Naciones Unidas A/76/135

Asamblea General

Distr. general
14 de julio de 2021
Español
Original: inglés

Septuagésimo sexto período de sesiones
Tema 96 de la lista provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional

Nota del Secretario General

El Secretario General tiene el honor de transmitir adjunto el informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. El Grupo se estableció en virtud del párrafo 3 de la resolución 73/266 de la Asamblea General.

* A/76/50.

Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional*

Resumen

A medida que la dependencia mundial de las tecnologías de la información y las comunicaciones sigue aumentando, el comportamiento responsable de los Estados en el uso de esas tecnologías ha adquirido una importancia vital para el mantenimiento de la paz y la seguridad internacionales.

En cumplimiento del mandato contenido en la resolución 73/266 de la Asamblea General, el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, activo entre 2019 y 2021, ha continuado estudiando, con miras a promover un entendimiento común y la aplicación eficaz, las posibles medidas de cooperación para encarar las amenazas reales y potenciales en el ámbito de la seguridad de la información.

El presente informe contiene las conclusiones del Grupo sobre las amenazas actuales y emergentes; las normas, reglas y principios de comportamiento responsable de los Estados; el derecho internacional; las medidas de fomento de la confianza; y la cooperación y asistencia internacionales en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones y la creación de capacidad. En cada uno de estos temas, el informe refleja una labor de reflexión que se añade a las conclusiones y recomendaciones de anteriores Grupos de Expertos Gubernamentales.

* Publicado sin revisión editorial.

Índice

Prólogo del Secretario General

Las tecnologías de la información y las comunicaciones siguen transformando rápidamente las sociedades, ofreciendo numerosas oportunidades y planteando al mismo tiempo importantes riesgos. La pandemia de enfermedad por coronavirus (COVID-19) ha acelerado aún más el tránsito de muchos aspectos de nuestra vida al espacio digital, así como nuestra dependencia de las tecnologías digitales.

Mientras tanto, la vigilancia y la manipulación digitales van en aumento y el mundo en línea está adquiriendo unos perfiles que no siempre sirven al interés público. Si este proceso no se controla, los efectos podrían ser destructivos tanto para las sociedades como para las personas. La necesidad de abordar estos retos, aprovechar los beneficios de las tecnologías de la información y las comunicaciones y promover el comportamiento responsable de los Estados en el contexto de la seguridad internacional es más urgente que nunca.

En cumplimiento de su mandato, el Grupo de Expertos Gubernamentales, activo entre 2019 y 2021, llevó a cabo amplias deliberaciones a lo largo de 18 meses. Este esfuerzo también se enriqueció con consultas informales a nivel regional y reuniones oficiosas abiertas a todos los Estados Miembros. El informe del Grupo y la labor del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, que aprobó un informe consensuado en marzo de 2021, son complementarios.

En los últimos años, los Estados y otras partes interesadas públicas y privadas han concedido una importancia creciente a los esfuerzos de las Naciones Unidas para promover el uso pacífico de las tecnologías de la información y las comunicaciones. Con este espíritu, el informe representa una contribución a la promoción de un entorno abierto, seguro, estable y accesible para esas tecnologías. También es un llamamiento renovado a una mayor cooperación con el fin de reducir los riesgos cibernéticos para la paz y la seguridad internacionales, y de garantizar la protección y promoción de los derechos humanos y las libertades fundamentales tanto en línea como fuera de ella.

Carta de envío

28 de mayo de 2021

Tengo el honor de transmitir adjunto el informe de consenso del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. El Grupo se estableció en 2018 en virtud del párrafo 3 de la resolución 73/266 de la Asamblea General.

En esta resolución, la Asamblea General solicitó que en 2019 se estableciera un grupo de expertos gubernamentales sobre la base de una distribución geográfica equitativa que, a partir de las evaluaciones y recomendaciones contenidas en los informes de consenso del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015, y con miras a promover un entendimiento común y la aplicación eficaz, continuara estudiando las posibles medidas de cooperación para encarar las amenazas reales y potenciales en el ámbito de la seguridad de la información, con inclusión de las normas, reglas y principios de comportamiento responsable de los Estados, las medidas de fomento de la confianza y el desarrollo de la capacidad, así como la forma en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones por los Estados. Se solicitó al Secretario General que presentara a la Asamblea en su septuagésimo sexto período de sesiones un informe sobre los resultados del estudio.

De acuerdo con el mandato del Grupo, está previsto que se publique en el sitio web de la Oficina de Asuntos de Desarme de las Naciones Unidas un compendio oficial de las contribuciones nacionales voluntarias de los expertos gubernamentales participantes sobre la cuestión de cómo se aplica el derecho internacional al uso de las tecnologías de la información y las comunicaciones por los Estados; las contribuciones se publicarán en el idioma original en que se hayan presentado, sin traducción (A/76/136).

Conforme a lo dispuesto en la resolución, se nombraron expertos de 25 Estados: Alemania, Australia, Brasil, China, Estados Unidos de América, Estonia, Federación Rusa, Francia, India, Indonesia, Japón, Jordania, Kazajstán, Kenya, Mauricio, Marruecos, México, Noruega, Países Bajos, Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania, Singapur, Sudáfrica, Suiza y Uruguay. La lista de expertos figura como anexo del informe.

El Grupo celebró cuatro períodos de sesiones oficiales: el primero, del 9 al 13 de diciembre de 2019 en la Sede de las Naciones Unidas, el segundo, del 24 al 28 de febrero de 2020 en Ginebra, el tercero, en formato virtual del 5 al 9 de abril de 2021, y el cuarto, en formato virtual del 24 al 28 de mayo de 2021. El tercer período de sesiones del Grupo se aplazó en virtud de la decisión 75/551 de la Asamblea General debido a la pandemia de COVID-19. No obstante, el Grupo continuó sus actividades durante ese tiempo mediante una serie consultas oficiosas entre períodos de sesiones. De acuerdo con su mandato, también se celebraron una serie de consultas con las organizaciones regionales pertinentes y reuniones consultivas abiertas con los Estados Miembros para mantener debates interactivos e intercambiar opiniones.

El Grupo desea expresar su agradecimiento por la contribución del equipo de apoyo conjunto de la Oficina de Asuntos de Desarme de las Naciones Unidas y del Instituto de las Naciones Unidas de Investigación sobre el Desarme.

También aprovecho esta oportunidad para expresar mi gratitud personal al Gobierno del Brasil por haberme designado y al Grupo por el honor de confiarme la presidencia. También doy las gracias a mis compañeros expertos, a mis colegas brasileños, a los miembros del equipo de apoyo conjunto y a la Secretaría de las Naciones Unidas, en particular al Alto Representante para Asuntos de Desarme, por su apoyo y por compartir su gran experiencia con un espíritu de compromiso constructivo.

(*Firmado*) Guilherme **de Aguiar Patriota**
Presidente del Grupo

I. Introducción

1. El presente informe refleja el resultado de los debates llevados a cabo por el Grupo de Expertos Gubernamentales en cumplimiento de la resolución 73/266 de la Asamblea General, relativa a la “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”. Una parte fundamental de la labor del Grupo se llevó a cabo durante la pandemia de enfermedad por coronavirus (COVID-19), que ha puesto de relieve el enorme potencial de las tecnologías digitales, al tiempo que ha acelerado la dependencia mundial respecto de esas tecnologías. Esto, a su vez, ha destacado aún más la importancia de un comportamiento responsable en el uso de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la seguridad internacional.

2. El informe se basa en las evaluaciones y recomendaciones de los informes de consenso de 2010, 2013 y 2015 de los diversos Grupos de Expertos Gubernamentales de las Naciones Unidas relativas a las amenazas actuales y emergentes, las normas, reglas y principios de comportamiento responsable de los Estados, el derecho internacional, el fomento de la confianza y la cooperación internacional y la creación de capacidad, y reafirma tales evaluaciones y recomendaciones, que en conjunto representan un marco acumulativo y evolutivo para el comportamiento responsable de los Estados en su uso de las TIC. El Grupo valora positivamente la aprobación por consenso del informe del Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, establecido de conformidad con la resolución 73/27 de la Asamblea General[1], que se basa en este marco y lo reafirma.

3. El Grupo examinó las cuestiones comprendidas en su mandato a la luz de su importancia para la paz y la seguridad internacionales. Además, su intención era aportar una reflexión adicional que facilitara la comprensión de las evaluaciones y recomendaciones de los anteriores informes del Grupo de Expertos Gubernamentales, a fin de ofrecer orientación para contribuir a su aplicación. Este nivel adicional de comprensión reafirma los vínculos entre los diferentes elementos sustantivos del mandato del Grupo y la importancia de involucrar a otros actores, incluidos el sector privado, la sociedad civil, el mundo académico y la comunidad técnica, cuando proceda, en los esfuerzos de los Estados por aplicar las recomendaciones.

4. El Grupo reconoce el importante papel que desempeñan los organismos regionales y subregionales a la hora de llevar adelante las evaluaciones y recomendaciones de los informes de los Grupos de Expertos Gubernamentales y de desarrollar mecanismos específicos para cada región y reforzar las iniciativas de creación de capacidad en apoyo de su aplicación. De acuerdo con el mandato del Grupo, estas y otras opiniones y experiencias pertinentes fueron compartidas con el Grupo durante las reuniones consultivas oficiosas que este mantuvo en Nueva York con los Estados Miembros y a través de una serie de consultas celebradas en colaboración con organizaciones regionales[2].

5. El Grupo reafirma que garantizar un entorno de las TIC que sea abierto, seguro, estable, accesible y pacífico es esencial para todas las personas y requiere una cooperación eficaz entre los Estados a fin de reducir los riesgos para la paz y la seguridad internacionales. La promoción del uso de las TIC con fines pacíficos es algo que interesa a todo el mundo y es fundamental para el bien común. El respeto a

[1] A/75/816.

