párrafo 4 de la resolución 68/243 de la Asamblea General.

* A/70/150.

15-12404(S) 050815 200815

Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Resumen

Las tecnologías de la información y las comunicaciones (TIC) brindan inmensas oportunidades y su importancia para la comunidad internacional es cada vez mayor. Sin embargo, existen tendencias preocupantes que generan riesgos para la paz y la seguridad internacionales. Para reducir estos riesgos, es esencial que exista una cooperación eficaz entre los Estados.

El Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2015 examinó las amenazas reales y potenciales derivadas de la utilización de las TIC por los Estados y analizó las acciones necesarias para hacerles frente, incluidas normas, reglas, principios y medidas de fomento de la confianza. Además, el Grupo examinó la forma en que el derecho internacional se aplica al uso por los Estados de las TIC. El Grupo actual avanzó mucho en esas esferas, sobre la base del trabajo realizado por los Grupos anteriores.

El presente informe amplía considerablemente la discusión sobre las normas. El Grupo recomendó que los Estados colaboraran para evitar la aplicación de prácticas perjudiciales en la esfera de las TIC y que no permitieran deliberadamente que su territorio fuera utilizado para que se cometan hechos internacionalmente ilícitos mediante esas tecnologías. También abogó por que se incrementara el intercambio de información y la asistencia para entablar acciones penales por el uso de las TIC con fines terroristas y delictivos, haciendo hincapié en que los Estados deberían garantizar el pleno respeto de los derechos humanos, incluido el derecho a la privacidad y la libertad de expresión.

Una recomendación importante fue que un Estado no debería realizar o apoyar de forma deliberada actividades en la esfera de las TIC que dañaran intencionadamente infraestructuras fundamentales o dificultaran de otro modo su utilización y funcionamiento. Los Estados también deberían tomar las medidas apropiadas para proteger sus infraestructuras fundamentales frente a las amenazas relacionadas con las TIC. Asimismo, los Estados no deberían dañar los sistemas de información de los equipos autorizados de respuesta a emergencias de otro Estado ni utilizar esos equipos para participar en una actividad internacional malintencionada. Los Estados deberían alentar la divulgación responsable de las vulnerabilidades de las TIC y adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro y evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC o funciones ocultas y dañinas.

Las medidas de fomento de la confianza mejoran la cooperación y la transparencia, y reducen el riesgo de conflictos. El Grupo indicó varias medidas de fomento de la confianza de carácter voluntario para aumentar la transparencia y sugirió que los Estados estudiaran otras para reforzar la cooperación. El Grupo insistió en la necesidad de que se mantuviera un diálogo regular con una amplia participación bajo los auspicios de las Naciones Unidas y a través de foros bilaterales, regionales y multilaterales. Si bien los Estados tienen la responsabilidad

primordial de garantizar un entorno de TIC seguro y pacífico, la cooperación internacional mejoraría si el sector privado, el mundo académico y la sociedad civil participaran de manera adecuada.

La creación de capacidad es fundamental para la cooperación y el fomento de la confianza. En el informe presentado por el Grupo en 2013 (véase A/68/98) se instó a la comunidad internacional a prestar asistencia para mejorar la seguridad de las infraestructuras fundamentales de tecnologías de la información y las comunicaciones, ayudar a desarrollar la pericia técnica y asesorar sobre la preparación de leyes, estrategias y marcos reguladores apropiados. El Grupo actual reiteró esas conclusiones e hizo hincapié en que todos los Estados podían aprender de los demás en relación con las amenazas a las que se enfrentaban y la eficacia de las consiguientes respuestas.

El Grupo destacó la importancia del derecho internacional, la Carta de las Naciones Unidas y el principio de soberanía como base para lograr una mayor seguridad en el uso de las TIC por los Estados. El Grupo, si bien reconoció que era necesario realizar un estudio más amplio, señaló el derecho inmanente que tienen los Estados de adoptar medidas de conformidad con el derecho internacional, con arreglo a lo dispuesto en la Carta. El Grupo también llamó la atención sobre la existencia de principios jurídicos internacionales establecidos, entre ellos, de ser aplicables, los principios de humanidad, necesidad, proporcionalidad y distinción.

En cuanto a la labor futura, el Grupo propuso que la Asamblea General estudiara la posibilidad de convocar un nuevo Grupo de Expertos Gubernamentales en 2016.

Asimismo, el Grupo pidió a los Estados Miembros que estudiaran seriamente sus recomendaciones y valoraran la forma de seguirlas desarrollando y aplicando.

Índice

Prólogo del Secretario General

Pocas tecnologías han sido tan poderosas como las tecnologías de la información y las comunicaciones (TIC) a la hora de producir cambios en las economías, las sociedades y las relaciones internacionales. El ciberespacio afecta a todos los aspectos de nuestras vidas. Las ventajas que ofrece son innumerables, pero también conlleva riesgos. Solo se puede lograr que el ciberespacio sea un entorno estable y seguro mediante la cooperación internacional, y la base de esta cooperación deben ser el derecho internacional y los principios de la Carta de las Naciones Unidas.