[2] Los informes de las diversas consultas están disponibles en: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf y https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

la soberanía y a los derechos humanos y las libertades fundamentales, así como el desarrollo sostenible y digital, siguen siendo el eje de estos esfuerzos.

II. Amenazas actuales y emergentes

6. Aunque las TIC, en un contexto mundial cada vez más digitalizado y conectado, ofrecen inmensas oportunidades a las sociedades de todo el planeta, el Grupo reafirma la persistencia de las graves amenazas relacionadas con las TIC que se describieron en informes anteriores. Los incidentes relacionados con el uso malintencionado de las TIC por parte de Estados y actores no estatales han aumentado en alcance, escala, gravedad y complejidad. Aunque las amenazas relacionadas con las TIC se manifiestan de forma diferente en cada región, sus efectos también pueden ser globales.

7. El Grupo subraya las conclusiones del informe de 2015 en el sentido de que varios Estados están desarrollando capacidades de TIC con fines militares, y que el uso de las TIC en futuros conflictos entre Estados es cada vez más probable.

8. La actividad malintencionada relacionada con las TIC por parte de actores que generan amenazas persistentes, incluidos los Estados y otros agentes, pueden suponer un riesgo significativo para la seguridad y la estabilidad internacionales y el desarrollo económico y social, así como para la seguridad y el bienestar de las personas.

9. Además, los Estados y otros actores están utilizando activamente capacidades de TIC más complejas y sofisticadas con fines políticos y de otro tipo. Por otra parte, el Grupo observa un aumento preocupante del uso malintencionado por los Estados de campañas de información encubiertas con ayuda de las TIC para influir en los procesos, los sistemas y la estabilidad general de otros Estados. Estos usos socavan la confianza y pueden dar lugar a escaladas y amenazar la paz y la seguridad internacionales. También pueden suponer un daño directo o indirecto para las personas.

10. Las actividades perjudiciales relacionadas con las TIC contra las infraestructuras críticas que prestan servicios a nivel nacional, regional o mundial, que han sido objeto de examen en informes anteriores del Grupo de Expertos Gubernamentales, son cada vez más graves. Preocupan especialmente las actividades malintencionadas relativas a las TIC que afectan a las infraestructuras de información críticas, las infraestructuras que prestan servicios esenciales al público, las infraestructuras técnicas esenciales que garantizan la disponibilidad general o la integridad de Internet y las entidades del sector de la salud. La pandemia de COVID-19 ha puesto en evidencia los riesgos y las consecuencias de las actividades malintencionadas relacionadas con las TIC con las que se trata de explotar las vulnerabilidades en momentos en que nuestras sociedades soportan una enorme presión.

11. Las tecnologías nuevas y emergentes están ampliando las oportunidades de desarrollo, aunque sus propiedades y características, en constante evolución, también amplían los ámbitos de ataque, creando nuevos vectores y vulnerabilidades que pueden ser explotados para actividades malintencionadas relacionadas con las TIC. Garantizar que las vulnerabilidades de la tecnología operacional y los dispositivos informáticos, plataformas, máquinas u objetos interconectados que constituyen la Internet de las cosas no se exploten con fines malintencionados se ha convertido en una grave preocupación.

12. Las capacidades para asegurar los sistemas de información siguen siendo diferentes en todo el mundo, al igual que las capacidades para desarrollar la

resiliencia, proteger la infraestructura de información crítica, detectar las amenazas y responder a ellas de manera oportuna. Estas diferencias en cuanto a capacidades y recursos, así como las disparidades en la legislación, la reglamentación y las prácticas nacionales relacionadas con el uso de las TIC y el desigual conocimiento y acceso a las medidas de cooperación regionales y mundiales disponibles para mitigar, investigar o recuperarse de tales incidentes, son factores que aumentan las vulnerabilidades y los riesgos para todos los Estados.

13. El Grupo reafirma que el uso de las TIC para fines terroristas, más allá del reclutamiento, la financiación, el adiestramiento y la incitación, incluso para ataques terroristas contra las TIC o las infraestructuras que dependen de esas tecnologías, es una posibilidad creciente que, si no se aborda, puede amenazar la paz y la seguridad internacionales.

14. El Grupo reafirma también que la diversidad de actores malintencionados de carácter no estatal, incluidos los grupos delictivos y los terroristas, sus diferentes motivos, la rapidez con la que pueden producirse las acciones malintencionadas relacionadas con las TIC y la dificultad de atribuir el origen de un incidente relativo a esas tecnologías son factores que aumentan el riesgo.

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

15. En relación con el uso de las TIC por los Estados, el Grupo reafirma que la existencia de normas voluntarias y no vinculantes de comportamiento responsable de los Estados puede reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. Las normas coexisten con el derecho internacional vigente y no pretenden limitar o prohibir una acción que, por lo demás, sea compatible con el derecho internacional. Las normas reflejan las expectativas de la comunidad internacional y establecen estándares de comportamiento responsable de los Estados. En este sentido, pueden ayudar a evitar conflictos en el entorno de las TIC y contribuir a su uso pacífico y su realización plena a fin de aumentar el desarrollo social y económico mundial.

16. El Grupo también subraya la interrelación entre las normas, las medidas de fomento de la confianza, la cooperación internacional y la creación de capacidad. Dadas las singulares características de las TIC, el Grupo reafirma la observación del informe de 2015 de que, con el tiempo, pueden desarrollarse nuevas normas y, por otra parte, señala la posibilidad de que en el futuro se elaboren nuevas obligaciones vinculantes, si procede.

17. Además de la labor realizada en el sistema de las Naciones Unidas, el Grupo reconoce la valiosa experiencia en materia de normas que está surgiendo a nivel regional, incluidas las compartidas durante las consultas oficiosas celebradas con los Estados Miembros en Nueva York y en colaboración con las organizaciones regionales de acuerdo con su mandato, y señala que en los futuros trabajos sobre las TIC en el contexto de la seguridad internacional deberían tenerse en cuenta esos esfuerzos. El Grupo también observó la propuesta de China, la Federación de Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán de un código de conducta internacional para la seguridad de la información (véase A/69/723).

18. En la resolución 70/237, aprobada por consenso, la Asamblea General exhortó a los Estados Miembros a que, en su uso de las TIC, se guiaran por el informe de 2015 del Grupo de Expertos Gubernamentales, que incluía 11 normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados. De conformidad con su mandato de promover un comportamiento responsable, el Grupo realizó una

reflexión adicional para facilitar la comprensión de estas normas, subrayando su valor con respecto al comportamiento esperado de los Estados en su uso de las TIC en el contexto de la paz y la seguridad internacionales y proporcionando ejemplos de los tipos de acuerdos institucionales que los Estados pueden poner en marcha a nivel nacional y regional para apoyar su aplicación. El Grupo recuerda a los Estados que esos esfuerzos deben realizarse de acuerdo con las obligaciones que les incumben en virtud de la Carta de las Naciones Unidas y otras normas de derecho internacional, con el fin de preservar un entorno de las TIC abierto, seguro, estable, accesible y pacífico. Se exhorta a los Estados a que eviten los usos de las TIC que no se ajusten a las normas de comportamiento responsable del Estado y a que se abstengan de ellos.

Norma 13 a). En consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, los Estados deben cooperar en la formulación y aplicación de medidas para aumentar la estabilidad y la seguridad en el uso de las TIC y prevenir las prácticas relacionadas con esas tecnologías que se haya reconocido que son perjudiciales o que pueden entrañar amenazas a la paz y la seguridad internacionales.

19. El mantenimiento de la paz y la seguridad internacionales y la cooperación internacional son algunos de los propósitos fundacionales de las Naciones Unidas. Esta norma es un recordatorio de que la aspiración común y el interés de todos los Estados es cooperar y trabajar juntos para promover el uso de las TIC con fines pacíficos y prevenir los conflictos derivados de su uso indebido.

20. En este sentido, y en cumplimiento de la citada norma, el Grupo alienta a los Estados a que se abstengan de utilizar las TIC y las redes de TIC para llevar a cabo actividades que puedan amenazar el mantenimiento de la paz y la seguridad internacionales.

21. Las medidas recomendadas por anteriores Grupos de Expertos Gubernamentales y 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 representan un marco inicial para el comportamiento responsable de los Estados en el uso de las TIC. Como orientación adicional, y a fin de facilitar dicha cooperación, el Grupo recomienda que los Estados establezcan o refuercen los mecanismos, estructuras y procedimientos existentes a nivel nacional, como la política y la legislación pertinentes y los procesos de revisión correspondientes; mecanismos de gestión de crisis e incidentes; acuerdos pangubernamentales de cooperación y asociación; y acuerdos de cooperación y diálogo con el sector privado, el mundo académico, la sociedad civil y la comunidad técnica. También se alienta a los Estados a que recopilen y simplifiquen la información que presenten sobre la aplicación de las normas, incluso mediante la realización de encuestas voluntarias sobre sus esfuerzos nacionales y la puesta en común de sus experiencias.

Norma 13 b). En el caso de incidentes relacionados con las TIC, los Estados deben 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 y la naturaleza y el alcance de las consecuencias.

22. Esta norma reconoce que la atribución es una operación compleja y que deben tenerse en cuenta diversos factores antes de establecer el origen de un incidente relacionado con las TIC. A este respecto, la cautela que se pide en el párrafo 71 g) del presente informe y en informes anteriores del Grupo de Expertos Gubernamentales puede ayudar a evitar malentendidos y una escalada de tensiones entre los Estados.

23. Se alienta a los Estados que son objeto de actividades malintencionadas relacionadas con las TIC, y a los Estados desde cuyo territorio se sospecha que se han originado dichas actividades, a que mantengan consultas entre las autoridades competentes que procedan.

24. Un Estado que es víctima de un incidente malintencionado relacionado con las TIC debe tener en cuenta todos los aspectos en su evaluación del incidente. Esos aspectos, que han de basarse en hechos probados, pueden incluir las características técnicas del incidente; su alcance, escala y efectos; el contexto más amplio, incluida la relación del incidente con la paz y la seguridad internacionales; y los resultados de las consultas entre los Estados afectados.

25. La respuesta de un Estado afectado a una actividad malintencionada relacionada con las TIC atribuible a otro Estado debe ser conforme a las obligaciones que le incumben en virtud de la Carta de las Naciones Unidas y otras normas del derecho internacional, incluidas las relativas a la solución de controversias por medios pacíficos y a los hechos internacionalmente ilícitos. Los Estados también pueden aprovechar toda la gama de opciones diplomáticas, jurídicas y de consulta que tienen a su disposición, así como los mecanismos voluntarios y otros compromisos políticos que permiten la solución de desacuerdos y controversias mediante consultas y otros medios pacíficos.

26. Para hacer operativa esta norma a nivel nacional y facilitar la investigación y resolución de los incidentes relacionados con las TIC que afectan a otros Estados, los Estados pueden establecer o reforzar las estructuras nacionales pertinentes, las políticas, procesos, marcos legislativos y mecanismos de coordinación relacionados con las TIC y las asociaciones y otras formas de colaboración con las partes interesadas pertinentes para evaluar la gravedad y la posibilidad de reproducción de un incidente relacionado con las TIC.

27. La cooperación a nivel regional e internacional, incluso entre los equipos de respuesta a emergencias informáticas o los equipos de respuesta a incidentes de ciberseguridad nacionales, las autoridades de los Estados competentes en materia de TIC y la comunidad diplomática, puede fortalecer la capacidad de los Estados para detectar e investigar los incidentes malintencionados relacionados con las TIC y fundamentar sus preocupaciones y constataciones antes de llegar a una conclusión sobre un incidente.

28. Los Estados también pueden utilizar plataformas multilaterales, regionales, bilaterales y de múltiples partes interesadas para intercambiar prácticas y compartir información sobre enfoques nacionales de atribución, incluso sobre el modo en que distinguen entre distintos tipos de atribución, y sobre amenazas e incidentes relacionados con las TIC. El Grupo también recomienda que en la labor futura de las Naciones Unidas se estudie además la forma de fomentar entendimientos comunes y el intercambio de prácticas sobre la atribución.

Norma 13 c). Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC.

29. Esta norma refleja la expectativa de que si un Estado tiene constancia o es informado de buena fe de que un hecho internacionalmente ilícito realizado usando TIC se origina en su territorio o lo utiliza, debe tomar todas las medidas apropiadas y razonablemente disponibles y factibles para detectar, investigar y abordar la situación. La norma expresa el entendimiento de que un Estado no debe permitir que otro Estado o actor no estatal utilice las TIC dentro de su territorio para cometer hechos internacionalmente ilícitos.

30. Al considerar cómo cumplir los objetivos de esta norma, los Estados deben tener en cuenta lo siguiente:

a) La norma establece la expectativa de que los Estados tomen medidas razonables dentro de su capacidad para poner fin a la actividad que tiene lugar en su territorio por medios que sean proporcionados, apropiados y eficaces y de forma coherente con el derecho internacional e interno. No obstante, no se espera que los Estados puedan o deban controlar todas las actividades relacionadas con las TIC que se realizan en su territorio.

b) Un Estado que sea consciente de que se están cometiendo hechos internacionalmente ilícitos utilizando TIC situadas en su territorio, pero carezca de la capacidad necesaria para hacerles frente, puede considerar la posibilidad de solicitar asistencia a otros Estados o al sector privado de forma coherente con el derecho internacional e interno. El establecimiento de las estructuras y mecanismos pertinentes para formular y responder a las solicitudes de asistencia puede contribuir a la aplicación de esta norma. Los Estados deben actuar de buena fe y de conformidad con el derecho internacional al prestar asistencia y no aprovechar la oportunidad para realizar actividades malintencionadas contra el Estado que la solicita o contra un tercer Estado.

c) Un Estado afectado por una actividad debe notificarla al Estado en el que se origina. El Estado notificado debe acusar recibo de la notificación para facilitar la cooperación y la clarificación de los hechos y hacer todos los esfuerzos razonables para contribuir a determinar si se ha cometido un hecho internacionalmente ilícito. El acuse de recibo de esta notificación no indica que se esté de acuerdo con la información contenida en ella.

d) El hecho de que un incidente relacionado con las TIC tenga su origen en el territorio o la infraestructura de un tercer Estado no implica, por sí mismo, la responsabilidad de ese Estado en el incidente. Además, la notificación a un Estado de que su territorio se está utilizando para realizar un hecho ilícito no implica, por sí misma, que sea responsable de ese hecho.

Norma 13 d). Los Estados deben estudiar la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, enjuiciar la utilización de las TIC con fines terroristas y delictivos e implementar otras medidas de cooperación para hacer frente a esas amenazas. Tal vez los Estados deban considerar si es necesario elaborar nuevas medidas a este respecto.

31. Esta norma recuerda a los Estados la importancia de la cooperación internacional para hacer frente a las amenazas transfronterizas que supone la utilización de Internet y las TIC por los actores terroristas y delictivos, incluso para fines de reclutamiento, financiación, adiestramiento e incitación, planificación y coordinación de atentados y promoción de sus ideas y acciones, y otros propósitos similares que se destacan en el presente informe. La norma reconoce que los avances en la respuesta a estas y otras amenazas del mismo tipo que implican a grupos e individuos terroristas y delictivos, a través de las medidas existentes y de otras medidas, pueden contribuir a la paz y la seguridad internacionales.

32. La observancia de esta norma implica la existencia de políticas, legislación, estructuras y mecanismos nacionales que faciliten la cooperación transfronteriza en cuestiones técnicas, policiales, jurídicas y diplomáticas pertinentes para abordar la utilización de las TIC con fines delictivos y terroristas.

33. Se alienta a los Estados a que refuercen y sigan desarrollando mecanismos que puedan facilitar los intercambios de información y asistencia entre las organizaciones nacionales, regionales e internacionales pertinentes con el fin de aumentar la

conciencia sobre la seguridad de las TIC entre los Estados y reducir el espacio operativo de las actividades terroristas y delictivas en línea. Estos mecanismos pueden fortalecer la capacidad de las organizaciones y organismos pertinentes, al tiempo que fomentan la confianza entre los Estados y refuerzan el comportamiento responsable de estos. También se alienta a los Estados a que desarrollen protocolos y procedimientos apropiados para recopilar, manejar y almacenar las pruebas en línea relevantes para la utilización de las TIC con fines delictivos y terroristas y a que proporcionen asistencia para las investigaciones de manera oportuna, garantizando que dichas acciones se lleven a cabo de conformidad con las obligaciones del Estado en virtud del derecho internacional.

34. En el seno de las Naciones Unidas, varios foros, procesos y resoluciones específicos abordan las amenazas que plantea la utilización de las TIC con fines terroristas y delictivos y los enfoques cooperativos necesarios para hacer frente a esas amenazas. Entre las resoluciones pertinentes de la Asamblea General destacan la resolución 65/230 sobre el 12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, por la que se estableció un grupo intergubernamental de expertos de composición abierta para que realizara un estudio exhaustivo del problema de la ciberdelincuencia; la resolución 74/173, relativa al fomento de la asistencia técnica y la creación de capacidad con el fin de fortalecer las medidas nacionales y la cooperación internacional para luchar contra la utilización de las TIC con fines delictivos, incluido el intercambio de información; y la resolución 74/247 sobre la lucha contra el uso de las TIC con fines delictivos.

35. Los Estados también pueden utilizar los procesos, iniciativas e instrumentos jurídicos existentes y considerar otros procedimientos o cauces de comunicación para facilitar el intercambio de información y asistencia a fin de hacer frente a la utilización de las TIC con fines delictivos y terroristas. A este respecto, se alienta a los Estados a que sigan reforzando las iniciativas en curso en las Naciones Unidas y a nivel regional para responder a la utilización de Internet y las TIC con fines delictivos y terroristas, y a que, con tal fin, desarrollen asociaciones de cooperación con organizaciones internacionales, actores económicos, el mundo académico y la sociedad civil.

Norma 13 e). Para garantizar la utilización segura de las TIC, los Estados deben 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.

36. Esta norma recuerda a los Estados que deben respetar y proteger los derechos humanos y las libertades fundamentales, tanto en línea como fuera de ella, de acuerdo con sus respectivas obligaciones. A este respecto, requieren especial atención el derecho a la libertad de expresión, incluido el derecho a buscar, recibir y difundir información sin limitación de fronteras y por cualquier medio de expresión, y otras disposiciones pertinentes previstas en el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, y contempladas en la Declaración Universal de Derechos Humanos. El cumplimiento de esta norma también puede contribuir a promover la no discriminación y a reducir la brecha digital, en particular en los que respecta al género.

37. La aprobación de las resoluciones a las que se refiere esta norma y otras que se han aprobado desde entonces es un reconocimiento de los nuevos retos y dilemas que han surgido en torno al uso de las TIC por los Estados y la correspondiente necesidad de abordarlos. Prácticas estatales como la vigilancia masiva arbitraria o ilegal pueden

tener efectos especialmente negativos en el ejercicio y el disfrute de los derechos humanos, en particular del derecho a la privacidad.