El presente informe recoge las recomendaciones preparadas por expertos gubernamentales de 20 Estados destinadas a hacer frente a las amenazas reales y potenciales derivadas del uso de las TIC, tanto por agentes estatales como no estatales, que puedan comprometer la paz y la seguridad internacionales. Los expertos han tomado como base los informes aprobados por consenso publicados en 2010 y 2013 y ofrecen ideas sobre el establecimiento de normas, el fomento de la confianza, la creación de capacidad y la aplicación del derecho internacional.

Entre las cuestiones complejas que han surgido figura el creciente uso malintencionado de las TIC por extremistas, terroristas y grupos delictivos organizados. El presente informe recoge propuestas que pueden ayudar a abordar esta preocupante tendencia y contribuir a la formulación de mi próximo plan de acción para prevenir el extremismo violento.

A todos los Estados les interesa que el ciberespacio sea más seguro. Las iniciativas que se tomen en este ámbito deben respetar el compromiso mundial de favorecer que Internet sea abierta, segura y pacífica. En este espíritu, encomiendo el presente informe a la Asamblea General y a la comunidad mundial en general como un documento que contribuye de manera crucial a garantizar la seguridad del entorno de las TIC.

Carta de envío

26 de junio de 2015

Tengo el honor de adjuntar a la presente el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. El Grupo fue establecido en 2014 en aplicación del párrafo 4 de la resolución 68/243 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Como Presidente del Grupo, me complace señalar que el informe se aprobó por consenso.

En su resolución, la Asamblea General solicitó que en 2014 se estableciera un grupo de expertos gubernamentales sobre la base de una distribución geográfica equitativa, con el mandato de seguir examinando, con miras a promover un entendimiento común, las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza, las cuestiones relativas al uso de las tecnologías de la información y las comunicaciones en los conflictos y la manera en que se aplica el derecho internacional al uso de esas tecnologías por los Estados, así como los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. También se pidió al Grupo que tuviese en cuenta las evaluaciones y recomendaciones de un Grupo anterior (véase A/68/98) y se solicitó al Secretario General que presentase un informe sobre los resultados de dicho examen a la Asamblea en su septuagésimo período de sesiones.

De conformidad con lo dispuesto en la resolución, se designó a expertos de 20 Estados: Alemania, Belarús, Brasil, China, Colombia, Egipto, España, Estados Unidos de América, Estonia, Federación de Rusia, Francia, Ghana, Israel, Japón, Kenya, Malasia, México, Pakistán, Reino Unido de Gran Bretaña e Irlanda del Norte y República de Corea. La lista de expertos figura en el anexo.

En las reuniones del Grupo hubo un intercambio amplio y profundo de opiniones sobre las novedades que se habían producido en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. El Grupo celebró cuatro períodos de sesiones: el primero, del 21 al 25 de julio de 2014, en la Sede de las Naciones Unidas; el segundo, del 12 al 16 de enero de 2014, en Ginebra; y el tercero y el cuarto, del 13 al 17 de abril de 2015 y del 22 al 26 de junio de 2015, respectivamente, en la Sede de las Naciones Unidas.

El Grupo desea expresar su agradecimiento a los expertos que actuaron como facilitadores en las deliberaciones del proyecto de informe: el Sr. Ricardo Mor (España), la Sra. Florence Mangin (Francia), la Sra. Katherine Getao (Kenya), el Sr. Ausaf Ali (Pakistán) y la Sra. Olivia Preston (Reino Unido).

El Grupo desea expresar su reconocimiento por la contribución aportada por el Instituto de las Naciones Unidas de Investigación sobre el Desarme, que prestó asesoramiento al Grupo y estuvo representado por el Sr. James Lewis y la Sra. Kerstin Vignard. También desea dar las gracias al Sr. Ewen Buchanan, de la Oficina de Asuntos de Desarme de las Naciones Unidas, que se desempeñó como Secretario del Grupo, y a otros funcionarios de la Secretaría que le prestaron su asistencia.

(*Firmado*) Carlos Luís Dantas Coutinho **Perez**
Presidente del Grupo

I. Introducción

1. De conformidad con la resolución 68/243 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, el Secretario General estableció, sobre la base de una distribución geográfica equitativa, un grupo de expertos gubernamentales con el mandato de seguir examinando, con miras a promover un entendimiento común, las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza, las cuestiones relativas al uso de las tecnologías de la información y las comunicaciones en los conflictos y la manera en que se aplica el derecho internacional al uso de esas tecnologías por los Estados, así como los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

2. La existencia de un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las tecnologías de la información y las comunicaciones (TIC) es esencial para todos y requiere que exista una cooperación eficaz entre los Estados a fin de reducir los riesgos para la paz y la seguridad internacionales. El presente informe recoge las recomendaciones del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y profundiza la labor realizada por los Grupos anteriores (véanse A/65/201 y A/68/98). El Grupo examinó los conceptos internacionales pertinentes y las posibles medidas de cooperación que atañen a su mandato y reafirmó que promover la utilización de las TIC con fines pacíficos y prevenir conflictos derivados del uso de estas tecnologías redunda en interés de todos los Estados.