38. Al aplicar esta norma, los Estados deben tener en cuenta las orientaciones específicas contenidas en las resoluciones citadas. También deben tomar nota de las nuevas resoluciones aprobadas desde el informe de 2015 del Grupo de Expertos Gubernamentales y contribuir a las nuevas resoluciones que tal vez sea necesario proponer a la luz de los acontecimientos en curso.

39. Los esfuerzos de los Estados para promover el respeto y la observancia los derechos humanos y garantizar el uso responsable y seguro de las TIC deben ser complementarios, reforzarse mutuamente y ser interdependientes. Este enfoque promueve un entorno de las TIC abierto, seguro, estable, accesible y pacífico. También puede contribuir a la consecución de los Objetivos de Desarrollo Sostenible.

40. Aunque se reconoce la importancia de la innovación tecnológica para todos los Estados, las tecnologías nuevas y emergentes también pueden tener importantes consecuencias para los derechos humanos y la seguridad de las TIC. Para abordar esta cuestión, los Estados pueden considerar la posibilidad de promover e invertir en medidas técnicas y jurídicas a fin de orientar el desarrollo y el uso de las TIC de una manera más inclusiva y accesible y que no afecte negativamente a los miembros de comunidades o grupos individuales.

41. El Grupo observa que en el seno de las Naciones Unidas hay varios foros que se dedican específicamente a cuestiones de derechos humanos. Además, reconoce que diversas partes interesadas contribuyen de distintas maneras a la protección y promoción de los derechos humanos y las libertades fundamentales en línea y fuera de ella. La participación de estas voces en los procesos de elaboración de políticas relacionadas con la seguridad de las TIC puede servir de apoyo a los esfuerzos de promoción, protección y disfrute de los derechos humanos en línea y contribuir a aclarar y minimizar los posibles efectos negativos de las políticas en las personas, incluidas las que se encuentran en situaciones vulnerables.

Norma 13 f). Los Estados no deben realizar ni apoyar a sabiendas actividades de las TIC contrarias a las obligaciones que les incumben en virtud del derecho internacional que perjudiquen intencionadamente las infraestructuras críticas o dificulten de otro modo la utilización y funcionamiento de esas infraestructuras para prestar servicios al público.

42. En relación con esta norma, la actividad de las TIC que intencionadamente causa un perjuicio a las infraestructuras críticas o dificulta de otro modo su utilización y funcionamiento para prestar servicios al público puede tener efectos en cascada a nivel nacional, regional y mundial. Supone un elevado riesgo de daños para la población y puede dar lugar a escaladas susceptibles de desembocar en un conflicto.

43. La norma también señala la importancia fundamental de las infraestructuras críticas como activo nacional, ya que estas infraestructuras constituyen la columna vertebral de las funciones, servicios y actividades vitales de cualquier sociedad. Si estas se vieran significativamente dañadas o perjudicadas, los costos humanos y los efectos en la economía, el desarrollo, el funcionamiento político y social y la seguridad nacional del Estado podrían ser sustanciales.

44. Como se indica en la norma 13 g), los Estados deben tomar medidas apropiadas para proteger sus infraestructuras críticas. A este respecto, cada Estado determina qué infraestructuras o sectores considera críticos dentro de su jurisdicción, de conformidad con las prioridades nacionales y los métodos de categorización de las infraestructuras críticas.

45. La pandemia de COVID-19 hizo que se tomara más conciencia de la importancia crítica de proteger las infraestructuras e instalaciones sanitarias y médicas, incluso mediante la aplicación de las normas relativas a las infraestructuras críticas (como esta norma y las normas g) y h)). Otros ejemplos de sectores de infraestructuras críticas que prestan servicios esenciales al público son la energía, la generación de electricidad, el agua y el saneamiento, la educación, los servicios comerciales y financieros, el transporte, las telecomunicaciones y los procesos electorales. Las infraestructuras críticas también pueden referirse a las infraestructuras que prestan servicios a varios Estados, como la infraestructura técnica esencial para la integridad o disponibilidad general de Internet. Estas infraestructuras pueden ser críticas para el comercio internacional, los mercados financieros, el transporte mundial, las comunicaciones, la sanidad o la acción humanitaria. El hecho de que estas infraestructuras se citen como ejemplos no excluye en absoluto que los Estados designen como críticas otras infraestructuras, ni aprueba las actividades malintencionadas contra las categorías de infraestructuras no mencionadas anteriormente.

46. Para apoyar la aplicación de la norma, además de tener en cuenta los factores señalados con anterioridad, se alienta a los Estados a que establezcan las medidas políticas y legislativas pertinentes a nivel nacional para garantizar que las actividades de TIC realizadas o apoyadas por un Estado que puedan afectar a las infraestructuras críticas de otro Estado o a la prestación de servicios públicos esenciales en él se ajusten a esta norma, se lleven a cabo de conformidad con sus obligaciones jurídicas internacionales y estén sujetas a una revisión y supervisión exhaustivas.

Norma 13 g). Los Estados deben tomar medidas apropiadas para proteger sus infraestructuras críticas frente a amenazas relacionadas con las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General.

47. Esta norma reafirma el compromiso de todos los Estados de proteger las infraestructuras críticas bajo su jurisdicción de las amenazas relacionadas con las TIC y la importancia de la cooperación internacional en este sentido.

48. La designación de una infraestructura o un sector como crítico por un Estado puede ser útil para proteger dicha infraestructura o sector. Además de determinar las infraestructuras o sectores de infraestructura que considera críticos, cada Estado determina las medidas estructurales, técnicas, organizativas, legislativas y reglamentarias necesarias para proteger sus infraestructuras críticas y restablecer su funcionamiento si se produce un incidente. La resolución 58/199 de la Asamblea General relativa a la creación de una cultura mundial de seguridad cibernética y la protección de las infraestructuras de información esenciales y el anexo que la acompaña[3] destacan las medidas que los Estados pueden adoptar a nivel nacional con ese fin.

49. Algunos Estados albergan infraestructuras que prestan servicios a nivel regional o internacional. Las amenazas relacionadas con las TIC a esas infraestructuras podrían tener efectos desestabilizadores. Los Estados que participan en estos acuerdos podrían fomentar la cooperación transfronteriza con los propietarios y operadores de las infraestructuras pertinentes para mejorar las medidas de seguridad de las TIC que se aplican a dichas infraestructuras y reforzar los procesos y procedimientos existentes o desarrollar otros complementarios a fin de detectar y mitigar los incidentes relacionados con las TIC que afecten a dichas infraestructuras.

[3] A/RES/58/199, que forma parte de un conjunto de tres resoluciones de la Asamblea General que incluye también las resoluciones A/RES/57/239 y A/RES/64/211.

50. El fomento de medidas que garanticen la seguridad y la protección de los productos de las TIC a lo largo de su ciclo de vida o la clasificación de los incidentes relacionados con las TIC en función de su escala y gravedad también contribuiría a lograr el objetivo de esta norma.

Norma 13 h). Los Estados deben atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras críticas sean objeto de actos malintencionados relacionados con las TIC. Los Estados también deben atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio que se dirija contra infraestructuras críticas de otro Estado, teniendo debidamente en cuenta la soberanía.

51. Esta norma recuerda a los Estados que la cooperación internacional, el diálogo y el debido respeto a la soberanía de todos los Estados son fundamentales para atender las solicitudes de asistencia de otro Estado cuyas infraestructuras críticas sean objeto de actos malintencionados relacionados con las TIC. La norma es especialmente importante cuando se trata de actos que pueden amenazar la paz y la seguridad internacionales.

52. Al recibir una solicitud de asistencia, los Estados deben ofrecer cualquier asistencia que su capacidad y recursos le permitan proporcionar, que esté razonablemente disponible y que sea factible teniendo en cuenta las circunstancias. Un Estado puede optar por recabar asistencia de forma bilateral o a través de acuerdos regionales o internacionales. Los Estados también pueden solicitar los servicios del sector privado para ayudar a responder a las solicitudes de asistencia.

53. Disponer de las estructuras y mecanismos nacionales necesarios para detectar y mitigar los incidentes relacionados con las TIC que puedan amenazar la paz y la seguridad internacionales permite la aplicación efectiva de esta norma. Esos mecanismos complementan los dispositivos existentes para la gestión y resolución diarias de los incidentes relacionados con las TIC. Por ejemplo, a un Estado que desee solicitar la asistencia de otro Estado le puede resultar útil saber a quién dirigirse y el canal de comunicación adecuado que debe utilizar. El Estado que recibe una solicitud de asistencia debe determinar, de la manera más transparente y oportuna posible y respetando la urgencia y la sensibilidad de la solicitud, si tiene la capacidad, la aptitud y los recursos necesarios para prestar la asistencia solicitada. No se espera que los Estados a los que se solicita asistencia garanticen un resultado o un efecto concreto.

54. La existencia de procesos y procedimientos comunes y transparentes para solicitar asistencia a otro Estado y para responder a las solicitudes de asistencia puede facilitar la cooperación que se describe en la norma. A este respecto, la utilización de plantillas comunes para solicitar asistencia y responder a tales solicitudes puede garantizar que el Estado que solicita la asistencia proporcione la información más completa y precisa posible al Estado cuya asistencia solicita, facilitando así la cooperación y la puntualidad de la respuesta. Esas plantillas podrían desarrollarse voluntariamente a nivel bilateral, multilateral o regional. Una plantilla común para responder a las solicitudes de asistencia podría incluir elementos que permitan acusar recibo de la solicitud y, si la asistencia es posible, una indicación del plazo, la naturaleza, el alcance y las condiciones de la asistencia que podría prestarse.

55. Cuando la actividad malintencionada se origina en el territorio de un Estado concreto, su ofrecimiento de proporcionar la asistencia solicitada y la prestación de dicha asistencia pueden contribuir a minimizar los daños, evitar percepciones erróneas, reducir el riesgo de escalada y facilitar el restablecimiento de la confianza. La participación en mecanismos de cooperación que definan los medios y el modo de

las comunicaciones en casos de crisis y de la gestión y resolución de los incidentes puede reforzar la observancia de esta norma.

Norma 13 i). Los Estados deben adoptar medidas razonables para garantizar la integridad de la cadena de suministro, de modo que los usuarios finales puedan confiar en la seguridad de los productos de las TIC. Los Estados deben tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC, así como el uso de funciones ocultas perniciosas.

56. Esta norma reconoce la necesidad de promover la confianza del usuario final en un entorno de las TIC abierto, seguro, estable, accesible y pacífico. Garantizar la integridad de la cadena de suministro de las TIC y la seguridad de los productos relacionados con esas tecnologías y evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC y el uso de funciones ocultas perniciosas son cuestiones cada vez más importante para esos fines, así como para la seguridad internacional y el desarrollo digital y económico en un sentido más amplio.

57. Las cadenas mundiales de suministro de las TIC son amplias y cada vez más complejas e interdependientes, e implican a una diversidad de partes. Entre las medidas razonables para promover la apertura y garantizar la integridad, la estabilidad y la seguridad de la cadena de suministro pueden mencionarse las siguientes:

a) Poner en marcha a nivel nacional marcos y mecanismos integrales, transparentes, objetivos e imparciales para la gestión del riesgo en la cadena de suministro, en consonancia con las obligaciones internacionales del Estado. Estos marcos pueden incluir evaluaciones de riesgo que tengan en cuenta una serie de factores, incluidos los beneficios y riesgos de las nuevas tecnologías.

b) Establecer políticas y programas para promover objetivamente la adopción de buenas prácticas por parte de los proveedores y vendedores de equipos y sistemas de TIC, con el fin de fomentar la confianza internacional en la integridad y seguridad de los productos y servicios de TIC, mejorar la calidad y promover la elección.

c) Prestar una mayor atención en el ámbito de la política nacional y en el diálogo con los Estados y los actores pertinentes en el marco de las Naciones Unidas y otros foros al modo de garantizar que todos los Estados puedan competir e innovar en igualdad de condiciones, a fin de permitir la plena realización del potencial de las TIC para aumentar el desarrollo social y económico mundial y contribuir al mantenimiento de la paz y la seguridad internacionales, al tiempo que también se salvaguarda la seguridad nacional y el interés público.

d) Introducir medidas de cooperación como el intercambio de buenas prácticas a nivel bilateral, regional y multilateral sobre la gestión del riesgo en la cadena de suministro; el desarrollo y la aplicación de reglas y normas comunes interoperables a nivel mundial para la seguridad de la cadena de suministro; y otros enfoques destinados a disminuir las vulnerabilidades de la cadena de suministro.

58. Para evitar el desarrollo y la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC y el uso de funciones ocultas perniciosas, como las puertas traseras, los Estados pueden considerar la posibilidad de establecer a nivel nacional:

a) Medidas para mejorar la integridad de la cadena de suministro, incluso exigiendo a los proveedores de TIC que incorporen la seguridad y la protección en el diseño, el desarrollo y todo el ciclo de vida de los productos de TIC. Para ello, los Estados también pueden considerar la posibilidad de establecer procesos de certificación independientes e imparciales.

b) Salvaguardias legislativas y de otro tipo que mejoren la protección de los datos y la privacidad.

c) Medidas que prohíban la introducción de funciones ocultas perniciosas y la explotación de vulnerabilidades en los productos de las TIC que puedan poner en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas y las redes, incluso en las infraestructuras críticas.

59. Además de las iniciativas y medidas señaladas anteriormente, los Estados deben seguir alentando al sector privado y a la sociedad civil a que desempeñen un papel adecuado para mejorar la seguridad y el uso de las TIC, incluida la seguridad de la cadena de suministro de los productos de esas tecnologías, y contribuir así a cumplir los objetivos de esta norma.

Norma 13 j). Los Estados deben alentar la divulgación responsable de información sobre las vulnerabilidades relacionadas con las TIC y compartir la información sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o las infraestructuras que dependen de ellas.

60. Esta norma recuerda a los Estados la importancia de garantizar que las vulnerabilidades relacionadas con las TIC se aborden rápidamente para reducir la posibilidad de que sean explotadas por actores malintencionados. La detección oportuna y la divulgación y comunicación responsables de las vulnerabilidades relacionadas con las TIC pueden evitar prácticas perjudiciales o amenazadoras, aumentar la confianza y reducir las amenazas relativas a la seguridad y la estabilidad internacionales.

61. Las políticas y programas de divulgación de las vulnerabilidades, así como la cooperación internacional conexa, tienen como objetivo ofrecer un proceso fiable y coherente para convertir esa divulgación en una práctica rutinaria. Un proceso coordinado de divulgación de vulnerabilidades puede minimizar el daño que los productos vulnerables suponen para la sociedad y sistematizar la notificación de vulnerabilidades relacionadas con las TIC y las solicitudes de asistencia entre los países y los equipos de respuesta a emergencias. Estos procesos deben ser coherentes con la legislación nacional.

62. A nivel nacional, regional e internacional, los Estados podrían considerar la posibilidad de establecer marcos jurídicos, políticas y programas imparciales para orientar la toma de decisiones sobre el tratamiento de las vulnerabilidades relacionadas con las TIC y limitar su distribución comercial como medio de protección contra cualquier uso indebido que pueda suponer un riesgo para la paz y la seguridad internacionales o los derechos humanos y las libertades fundamentales. Los Estados también podrían considerar la posibilidad de establecer protecciones jurídicas para los investigadores y los expertos en pruebas de intrusión.

63. Además, y en consulta con el sector económico pertinente y otros actores de la seguridad de las TIC, los Estados pueden desarrollar orientaciones e incentivos, en consonancia con las normas técnicas internacionales pertinentes, sobre la notificación y gestión responsables de las vulnerabilidades y las funciones y responsabilidades respectivas de las distintas partes interesadas en los procesos de notificación; los tipos de información técnica que deben divulgarse o compartirse públicamente, incluido el intercambio de información técnica sobre incidentes relacionados con las TIC que sean graves; y el modo de manejar los datos sensibles y garantizar la seguridad y confidencialidad de la información.

64. Las recomendaciones sobre el fomento de la confianza y la cooperación internacional en materia de asistencia y creación de capacidad de anteriores Grupos

de Expertos Gubernamentales pueden ser especialmente útiles para desarrollar una interpretación compartida de los mecanismos y procesos que los Estados pueden poner en marcha para la divulgación responsable de vulnerabilidades. Los Estados pueden considerar la posibilidad de utilizar los organismos multilaterales, regionales y subregionales existentes y otros cauces y plataformas pertinentes en los que participen distintas partes interesadas con este fin.

Norma 13 k). Los Estados no deben realizar ni apoyar a sabiendas actividades que perjudiquen los sistemas de información de los equipos de respuesta de emergencia autorizados (a veces conocidos como equipos de respuesta a emergencias informáticas o equipos de respuesta a incidentes de ciberseguridad) de otro Estado. Un Estado no debe utilizar equipos de respuesta de emergencia autorizados para realizar actividades malintencionadas a nivel internacional.

65. Esta norma refleja el hecho de que los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad u otros órganos de respuesta autorizados tienen responsabilidades y funciones únicas en la gestión y resolución de los incidentes relacionados con las TIC, y por lo tanto desempeñan un papel importante en el mantenimiento de la paz y la seguridad internacionales. Son esenciales para detectar y mitigar eficazmente los efectos negativos inmediatos y a largo plazo de los incidentes relacionados con las TIC. Los daños causados a los equipos de respuesta de emergencia pueden socavar la confianza y mermar su capacidad para desempeñar sus funciones, y pueden tener consecuencias más amplias, a menudo imprevistas, en todos los sectores y potencialmente en la paz y la seguridad internacionales. El Grupo subraya la importancia de evitar la politización de los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad y de respetar el carácter independiente de sus funciones.

66. En reconocimiento de su papel esencial en la protección de la seguridad nacional y del público y en la prevención de pérdidas económicas derivadas de incidentes relacionados con las TIC, muchos Estados categorizan a los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad como parte de sus infraestructuras críticas.

67. Al considerar cómo pueden contribuir a la paz y la seguridad internacionales sus actividades en relación con los equipos de respuesta de emergencia, los Estados podrían declarar públicamente o establecer medidas que afirmen que no utilizarán los equipos de respuesta de emergencia autorizados para realizar actividades internacionales malintencionadas, y reconocer y respetar los ámbitos de operación y los principios éticos que orientan la labor de los equipos de respuesta de emergencia autorizados. El Grupo toma nota de las nuevas iniciativas en este sentido.

68. Los Estados también podrían considerar la posibilidad de adoptar otras medidas, como el establecimiento de un marco nacional de gestión de incidentes de seguridad de las TIC con funciones y responsabilidades específicas, incluso para los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad, para facilitar la cooperación y coordinación entre esos equipos y otros organismos técnicos y de seguridad pertinentes a nivel nacional, regional e internacional. Dicho marco puede incluir la elaboración de políticas, medidas reguladoras o procedimientos que aclaren el estatus, la autoridad y los mandatos de los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad y que distingan las funciones únicas de esos equipos de otras funciones gubernamentales.