II. Amenazas reales y potenciales

3. Las TIC brindan inmensas oportunidades para el desarrollo social y económico, y su importancia para la comunidad internacional es cada vez mayor. Sin embargo, existen tendencias preocupantes en el entorno mundial de las TIC, en particular un aumento pronunciado de incidentes relacionados con el uso malintencionado de dichas tecnologías por agentes estatales y no estatales. Estas tendencias generan riesgos para todos los Estados y un uso indebido de estas tecnologías puede socavar los esfuerzos por mantener la paz y la seguridad internacionales.

4. Varios Estados están desarrollando capacidad en materia de TIC con fines militares y aumentando las probabilidades de que los futuros conflictos entre Estados entrañen el uso de esas tecnologías.

5. Entre los ataques más perjudiciales en los que se utilizan las TIC se encuentran los dirigidos contra la infraestructura fundamental y los sistemas de información conexos de un Estado. El riesgo de ataques dañinos de esta naturaleza contra infraestructura fundamental es a la vez real y grave.

6. La utilización de las TIC con fines de terrorismo, más allá del reclutamiento, la financiación, la capacitación y la incitación, e incluso la comisión de atentados terroristas contra las TIC o infraestructuras dependientes de estas tecnologías, es

una posibilidad creciente que, si no se aborda, podría amenazar la paz y la seguridad internacionales.

7. Algunos factores que agravan los riesgos son la diversidad de agentes no estatales malintencionados, incluidos los grupos delictivos y los terroristas, sus distintas motivaciones, la velocidad con la que pueden producirse actos maliciosos relacionados con las TIC y la dificultad de determinar el origen de los incidentes en esta esfera. Los Estados están legítimamente preocupados por el peligro que representan las percepciones erróneas y desestabilizadoras, el potencial para generar conflictos y la posibilidad de que se inflijan daños a sus ciudadanos, los bienes y la economía.

8. Las diferencias en los niveles de capacidad que tienen los Estados en la esfera de la seguridad de las TIC pueden aumentar la vulnerabilidad en un mundo interconectado.

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

9. El entorno de las TIC ofrece a la comunidad internacional oportunidades y retos a la hora de determinar cómo se aplican las normas, reglas y principios a las actividades que realizan los Estados en la esfera de estas tecnologías. Un objetivo es seguir determinando qué normas pueden ser voluntarias y no vinculantes para el comportamiento responsable de los Estados y fortalecer un entendimiento común para aumentar la estabilidad y la seguridad en el entorno mundial de las TIC.

10. Las normas voluntarias y no vinculantes del comportamiento responsable de los Estados pueden reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. Por consiguiente, las normas no tratan de limitar ni prohibir acciones que, por lo demás, son compatibles con el derecho internacional. Las normas reflejan las expectativas de la comunidad internacional, establecen criterios para un comportamiento responsable de los Estados y permiten que la comunidad internacional evalúe las actividades e intenciones de estos. Las normas pueden ayudar a prevenir los conflictos en el entorno de las TIC y contribuir a su utilización con fines pacíficos para permitir que la plena realización de esas tecnologías incremente el desarrollo social y económico mundial.

11. Los informes anteriores del Grupo muestran que existe un consenso incipiente sobre el comportamiento responsable de los Estados en lo que respecta a la seguridad y al uso de las TIC derivado de las normas y los compromisos internacionales existentes. El Grupo actual tenía ante sí la tarea de seguir examinando normas de comportamiento responsable de los Estados con miras a promover un entendimiento común; determinar los casos en que deben formularse las normas vigentes para que se las aplique en el entorno de las TIC; fomentar una mayor aceptación de tales normas; y señalar los ámbitos en que es preciso elaborar normas complementarias que tengan en cuenta la complejidad y las características singulares de estas tecnologías.

12. El Grupo tomó nota de la propuesta de China, la Federación de Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán de un código internacional de conducta para la seguridad de la información (véase A/69/723).

13. Teniendo en cuenta las amenazas reales y potenciales, los riesgos y las vulnerabilidades, y tomando como base las evaluaciones y recomendaciones que figuran en los informes de los Grupos anteriores de 2010 y 2013, el Grupo actual ofrece las siguientes recomendaciones para el examen por los Estados de normas, reglas y principios voluntarios y no vinculantes de comportamiento responsable de los Estados con miras a promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las TIC:

a) Los Estados, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, deberían colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las TIC y evitar las prácticas en la esfera de las TIC que se consideran que son perjudiciales o que pueden poner en peligro la paz y la seguridad internacionales;

b) En el caso de incidentes relacionados con las TIC, los Estados deberían tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías, así como la naturaleza y el alcance de las consecuencias;

c) Los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC;