IV. Derecho internacional

69. El derecho internacional es la base del compromiso compartido por los Estados de prevenir conflictos y mantener la paz y la seguridad internacionales y es clave para aumentar la confianza entre los Estados. En su examen del modo en que el derecho internacional se aplica al uso de las TIC por parte de los Estados, el Grupo reafirma las evaluaciones y recomendaciones sobre derecho internacional que figuran en los informes de anteriores Grupos de Expertos Gubernamentales, en particular que el derecho internacional, y en concreto la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y para promover un entorno de las TIC abierto, seguro, estable, accesible y pacífico. Estas evaluaciones y recomendaciones, junto con otros elementos sustantivos de informes anteriores, ponen de relieve que la adhesión de los Estados al derecho internacional, en particular a las obligaciones que les impone la Carta, es un marco esencial para su actuación en el uso de las TIC.

70. A este respecto, el Grupo reafirmó los compromisos de los Estados con los siguientes principios de la Carta y otras normas de derecho internacional: la igualdad soberana; la solución de controversias internacionales por medios pacíficos de manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia; la abstención de recurrir, en sus 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 Estados.

71. Sumándose a la labor de los anteriores Grupos de Expertos Gubernamentales y guiado por la Carta y el mandato contenido en la resolución 73/266, el presente Grupo ofrece una reflexión adicional destinada a facilitar la comprensión de las evaluaciones y recomendaciones del informe del Grupo de Expertos Gubernamentales de 2015 sobre el modo en que el derecho internacional se aplica al uso de las TIC por los Estados, en los términos siguientes:

a) El Grupo observa que, de acuerdo con las obligaciones que les incumben en virtud del Artículo 2, apartado 3, y el Capítulo VI de la Carta de las Naciones Unidas, los Estados partes en una controversia internacional, incluidas las relativas al uso de las TIC, cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales deben tratar de buscarle solución, ante todo, por los medios que se enumeran en el Artículo 33 de la Carta, es decir, la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección. El Grupo también señala la importancia de otras disposiciones de la Carta relativas a la solución de controversias por medios pacíficos.

b) El Grupo reafirma que la soberanía de los Estados y las normas y principios internacionales que de ella dimanan son aplicables a la realización por los Estados de actividades relacionadas con las TIC y a su jurisdicción sobre la infraestructura relativa a esas tecnologías que se halle en su territorio. Las obligaciones existentes en virtud del derecho internacional son aplicables a la actividad de los Estados relacionada con las TIC. Los Estados ejercen su jurisdicción sobre la infraestructura de las TIC situada en su territorio, entre otras cosas, estableciendo las políticas y la legislación y creando los mecanismos necesarios para proteger la infraestructura relativa a esas tecnologías ubicada en su territorio de las amenazas relacionadas con las TIC.

c) De conformidad con el principio de no intervención, los Estados no deben intervenir directa o indirectamente en los asuntos internos de otro Estado, incluso por medio de las TIC.

d) En su uso de las TIC, y según se desprende de la Carta de las Naciones Unidas, los Estados deben abstenerse de recurrir, en sus 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.

e) Subrayando las aspiraciones de la comunidad internacional de que las TIC se utilicen pacíficamente para el bien común de la humanidad, y recordando que la Carta se aplica en su totalidad, el Grupo observa de nuevo el derecho inherente de los Estados a adoptar medidas compatibles con el derecho internacional y reconocidas en la Carta, así como la necesidad de seguir estudiando esta cuestión.

f) El Grupo observa que el derecho internacional humanitario solo se aplica en situaciones de conflicto armado. En este sentido, recuerda los principios jurídicos internacionales establecidos, incluidos, en su caso, los principios de humanidad, necesidad, proporcionalidad y distinción que se señalaron en el informe de 2015. El Grupo reconoce la necesidad de seguir estudiando cómo y cuándo se aplican estos principios al uso de las TIC por parte de los Estados y subraya que recordar estos principios no legitima ni fomenta en absoluto los conflictos.

g) El Grupo reafirma que los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional. También reafirma que los Estados no deben recurrir a terceros para cometer hechos internacionalmente ilícitos utilizando las TIC, y deben tratar de garantizar que su territorio no sea utilizado por actores no estatales para realizar esos hechos. Al mismo tiempo, el Grupo recuerda que el indicio de que una actividad de TIC se ha iniciado o tiene su origen en el territorio o la infraestructura de TIC de un Estado puede ser insuficiente por sí solo para atribuir la actividad a ese Estado, y observa que las acusaciones de organizar y llevar a cabo hechos ilícitos formuladas contra los Estados deben fundamentarse. La invocación de la responsabilidad del Estado por un hecho internacionalmente ilícito implica consideraciones técnicas, jurídicas y políticas complejas.

72. Sin perjuicio del derecho internacional vigente y de que el derecho internacional siga desarrollándose en el futuro, el Grupo reconoció que la continuación de los debates e intercambios de opiniones por parte de los Estados de forma colectiva en las Naciones Unidas sobre el modo en que las normas y principios específicos del derecho internacional se aplican al uso de las TIC por los Estados es esencial para profundizar en los entendimientos comunes, evitar malentendidos y aumentar la previsibilidad y la estabilidad. Tales debates pueden fundamentarse y apoyarse mediante el intercambio de opiniones entre los Estados a nivel regional y bilateral.

73. De acuerdo con el mandato del Grupo, se publicará en el sitio web de la Oficina de Asuntos de Desarme de las Naciones Unidas un compendio oficial (A/76/136) de las contribuciones nacionales voluntarias de los expertos gubernamentales participantes sobre la cuestión de cómo se aplica el derecho internacional al uso de las TIC por los Estados. El Grupo alienta a todos los Estados a que sigan compartiendo voluntariamente sus opiniones y evaluaciones nacionales por conducto del Secretario General de las Naciones Unidas y por otras vías, según proceda.

V. Medidas de fomento de la confianza

74. El Grupo observa que, al fomentar la confianza, la cooperación, la transparencia y la previsibilidad, las medidas de fomento de la confianza pueden promover la estabilidad y contribuir a reducir el riesgo de malentendidos, escaladas y conflictos. El fomento de la confianza es un compromiso progresivo y a largo plazo que requiere

la determinación sostenida de los Estados. El apoyo de las Naciones Unidas, los órganos regionales y subregionales y otras partes interesadas puede contribuir a la puesta en práctica efectiva y el fortalecimiento de las medidas de fomento de la confianza.

75. A fin de respaldar sus esfuerzos por fomentar la confianza y garantizar un entorno de las TIC que sea pacífico, se alienta a los Estados a que reiteren públicamente su compromiso con el marco para el comportamiento responsable de los Estados mencionado en el párrafo 2 y a que actúen de acuerdo con él. También se alienta a los Estados a que tomen en consideración las Directrices para las Medidas de Fomento de la Confianza adoptadas por la Comisión de Desarme de las Naciones Unidas en 1988 y aprobadas por consenso por la Asamblea General en la resolución 43/78 H, así como las prácticas emergentes a nivel regional y subregional pertinentes para las medidas de fomento de la confianza y su puesta en marcha.

Medidas de cooperación

Puntos de contacto

76. La identificación de puntos de contacto apropiados a nivel técnico y de políticas puede facilitar las comunicaciones seguras y directas entre los Estados para contribuir a prevenir y abordar los incidentes graves relacionados con las TIC y rebajar las tensiones en situaciones de crisis. La comunicación entre los puntos de contacto puede ayudar a reducir las tensiones y evitar los malentendidos y las percepciones erróneas que pueden derivarse de los incidentes relacionados con las TIC, incluidos los que afectan a las infraestructuras críticas y los que tienen repercusiones nacionales, regionales o mundiales. También pueden aumentar el intercambio de información y permitir que los Estados gestionen y resuelvan más eficazmente los incidentes relacionados con las TIC.

77. A la hora de establecer puntos de contacto o participar en redes de puntos de contacto, los Estados podrían considerar la posibilidad de:

a) Nombrar puntos de contacto específicos a nivel diplomático, técnico y de políticas y ofrecer orientación sobre las características concretas de los puntos de contacto, incluidas las funciones y responsabilidades previstas, las funciones de coordinación y los requisitos de preparación.

b) Crear procedimientos inter e intragubernamentales para garantizar una comunicación eficaz entre los puntos de contacto durante las crisis. Las plantillas estandarizadas pueden indicar los tipos de información requeridos, incluidos los datos técnicos y la naturaleza de la solicitud, pero deben ser lo suficientemente flexibles para permitir la comunicación, incluso si hay alguna información que no esté disponible.

c) Extraer enseñanzas y buenas prácticas de las redes regionales de puntos de contacto, incluso en lo que respecta a debatir, desarrollar y aplicar enfoques prácticos para utilizar las redes de puntos de contacto en contextos nacionales, regionales e internacionales, en particular para el conocimiento temprano de incidentes graves relacionados con las TIC, con el objetivo de reforzar la coordinación y el intercambio de información entre los puntos de contacto designados.

78. Para hacer frente a las amenazas globales a la seguridad de las TIC también se necesitan enfoques globales que sean inclusivos y universales. Los Estados podrían invitar al Secretario General de las Naciones Unidas a que facilitara los intercambios voluntarios entre todos los Estados Miembros sobre las enseñanzas, las buenas prácticas y las orientaciones pertinentes para las redes de puntos de contacto que ya existen a nivel regional y subregional. Esa labor podría contribuir a mantener debates

pertinentes para el establecimiento de un directorio de tales puntos de contacto a nivel mundial.

Diálogo y consultas

79. El diálogo a través de consultas e intercambios bilaterales, subregionales, regionales y multilaterales puede hacer avanzar el entendimiento entre los Estados, fomentar una mayor confianza y contribuir a una cooperación interestatal más estrecha a la hora de mitigar los incidentes relacionados con las TIC, reduciendo al mismo tiempo los riesgos de percepción errónea y de escalada. Otras partes interesadas, como el sector privado, el mundo académico, la sociedad civil y la comunidad técnica, pueden contribuir de manera significativa a facilitar esas consultas e intercambios.

80. Los organismos regionales han tomado medidas importantes para elaborar y aplicar medidas de fomento de la confianza que permitan reducir los riesgos de percepción errónea, escalada y conflicto que pueden derivarse de los incidentes relacionados con las TIC. La participación en estas agrupaciones permite centrarse en las características y preocupaciones regionales, mientras que los intercambios interregionales facilitan el aprendizaje mutuo entre dichas organizaciones. Se alienta a los Estados a que continúen esta labor y a que interactúen de forma activa con los Estados que actualmente no pertenecen a ninguna organización regional o subregional pertinente.

81. A fin de seguir reforzando las medidas de cooperación pertinentes para los equipos nacionales de respuesta a emergencias informáticas y otros organismos autorizados, los Estados podrían fomentar el intercambio y la difusión de información y buenas prácticas sobre el establecimiento y mantenimiento de equipos de respuesta a emergencias informáticas y equipos de respuesta a incidentes de ciberseguridad de alcance nacional y sobre la gestión de incidentes a través de las organizaciones y redes de respuesta de emergencia a nivel regional y mundial ya existentes. Este estímulo y apoyo a los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad también serviría para concienciar a los Estados de sus compromisos en relación con esos equipos y otros organismos conexos en virtud de la norma 13 k).

Medidas de transparencia

82. Asegurar la transparencia de forma voluntaria mediante el intercambio de opiniones y prácticas nacionales sobre los incidentes de seguridad relacionados con las TIC y otras amenazas conexas, y poniendo a disposición del público el asesoramiento, las orientaciones, la base empírica y los datos de apoyo de las decisiones en materia de seguridad de las TIC es importante para fomentar la confianza y la previsibilidad, reducir las posibilidades de interpretación errónea y de escalada y ayudar a las organizaciones y organismos a tomar decisiones correctas en materia de gestión de riesgos.

83. Para seguir avanzando en la transparencia y la previsibilidad del comportamiento de los Estados, dar a conocer una gama más amplia de puntos de vista y experiencias y mejorar la preparación de los Estados y el conocimiento temprano de las amenazas crecientes, los Estados podrían considerar la posibilidad de utilizar los foros bilaterales, subregionales, regionales y multilaterales y las consultas oficiosas para compartir voluntariamente información y buenas prácticas, enseñanzas o libros blancos sobre las amenazas y los incidentes actuales y emergentes relacionados con la seguridad de las TIC; estrategias y normas nacionales para el análisis de la vulnerabilidad de los productos de las TIC; y enfoques nacionales y regionales sobre la gestión de riesgos y la prevención de conflictos, incluidos

enfoques nacionales para la clasificación de los incidentes relacionados con las TIC en función de su escala y gravedad.

84. Los Estados también pueden aprovechar los foros existentes para aclarar posiciones e intercambiar voluntariamente información sobre los enfoques nacionales de la seguridad de las TIC; la protección de los datos; la protección de las infraestructuras críticas basadas en las TIC; y la misión y las funciones de los organismos de seguridad de las TIC, y la estrategia de las TIC a nivel nacional u organizativo, así como los regímenes jurídicos y de supervisión bajo los que operan.

85. Las recomendaciones sobre las medidas de fomento de la confianza incluidas en informes anteriores del Grupo de Expertos Gubernamentales proporcionan una base de cooperación para hacer frente a las crecientes amenazas relativas a los retos relacionados con las infraestructuras críticas y para aplicar las normas pertinentes. Se alienta a los Estados a que sigan creando conciencia sobre la importancia de la protección de las infraestructuras críticas, promoviendo el intercambio de información entre las partes interesadas en esas infraestructuras y compartiendo buenas prácticas y orientaciones. En su caso, pueden utilizar las plataformas y modalidades de notificación existentes (véase el párrafo 86) para compartir voluntariamente las opiniones nacionales sobre la clasificación de las infraestructuras nacionales críticas y de las infraestructuras críticas que prestan servicios esenciales a nivel regional o internacional, las políticas y la legislación nacionales pertinentes, y los marcos para la evaluación de riesgos y para la identificación, clasificación y gestión de los incidentes relacionados con las TIC que afectan a las infraestructuras críticas.

86. Los Estados también podrían utilizar los recursos de las Naciones Unidas, como la presentación voluntaria de información al Secretario General y el Cyber Policy Portal del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR), así como los recursos de otras organizaciones internacionales y regionales pertinentes, para consolidar la información y las buenas prácticas proporcionadas voluntariamente por los Estados sobre las estrategias, políticas, legislación y programas nacionales que abordan cuestiones de seguridad de las TIC pertinentes para la seguridad y la estabilidad internacionales.

VI. Cooperación y asistencia internacionales en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones y la creación de capacidad

87. El Grupo recalca la importancia de la cooperación y la asistencia en el ámbito de la seguridad de las TIC y la creación de capacidad, así como su relevancia para todos los elementos del mandato del Grupo. El aumento de la cooperación, junto con actividades más eficaces en materia de asistencia y creación de capacidad en la esfera de la seguridad de las TIC con la participación de otras partes interesadas, como el sector privado, el mundo académico, la sociedad civil y la comunidad técnica, puede ayudar a los Estados a aplicar el marco para un comportamiento responsable de estos en su uso de las TIC. Tales esfuerzos son esenciales para salvar las diferencias existentes dentro de los Estados y entre ellos sobre cuestiones jurídicas, técnicas y de política relacionadas con la seguridad de las TIC. También pueden contribuir a cumplir otros objetivos de la comunidad internacional, como los Objetivos de Desarrollo Sostenible.

88. La cooperación y la asistencia internacionales en el ámbito de la seguridad de las TIC y la creación de capacidad pueden reforzar la capacidad de los Estados para detectar, investigar y responder a las amenazas y garantizar que todos los Estados

tengan la capacidad de actuar de forma responsable en su uso de las TIC. También pueden contribuir a garantizar que todos los Estados alcancen los niveles necesarios de protección y seguridad de las infraestructuras críticas, dispongan de capacidades adecuadas de gestión de incidentes, y puedan solicitar asistencia, o responder a peticiones al respecto, en caso de actividades malintencionadas relacionadas con las TIC que se originen en su territorio o lo afecten.

89. El Grupo recomienda que se siga reforzando la cooperación y la asistencia internacionales en el ámbito de la seguridad de las TIC y la creación de capacidad para apoyar a los Estados en los siguientes ámbitos:

a) Elaborar y aplicar políticas, estrategias y programas relacionados con las TIC a nivel nacional.

b) Crear y mejorar la capacidad de los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad y fortalecer los acuerdos de cooperación entre esos equipos.

c) Mejorar la seguridad, resiliencia y protección de las infraestructuras críticas.

d) Crear o mejorar las capacidades técnicas, jurídicas y de política de los Estados para detectar, investigar y resolver los incidentes relacionados con las TIC, en particular mediante la inversión en el desarrollo de recursos humanos, instituciones, tecnología resiliente y programas educativos.

e) Profundizar en la comprensión común de cómo se aplica el derecho internacional al uso de las TIC por los Estados y promover los intercambios entre los Estados, en particular mediante debates en las Naciones Unidas a este respecto.

f) Mejorar las capacidades técnicas y jurídicas de todos los Estados para investigar y resolver los incidentes graves relacionados con las TIC.

g) Aplicar normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados.

h) A tal fin, y como medio para evaluar sus propias prioridades, necesidades y recursos, se alienta a los Estados a que utilicen la Encuesta de Aplicación Nacional voluntaria recomendada por el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[4].

90. En aras de reducir las brechas digitales y garantizar que todos los Estados se beneficien de estas y otras esferas de asistencia y creación de capacidad, se alienta a los Estados a que, cuando sea posible, destinen a tales fines recursos financieros y conocimientos técnicos y en materia de políticas, y apoyen a los países que soliciten asistencia en sus esfuerzos por mejorar la seguridad de las TIC.

91. Al promover la cooperación y la asistencia internacionales en el ámbito de la seguridad de las TIC y la creación de capacidad, el Grupo recalca el carácter voluntario, políticamente neutral, mutuamente beneficioso y recíproco de la creación de capacidad. A este respecto, el Grupo valora positivamente los principios de creación de capacidad relativos al proceso, el propósito, las asociaciones y las personas recomendados por 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 y alienta a todos los Estados a que se guíen por estos principios en sus esfuerzos por promover la cooperación y la asistencia[5].

[4] Informe sustantivo final del Grupo de Trabajo de Composición Abierta, párr. 65.
[5] Informe sustantivo final del Grupo de Trabajo de Composición Abierta, párr. 56.

92. La promoción de un entendimiento común y el aprendizaje mutuo también pueden reforzar la cooperación y la asistencia internacionales en el ámbito de la seguridad de las TIC y la creación de capacidad. Los Estados deberían considerar la posibilidad de enfocar la cooperación en la esfera de la seguridad de las TIC y la creación de capacidad de manera que sea multidisciplinar, incorpore a múltiples partes interesadas, tenga carácter modular y sea mensurable. Esto puede lograrse colaborando con las Naciones Unidas y otros órganos mundiales, regionales y subregionales, junto con otras partes interesadas pertinentes, para facilitar la coordinación y aplicación eficaces de los programas de creación de capacidad y fomentando la transparencia y el intercambio de información sobre su eficacia.