d) Los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas. Quizás los Estados deberían considerar si existe la necesidad de elaborar nuevas medidas a este respecto;

e) Los Estados, para garantizar la utilización segura de las TIC, han de acatar las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión;

f) Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras fundamentales que prestan servicios al público o dificultaran de otro modo su utilización y funcionamiento;

g) Los Estados deberían tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta, la resolución 58/199 de la Asamblea General sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales y otras resoluciones pertinentes;

h) Los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales fueran objeto de actos malintencionados relacionados con las TIC. Los Estados también deberían atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada

con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía;

i) Los Estados deberían adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confiaran en la seguridad de los productos relacionados con las TIC. Los Estados deberían tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC, así como el uso de funciones ocultas y dañinas;

j) Los Estados deberían alentar la divulgación responsable de las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o infraestructuras dependientes de esas tecnologías;

k) Los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática) de otro Estado. Un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada.

14. El Grupo señaló que, aunque estas medidas puedan ser esenciales para promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las TIC, su aplicación inmediata podría no ser posible, concretamente en países en desarrollo, hasta que estos adquieran la capacidad adecuada.

15. Teniendo en cuenta los atributos singulares de las TIC, con el tiempo podrían elaborarse más normas.

IV. Medidas de fomento de la confianza

16. Las medidas de fomento de la confianza fortalecen la paz y la seguridad internacionales y pueden incrementar la cooperación, la transparencia, la previsibilidad y la estabilidad entre los Estados. En su labor orientada a fomentar la confianza, con miras a asegurar un entorno pacífico en la esfera de las TIC, los Estados deberían tener en cuenta las Directrices para las Medidas de Fomento de la Confianza aprobadas por la Comisión de Desarme en 1988 y que la Asamblea General hizo suyas por consenso en su resolución 43/78 (H). Con objeto de promover la confianza y la cooperación y reducir el riesgo de conflicto, el Grupo recomienda que los Estados consideren las siguientes medidas de fomento de la confianza de carácter voluntario:

a) Establecer puntos de contacto adecuados en los niveles técnico y de políticas para abordar los incidentes graves en la esfera de las TIC y crear un directorio de contactos de ese tipo;

b) Establecer mecanismos y procesos de consulta bilateral, regional, subregional y multilateral, y dar apoyo a esos mecanismos y procesos, según proceda, con objeto de mejorar el fomento de la confianza entre los Estados y reducir el riesgo que representan las percepciones erróneas, la escalada de los incidentes y el conflicto que puedan derivarse de los incidentes relacionados con las TIC;

c) Fomentar, con carácter voluntario, la transparencia en los planos bilateral, subregional, regional y multilateral, según proceda, a fin de aumentar la confianza y para que sirva de base a la labor futura, lo que podría incluir el intercambio voluntario de información y opiniones sobre diversos aspectos de las amenazas nacionales y transnacionales a las TIC y la utilización de esas tecnologías; las vulnerabilidades y las funciones que se han descubierto, ocultas y dañinas, de los productos relacionados con las TIC; las mejores prácticas para la seguridad de las TIC; las medidas de fomento de la confianza elaboradas en foros regionales y multilaterales; y las organizaciones, estrategias, políticas y programas nacionales pertinentes para la seguridad de las TIC;

d) La presentación voluntaria por los Estados de sus opiniones nacionales sobre las categorías de infraestructura que consideran fundamentales y de las medidas nacionales para protegerlas, incluida información sobre leyes y políticas nacionales para la protección de datos y de infraestructuras sustentadas en las TIC. Los Estados deberían tratar de facilitar la cooperación transfronteriza para hacer frente a las vulnerabilidades de las infraestructuras fundamentales que trascienden las fronteras nacionales. Estas medidas podrían incluir lo siguiente:

i) Un repositorio de las leyes y políticas nacionales para la protección de datos y de infraestructuras sustentadas en las TIC y la publicación de los materiales sobre estas leyes y políticas nacionales que estimen adecuados para su distribución;

ii) El desarrollo de mecanismos y procesos de consulta bilateral, subregional, regional y multilateral sobre la protección de infraestructuras fundamentales sustentadas en las TIC;

iii) La elaboración en los planos bilateral, subregional, regional y multilateral de mecanismos técnicos, jurídicos y diplomáticos para hacer frente a las solicitudes relacionadas con las TIC;

iv) La adopción de mecanismos nacionales de carácter voluntario para clasificar los incidentes relacionados con las TIC en función de la escala y de la gravedad de esos hechos, a fin de fomentar el intercambio de información sobre ellos.