VII. Conclusiones y recomendaciones para la labor futura

93. A medida que los Estados se vuelven cada vez más dependientes de las TIC, es esencial que se observe un marco común de comportamiento estatal responsable en el uso de las TIC en el contexto de la seguridad internacional para que todos los Estados se beneficien de las tecnologías, se protejan frente a su uso indebido y puedan responder ante él.

94. Centrando sus esfuerzos en la promoción de un entendimiento común y una aplicación efectiva, y basándose en las recomendaciones de informes anteriores, el Grupo determinó los enfoques que pueden adoptar los Estados y aportó mayor claridad y orientación al respecto a fin de garantizar que las medidas de cooperación hagan frente de manera efectiva a las amenazas existentes y potenciales en el ámbito de la seguridad de las TIC. Estos enfoques se describen claramente en las secciones del informe relativas a las normas, reglas y principios de comportamiento responsable de los Estados; el derecho internacional; el fomento de la confianza; y la cooperación internacional y la creación de capacidad, cada una de las cuales profundiza en los elementos esenciales del comportamiento responsable de los Estados que habían sido desarrollados en anteriores informes del Grupo de Expertos Gubernamentales.

95. El Grupo también determinó posibles áreas de actuación para la labor futura, que incluyen, entre otras, las siguientes:

a) Intensificar la cooperación a nivel bilateral, regional y multilateral para fomentar un entendimiento común sobre las amenazas actuales y emergentes y los posibles riesgos para la paz y la seguridad internacionales que plantea el uso malintencionado de las TIC y sobre la seguridad de las infraestructuras que posibilitan las TIC.

b) Seguir compartiendo e intercambiando opiniones sobre las normas, reglas y principios de comportamiento responsable de los Estados y las prácticas nacionales y regionales de aplicación de las normas y las medidas de fomento de la confianza, y sobre el modo en que se aplica el derecho internacional al uso de las TIC por los Estados, incluso designando temas de derecho internacional específicos para mantener más debates en profundidad.

c) Seguir reforzando la cooperación internacional y la creación de capacidad sobre las evaluaciones y recomendaciones del presente informe para garantizar que todos los Estados puedan contribuir al mantenimiento de la paz y la seguridad internacionales, teniendo en cuenta lo indicado en el párrafo 90.

d) Determinar mecanismos que faciliten la participación de otras partes interesadas esenciales, como el sector privado, el mundo académico, la sociedad civil y la comunidad técnica, en los esfuerzos por aplicar el marco de comportamiento responsable, cuando proceda.

e) Solicitar al UNIDIR, que está al servicio de todos los Estados Miembros, que realice estudios pertinentes sobre los temas tratados en el presente informe y alentar a otros grupos de reflexión e instituciones de investigación adecuados a que hagan lo propio.

96. El Grupo alienta a que continúe el proceso de negociación inclusivo y transparente sobre las TIC en el contexto de la seguridad internacional bajo los auspicios de las Naciones Unidas, incluyendo y reconociendo al Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), establecido en virtud de la resolución 75/240 de la Asamblea General. El grupo recomienda que la labor futura se base en los trabajos de los distintos Grupos de Expertos Gubernamentales y 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.

97. El Grupo alienta a los Estados a que sigan esforzándose por impulsar el marco de comportamiento responsable de los Estados en las Naciones Unidas y en otros foros regionales y multilaterales para apoyar actividades periódicas de diálogo, consulta y creación de capacidad que sean inclusivas y transparentes, estén impulsadas por el consenso y se orienten a la acción. A este respecto, y en consonancia con el resultado de la labor del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, el Grupo observa la existencia de una serie de propuestas para promover el comportamiento responsable de los Estados en materia de TIC, las cuales, entre otras cosas, apoyarían las capacidades de los Estados para cumplir los compromisos con respecto a su uso de las TIC, en particular el Programa de Acción. Al considerar estas propuestas, deben tenerse en cuenta las preocupaciones e intereses de todos los Estados mediante su participación equitativa en las Naciones Unidas. A este respecto, habría que seguir desarrollando el Programa de Acción, incluso en el marco del proceso del Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 75/240 de la Asamblea General.

98. El Grupo recomienda a los Estados Miembros que se guíen por las evaluaciones y recomendaciones que figuran en el presente informe y en los de anteriores Grupos de Expertos Gubernamentales, así como por las conclusiones y recomendaciones del informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (A/75/816), y que estudien el modo en que se podrían seguir desarrollando y aplicando.

Anexo

Lista de miembros del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional

Alemania
Regine Grienberger (períodos de sesiones tercero y cuarto)
Embajadora de Ciberpolítica Exterior, Ministerio Federal de Relaciones Exteriores

Wolfram von Heynitz (períodos de sesiones primero y segundo)
Jefe de Personal de Coordinación de Ciberpolítica Internacional, Ministerio Federal de Relaciones Exteriores

Australia
Johanna Weaver
Asesora Especial del Embajador de Australia para Asuntos Cibernéticos
Departamento de Relaciones Exteriores y Comercio

Brasil
Guilherme de Aguiar Patriota
Embajador, Cónsul General del Brasil en Mumbai

China
Wang Lei
Coordinador de Asuntos Cibernéticos, Ministerio de Relaciones Exteriores

Estados Unidos
Michele Markoff
Coordinadora Interina para Cuestiones Cibernéticas, Departamento de Estado de los Estados Unidos

Estonia
Heli Tiirmaa-Klaar
Embajadora en Misión Especial para la Ciberdiplomacia, Directora General, Departamento de Ciberdiplomacia, Ministerio de Relaciones Exteriores

Federación de Rusia
Andrey Krutskikh
Representante Especial del Presidente de la Federación de Rusia para la Cooperación Internacional en materia de Seguridad de la Información, Director del Departamento de Seguridad Internacional de la Información, Ministerio de Relaciones Exteriores

Vladimir Shin (períodos de sesiones tercero y cuarto)
Director Adjunto, Departamento de Seguridad Internacional de la Información, Ministerio de Relaciones Exteriores

Francia
Henri Verdier
Embajador para Asuntos Digitales, Ministerio de Europa y de Relaciones Exteriores

India
S. Janakiraman
Secretario y Jefe de las Divisiones de Gobernanza Electrónica y Tecnología de la Información y de Ciberdiplomacia, Ministerio de Relaciones Exteriores

Indonesia
Rolliansyah Soemirat (períodos de sesiones tercero y cuarto)
Director de Seguridad Internacional y Desarme, Ministerio de Relaciones Exteriores

Harditya Suryawanto (segundo período de sesiones)
Consejero, Asuntos de Lucha contra el Terrorismo y Cibernéticos, Dirección de Seguridad Internacional y Desarme, Ministerio de Relaciones Exteriores

Grata Endah Werdaningtyas (primer período de sesiones)
Directora de Seguridad Internacional y Desarme, Dirección de Seguridad Internacional y Desarme, Ministerio de Relaciones Exteriores

Japón
Takeshi Akahori
Embajador para Asuntos de las Naciones Unidas y Ciberpolítica, Ministerio de Relaciones Exteriores

Jordania
Feras Mohammad Abdallah Alzoubi
Jefe de la Subdivisión del Programa Nacional de Ciberseguridad, Fuerzas Armadas de Jordania

Kazajstán
Asset Nussupov
Jefe de Sección, Oficina Ejecutiva del Presidente de la República de Kazajstán

Kenya
Katherine Getao
Directora General, Autoridad de Tecnologías de la Información y las Comunicaciones

Marruecos
Abdellah Boutrig
Coronel Mayor, Director de Asistencia, Capacitación, Control y Conocimientos Especializados, Dirección General de Seguridad de los Sistemas de Información, Administración de la Defensa Nacional

Mauricio
Kaleem Ahmed Usmani
Jefe del Equipo de Respuesta a Emergencias Informáticas de Mauricio (CERT-MU)

México
Gerardo Isaac Morales Tenorio
Coordinador de Seguridad Multidimensional, Secretaría de Relaciones Exteriores

Noruega
Simen Ekblom (períodos de sesiones tercero y cuarto)
Coordinador de Ciberpolítica, Ministerio de Relaciones Exteriores

Anniken Krutnes (períodos de sesiones primero y segundo)
Directora General Adjunta, Departamento de Política de Seguridad y Alto Norte, Ministerio de Relaciones Exteriores

Países Bajos
Carmen Gonsalves
Jefa de Ciberpolítica Internacional, Ministerio de Relaciones Exteriores

Rumania
Mihaela-Ionelia Popescu
Coordinadora de Ciberpolítica, Ministerio de Relaciones Exteriores

Singapur
David Koh
Director General de la Agencia de Ciberseguridad de Singapur y Comisionado de Ciberseguridad

Sudáfrica
Doc Mashabane
Director General del Departamento de Justicia y Desarrollo Constitucional

Moliehi Makumane (períodos de sesiones tercero y cuarto)
Asesora Especial del representante de Sudáfrica en el Grupo de Expertos Gubernamentales

Suiza
Nadine Olivieri Lozano
Embajadora, Jefa de la División de Seguridad Internacional, Departamento Federal de Relaciones Exteriores

Reino Unido
Kathryn Jones
Jefa de Cibergobernanza Internacional, Dirección de Seguridad Nacional, Ministerio de Relaciones Exteriores, del Commonwealth y de Desarrollo

Alexander Evans (primer período de sesiones)
Ex-Director de Asuntos Cibernéticos, Ministerio de Relaciones Exteriores, del Commonwealth y de Desarrollo

Uruguay
Noelia Martínez Franchi (períodos de sesiones tercero y cuarto)
Directora de Asuntos Multilaterales, Ministerio de Relaciones Exteriores

Alejandra Erramuspe (períodos de sesiones primero y segundo)
Oficial Superior, Agencia de Gobierno Electrónico y Sociedad de la Información, Oficina de la Presidencia