17. Los Estados deberían estudiar otras medidas de fomento de la confianza que contribuyan a reforzar la cooperación en los planos bilateral, subregional, regional y multilateral. Entre ellas podría figurar el acuerdo voluntario entre los Estados con el fin de:

a) Fortalecer mecanismos de cooperación entre los organismos competentes para hacer frente a los incidentes de seguridad relacionados con las TIC y elaborar nuevos mecanismos técnicos, jurídicos y diplomáticos para atender las solicitudes relacionadas con las infraestructuras sustentadas en las TIC, incluida la posibilidad de intercambiar personal en esferas como la respuesta ante los incidentes y el cumplimiento de la ley, cuando corresponda, y alentar intercambios entre las instituciones académicas y de investigación;

b) Promover la cooperación, en particular mediante el establecimiento de centros de coordinación para intercambiar información sobre la utilización malintencionada de las TIC y prestar asistencia en investigaciones;

c) Establecer a nivel nacional un equipo de respuesta a emergencias informáticas o un equipo de respuesta a incidentes de seguridad informática, o designar oficialmente a una organización que desempeñe esta función. Los Estados tal vez deseen examinar estos órganos con arreglo a su definición de infraestructura fundamental. Los Estados deberían apoyar y facilitar el funcionamiento de esos equipos nacionales de respuesta y la cooperación de esos equipos entre sí y con otros órganos autorizados;

d) Ampliar y apoyar las prácticas de cooperación entre los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de seguridad informática, según proceda, como el intercambio de información sobre las vulnerabilidades, las pautas de ataque y las mejores prácticas para mitigar los ataques, incluida la coordinación de las respuestas, la organización de simulacros, el apoyo a la gestión de incidentes relacionados con las TIC y la mejora de las prácticas de cooperación regionales y sectoriales;

e) Cooperar, con arreglo al derecho nacional e internacional, en relación con las solicitudes de asistencia de otros Estados para investigar delitos relacionados con las TIC o su uso con fines terroristas o para mitigar las actividades malintencionadas en la esfera de las TIC que se originen en su territorio.

18. El Grupo reitera que, dada la velocidad a que evolucionan las TIC y el alcance de la amenaza, es necesario afianzar el entendimiento común e intensificar la cooperación. En este sentido, el Grupo recomienda que se celebre con regularidad un diálogo institucional con una amplia participación bajo los auspicios de las Naciones Unidas y diálogos en foros bilaterales, regionales y multilaterales y otras organizaciones internacionales.

V. Cooperación y asistencia internacionales para promover la seguridad y la creación de capacidad en la esfera de las TIC

19. Aunque los Estados tienen la responsabilidad primordial de preservar la seguridad nacional y la de sus ciudadanos, incluso en el entorno de la TIC, quizás algunos de ellos carezcan de la capacidad suficiente para proteger sus redes de TIC. Esa falta de capacidad puede hacer que las infraestructuras fundamentales y los ciudadanos de un Estado sean vulnerables o convertir a un Estado en refugio involuntario de agentes malintencionados. La cooperación y la asistencia internacionales pueden desempeñar una función esencial para que los Estados garanticen la seguridad de las TIC y velen por su uso con fines pacíficos. La prestación de asistencia para crear capacidad en materia de seguridad de las TIC también es fundamental para la seguridad internacional, ya que mejora la capacidad de cooperación y acción colectiva de los Estados. El Grupo convino en que las medidas de creación de capacidad deberían tratar de promover la utilización de las TIC para fines pacíficos.

20. El Grupo hizo suyas las recomendaciones sobre creación de capacidad que figuran en los informes de 2010 y 2013. En el informe de 2010 se recomendó que los Estados determinaran qué medidas serían necesarias para apoyar la creación de capacidad en los países menos adelantados. En el informe de 2013 se instó a la comunidad internacional a colaborar en la prestación de asistencia para mejorar la

seguridad de las infraestructuras fundamentales de las TIC; desarrollar la pericia técnica y preparar leyes, estrategias y marcos reguladores apropiados para cumplir sus responsabilidades; y salvar las diferencias de seguridad de las TIC y su uso. El Grupo actual también hizo hincapié en que la creación de capacidad no se limita a que los países desarrollados transfieran conocimientos y competencias técnicas a los países en desarrollo, ya que todos los Estados pueden aprender de los demás en relación con las amenazas a las que se enfrentan y la eficacia de las consiguientes respuestas.

21. Tomando como base la labor originada en resoluciones e informes anteriores de las Naciones Unidas, incluida 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”, los Estados deberían plantearse la posibilidad de adoptar las siguientes medidas voluntarias para prestar asistencia técnica y de otro tipo a fin de crear capacidad para asegurar que cuenten con TIC los países que requieran y soliciten asistencia:

a) Prestar asistencia en lo que respecta al fortalecimiento de mecanismos de cooperación con los equipos de respuesta a emergencias cibernéticas nacionales y otros órganos autorizados;

b) Proporcionar a los países en desarrollo asistencia y capacitación para mejorar la seguridad en el uso de las TIC, incluida la infraestructura fundamental, e intercambiar las mejores prácticas jurídicas y administrativas;

c) Ayudar a proporcionar acceso a tecnologías que se consideran esenciales para la seguridad de las TIC;

d) Establecer procedimientos para la asistencia mutua a la hora de responder a los incidentes y de hacer frente a problemas a corto plazo de seguridad de las redes, incluidos los procedimientos para acelerar la asistencia;

e) Facilitar la cooperación transfronteriza para hacer frente a las vulnerabilidades de las infraestructuras fundamentales que trascienden las fronteras nacionales;

f) Elaborar estrategias de sostenibilidad en las iniciativas de creación de capacidad relativas a la seguridad de las TIC;

g) Dar prioridad a concienciar sobre la seguridad de las TIC y la creación de capacidad en los planes y presupuestos nacionales y asignar a la seguridad la debida importancia en la planificación del desarrollo y la asistencia, lo que podría incluir programas de sensibilización sobre la seguridad de las TIC encaminados a educar e informar a las instituciones y los ciudadanos. Estos programas podrían llevarse a cabo junto a iniciativas de las organizaciones internacionales, incluidas las Naciones Unidas y sus organismos, así como del sector privado, el mundo académico y organizaciones de la sociedad civil;

h) Alentar la continuación de la labor de creación de capacidad, por ejemplo en técnicas forenses o en medidas de cooperación para hacer frente al uso de las TIC con fines terroristas o delictivos.

22. Sería útil elaborar enfoques regionales de creación de capacidad, dado que en esos enfoques se podrían tener en cuenta aspectos específicos de carácter cultural,

geográfico, político, económico o social, y propiciar un enfoque adaptado a cada caso concreto.

23. En aras de crear capacidad en materia de seguridad en la esfera de las TIC, los Estados pueden examinar la posibilidad de elaborar iniciativas de cooperación bilateral y multilateral sobre la base de las relaciones de colaboración ya establecidas. Esas iniciativas ayudarían a mejorar el entorno para que los Estados se prestaran una asistencia mutua eficaz a la hora de responder a los incidentes relacionados con las TIC, y las organizaciones internacionales competentes, incluidas las Naciones Unidas y sus organismos, así como el sector privado, el mundo académico y organizaciones de la sociedad civil, podrían desarrollarlas aún más.

VI. Aplicación del derecho internacional al uso de las TIC

24. En el informe de 2013, se afirmó que el derecho internacional, en particular la Carta de las Naciones Unidas, 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 las TIC. De conformidad con su mandato, el Grupo actual examinó la forma en que el derecho internacional se aplica al uso por los Estados de las TIC.

25. La adhesión de los Estados al derecho internacional, en particular a las obligaciones que les competen en virtud de la Carta, constituye un marco esencial para sus acciones en lo que respecta a la utilización de las TIC, así como para promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de estas tecnologías. Esas obligaciones son esenciales para examinar la aplicación del derecho internacional al uso de las TIC por los Estados.

26. Al examinar la aplicación del derecho internacional a la utilización de estas tecnologías, el Grupo señaló la importancia fundamental que tenían los compromisos de los Estados con los siguientes principios de la Carta y otras normas del derecho internacional: la igualdad soberana; la solución de controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia; la abstención, en sus relaciones internacionales, de recurrir 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 libertades fundamentales; y la no intervención en los asuntos internos de otros Estados.

27. La soberanía de los Estados y las normas y principios internacionales dimanantes de la soberanía se aplican a la realización de actividades relacionadas con las TIC por parte de los Estados, así como a su jurisdicción sobre la infraestructura de esas tecnologías dentro de su territorio.

28. El Grupo actual, partiendo de la labor de los Grupos anteriores y guiado por la Carta y el mandato establecido en la resolución 68/243 de la Asamblea General, ofrece las siguientes opiniones, que no son exhaustivas, sobre la forma en que el derecho internacional se aplica al uso por los Estados de las TIC:

a) Los Estados ostentan la jurisdicción sobre las infraestructuras de TIC ubicadas en su territorio;

b) En su utilización de las TIC, los Estados deben observar, entre otros principios del derecho internacional, la soberanía de cada Estado, la igualdad soberana, la solución de controversias por medios pacíficos y la no intervención en los asuntos internos de otros Estados. Las obligaciones existentes en virtud del derecho internacional son aplicables al uso por los Estados de las TIC. Los Estados deben cumplir sus obligaciones en virtud del derecho internacional para respetar y proteger los derechos humanos y las libertades fundamentales;

c) El Grupo, subrayando las aspiraciones de la comunidad internacional de lograr el uso de las TIC con fines pacíficos para el bien común de la humanidad y recordando que la Carta se aplica en su totalidad, manifiesta que los Estados tienen el derecho inmanente de adoptar medidas compatibles con el derecho internacional como se reconoce en la Carta. El Grupo reconoce la necesidad de seguir examinando esta cuestión;

d) El Grupo señala que existen principios jurídicos internacionales establecidos, incluidos, si procede, los principios de humanidad, necesidad, proporcionalidad y distinción;

e) Los Estados no deben recurrir a terceros para cometer hechos internacionalmente ilícitos mediante las TIC y deberían tratar de garantizar que su territorio no sea utilizado por agentes no estatales para cometer tales hechos;

f) Los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional. No obstante, la determinación de que cierta actividad relacionada con las TIC se ha puesto en marcha o se ha originado de alguna manera en el territorio o en la infraestructura de las TIC de un Estado podría no ser suficiente en sí misma para atribuir dicha actividad a ese Estado. El Grupo señaló que las acusaciones de organizar y cometer hechos ilícitos dirigidas contra los Estados deberían estar fundamentadas.

29. Asimismo, el Grupo señaló que el entendimiento común sobre la forma en que se aplica el derecho internacional al uso por los Estados de las TIC era importante para promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de esas tecnologías.

VII. Conclusiones y recomendaciones para la labor futura

30. Se ha avanzado mucho en el reconocimiento de los riesgos que el uso malintencionado de las TIC representa para la paz y la seguridad internacionales. El Grupo, admitiendo que las TIC pueden ser una fuerza impulsora para acelerar los progresos hacia el desarrollo, y en consonancia con la necesidad de preservar la conectividad mundial y el flujo libre y seguro de la información, consideró útil señalar posibles medidas que podrían adoptarse para su labor futura, entre ellas, aunque no exclusivamente, las siguientes:

a) La realización por los Estados, individual y colectivamente, de una labor de profundización de los conceptos relativos a la paz y la seguridad internacionales en el uso de las TIC en el plano jurídico, técnico y político; y

b) El aumento de la cooperación a nivel regional y multilateral a fin de fomentar un entendimiento común sobre los posibles riesgos que representa para la

paz y la seguridad internacionales el uso malintencionado de las TIC y sobre la seguridad de las infraestructuras fundamentales sustentadas en esas tecnologías.

31. Si bien los Estados tienen la responsabilidad primordial de garantizar un entorno seguro y pacífico en la esfera de las TIC, la eficacia de la cooperación internacional mejoraría si se establecieran mecanismos para la participación, según procediera, del sector privado, el mundo académico y organizaciones de la sociedad civil.

32. Algunas esferas en las que podría ser útil la realización de nuevos estudios e investigaciones son, por ejemplo, los conceptos relacionados con el uso por los Estados de las TIC. El Instituto de las Naciones Unidas de Investigación sobre el Desarme, que presta servicios a todos los Estados Miembros, es una de las entidades a las que podría pedirse que realizara los estudios pertinentes, al igual que a otros centros de estudio y organizaciones de investigación.

33. Las Naciones Unidas deberían desempeñar una función primordial en la promoción del diálogo sobre la seguridad de las TIC cuando son utilizadas por los Estados y en el desarrollo de un entendimiento común sobre la aplicación del derecho internacional y las normas, reglas y principios de comportamiento responsable de los Estados. Como parte de la labor futura se podrían estudiar posibles mecanismos para el diálogo internacional y el intercambio de opiniones sobre cuestiones relacionadas con la seguridad de las TIC. Esas iniciativas no deberían duplicar la labor en curso de otras organizaciones y foros internacionales sobre cuestiones como el uso de las TIC con fines delictivos o terroristas, los derechos humanos y la gobernanza de Internet.

34. El Grupo señala la importancia de que la Asamblea General estudie la posibilidad de convocar un nuevo Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en 2016 con el mandato de seguir examinando, con miras a promover un entendimiento común, las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, así como la forma en que el derecho internacional se aplica al uso por los Estados de las TIC a saber, normas, reglas o principios de comportamiento responsable de los Estados, medidas de fomento de la confianza y la creación de capacidad.

35. El Grupo reconoce los valiosos esfuerzos realizados por las organizaciones internacionales y los grupos regionales en la esfera de las TIC. Los Estados, al colaborar en materia de seguridad en la utilización de las TIC, deberían tener en cuenta estas iniciativas y los Estados Miembros deberían alentar, cuando procediera, la creación de nuevos foros de diálogo, consulta y creación de capacidad bilaterales, regionales y multilaterales.

36. El Grupo recomienda que los Estados Miembros estudien seriamente las recomendaciones que figuran en el presente informe sobre cómo ayudar a crear un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las TIC, y examinen la forma en que podrían desarrollarlas y aplicarlas.

Anexo

Lista de los miembros del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Alemania

Sr. Karsten Geier
Jefe del Personal de Coordinación de Políticas sobre Asuntos Cibernéticos de la Oficina Federal de Relaciones Exteriores

Belarús

Sr. Aliaksandr Chasnouski (períodos de sesiones tercero y cuarto)
Jefe Adjunto del Departamento de Seguridad Internacional y de Control de Armamentos del Ministerio de Relaciones Exteriores

Embajador Vladimir N. Gerasimovich (primer período de sesiones)
Jefe del Departamento de Seguridad Internacional y de Control de Armamentos del Ministerio de Relaciones Exteriores

Sr. Ivan Grinevich (segundo período de sesiones)
Consejero de la Misión Permanente de Belarús ante las Naciones Unidas en Ginebra

Brasil

Sr. Carlos Luís Dantas Coutinho Perez
Ministro, Jefe de Estado Mayor del Viceministro de Asuntos Políticos del Ministerio de Relaciones Exteriores

China

Sr. Haitao Wu (períodos de sesiones tercero y cuarto)
Coordinador para Asuntos Cibernéticos del Ministerio de Relaciones Exteriores

Sr. Cong Fu (períodos de sesiones primero y segundo)
Coordinador para Asuntos Cibernéticos del Ministerio de Relaciones Exteriores

Colombia

Sr. Jorge Fernando Bejarano
Director de Estándares y Arquitectura de Tecnología de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones

Egipto

Sr. Sameh Aboul-Enein
Embajador, Viceministro de Relaciones Exteriores para Desarme, Seguridad Internacional y Energía Nuclear con Fines Pacíficos del Ministerio de Relaciones Exteriores

Sr. Amr Aljowaily (tercer período de sesiones)
Ministro, Misión Permanente de Egipto ante las Naciones Unidas

España

Sr. Ricardo Mor (cuarto período de sesiones)
Embajador en Misión Especial para la Ciberseguridad del Ministerio de Asuntos Exteriores y de Cooperación

Sra. Alicia Moral (períodos de sesiones primero, segundo y tercero)
Embajadora en Misión Especial para la Ciberseguridad del Ministerio de Asuntos Exteriores y de Cooperación

Estados Unidos de América

Sra. Michele G. Markoff
Coordinadora Adjunta de Asuntos Cibernéticos, Oficina del Coordinador de Asuntos Cibernéticos, Secretaría de Estado, Departamento de Estado

Estonia

Sra. Marina Kaljurand
Viceministra y Asesora Jurídica del Ministerio de Relaciones Exteriores

Federación de Rusia

Sr. Andrey V. Krutskikh
Representante Especial del Presidente de la Federación de Rusia para la Cooperación Internacional en Seguridad de la Información, Embajador en Misión Especial

Francia

Sra. Florence Mangin
Embajadora, Coordinadora de Seguridad Cibernética del Ministerio de Relaciones Exteriores

Sr. Leonard Rolland (primer período de sesiones)
Departamento de Asuntos Estratégicos, Seguridad y Desarme del Ministerio de Relaciones Exteriores

Ghana

Sr. Mark-Oliver Kevor
Miembro del Consejo de Administración de la Autoridad Nacional de Comunicaciones

Israel

Sr. Iddo Moed
Coordinador de Seguridad Cibernética del Ministerio de Relaciones Exteriores

Japón

Sr. Takashi Okada (períodos de sesiones tercero y cuarto)
Embajador a cargo de Asuntos de las Naciones Unidas y de Políticas sobre Asuntos Cibernéticos, Director General Adjunto de la Oficina de Política Exterior del Ministerio de Relaciones Exteriores

Sr. Akira Kono (segundo período de sesiones)
Embajador a cargo de Asuntos de las Naciones Unidas y de Políticas sobre Asuntos Cibernéticos, Director General Adjunto de la Oficina de Política Exterior del Ministerio de Relaciones Exteriores

Sr. Takao Imafuku (primer período de sesiones)
Negociador Superior sobre Asuntos de Seguridad Internacional de la Oficina de Política Exterior del Ministerio de Relaciones Exteriores

Kenya

Sra. Katherine Getao
Secretaria de Tecnología de la Información y las Comunicaciones del Ministerio de Información, Comunicaciones y Tecnología

Malasia

Sra. Nur Hayuna Abd Karim (cuarto período de sesiones)
Subsecretaria Principal de la División de Seguridad Cibernética y Espacial del Consejo Nacional de Seguridad

Sr. Md Shah Nuri bin Md Zain (períodos de sesiones primero, segundo y tercero)
Subsecretario de la División de Seguridad Cibernética y Espacial del Consejo Nacional de Seguridad

México

Sr. Edgar Zurita
Agregado ante Canadá y Estados Unidos, Comisión Nacional de Seguridad de México – Policía Federal

Pakistán

Sr. Ausaf Ali (períodos de sesiones primero, segundo y cuarto)
Director General de la Subdivisión de Asuntos Técnicos de la División de Planes Estratégicos en la Sede de los Jefes de Estado Mayor

Sr. Khalil Hashmi (tercer período de sesiones)
Ministro, Misión Permanente de Pakistán ante las Naciones Unidas

Reino Unido de Gran Bretaña e Irlanda del Norte

Sra. Olivia Preston
Directora Adjunta de la Oficina de Seguridad Cibernética y Seguridad de la Información, Oficina del Gabinete

República de Corea

Sr. Chul Lee (períodos de sesiones segundo y cuarto)
Director de la División de Seguridad Internacional del Ministerio de Relaciones Exteriores

Sr. Hyuncheol Jang (períodos de sesiones primero y tercero)
Asesor de la Embajada de la República de Corea en el Reino de Bélgica y la Unión Europea