Naciones Unidas A/75/816

Asamblea General

Distr. general
18 de marzo de 2021
Español
Original: inglés

Septuagésimo quinto período de sesiones
Tema 98 del programa
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Nota del Secretario General

El Secretario General tiene el honor de transmitir a los miembros de la Asamblea General el informe 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, de conformidad con lo dispuesto en la resolución 73/27 y la decisión 75/550 de la Asamblea.

21-03673 (S) 120421 140421

Informe 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

I. Introducción

1. En su resolución 73/27, la Asamblea General decidió establecer, a partir de 2019, un grupo de trabajo de composición abierta, que actuaría por consenso, para que siguiera elaborando con carácter prioritario las reglas, normas y principios de comportamiento responsable de los Estados, así como las modalidades de aplicación correspondientes; que, de ser necesario, les introdujera cambios o elaborara reglas de comportamiento adicionales; que estudiara la posibilidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas; y que siguiera estudiando, con miras a promover la comprensión común, las amenazas actuales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para hacerles frente y la forma en que el derecho internacional se aplicaba a la utilización de las tecnologías de la información y las comunicaciones por los Estados, así como las medidas de fomento de la confianza y la creación de capacidad, y en su septuagésimo quinto período de sesiones le presentara un informe sobre los resultados del estudio, y que ofreciera la posibilidad de que se celebrasen, dentro de los límites de las contribuciones voluntarias, reuniones consultivas entre períodos de sesiones con las partes interesadas, a saber, las empresas, las organizaciones no gubernamentales y los círculos académicos, para intercambiar opiniones sobre las cuestiones comprendidas en el mandato del grupo. La Asamblea decidió también que el grupo de trabajo de composición abierta celebrara un período de sesiones de organización en junio de 2019 para acordar sus disposiciones de organización.

2. En su decisión 75/550, la Asamblea General, observando que, debido a la pandemia de enfermedad por coronavirus (COVID-19), el tercer y último período de sesiones sustantivo, previsto para los días 6 a 10 de julio de 2020, había sido cancelado, decidió que el Grupo de Trabajo de Composición Abierta continuaría su labor de conformidad con su mandato previsto en la resolución 73/27 de la Asamblea, y convocaría su tercer y último período de sesiones sustantivo del 8 al 12 de marzo de 2021.

II. Cuestiones de organización

A. Apertura y duración de los períodos de sesiones

3. El Grupo de Trabajo celebró su período de sesiones de organización el 3 de junio de 2019, su primer período de sesiones sustantivo del 9 al 13 de septiembre de 2019, su segundo período de sesiones sustantivo del 10 al 14 de febrero de 2020 y su tercer período de sesiones sustantivo del 8 al 12 de marzo de 2021, todos en la Sede.

4. La Oficina de Asuntos de Desarme y el Instituto de las Naciones Unidas de Investigación sobre el Desarme prestaron apoyo sustantivo al Grupo de Trabajo. El Departamento de la Asamblea General y de Gestión de Conferencias prestó servicios de secretaría.

B. Participantes

5. La lista de participantes de los períodos de sesiones sustantivos figura en los documentos A/AC.290/2019/INF/1, A/AC.290/2020/INF/1 y A/AC.290/2021/INF/1.

C. Miembros de la Mesa

6. En su sesión de organización, celebrada el 3 de junio de 2019, el Grupo de Trabajo eligió por aclamación a Juerg Lauber (Suiza) para ocupar la Presidencia.

D. Aprobación del programa

7. En la misma sesión, el Grupo de Trabajo aprobó el programa, que figura en el documento A/AC.290/2019/1, de todos sus períodos de sesiones. El programa es el siguiente:

1. Elección de la Mesa.
2. Aprobación del programa
3. Organización de los trabajos.
4. Intercambio general de opiniones.
5. Debates sobre las cuestiones sustantivas que figuran en el párrafo 5 de la resolución 73/27 de la Asamblea General:
    a) Seguir elaborando las reglas, normas y principios de comportamiento responsable de los Estados enunciados en el párrafo 1 de la resolución 73/27 de la Asamblea General, así como las modalidades de aplicación correspondientes, y, de ser necesario, introducir cambios en ellas o elaborar reglas de comportamiento adicionales;
    b) Estudiar la posibilidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas;
    c) Seguir estudiando, con miras a promover la comprensión común, las amenazas actuales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para hacerles frente;
    d) La forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones por los Estados;
    e) Las medidas de fomento de la confianza;
    f) La creación de capacidad y los conceptos a que se hace referencia en el párrafo 3 de la resolución 73/27 de la Asamblea General.
6. Otros asuntos.
7. Aprobación del informe final.

8. Además, en la misma sesión, el Grupo de Trabajo decidió llevar a cabo su labor de conformidad con el reglamento de las comisiones principales de la Asamblea General, actuando por consenso, de conformidad con la resolución 73/27 de la Asamblea General. El Grupo de Trabajo decidió también que, en consonancia con el reglamento y la práctica de la Asamblea, todos los Estados Miembros tenían derecho a estar representados en el Grupo. Los Estados no miembros, las organizaciones intergubernamentales y las entidades a las que se había otorgado la condición de observadoras en la Asamblea tenían una invitación permanente para participar en los períodos de sesiones y en la labor del Grupo en calidad de observadores. También se invitaría a participar a las entidades pertinentes del sistema de las Naciones Unidas únicamente con el propósito de que proporcionasen información técnica. Asimismo, las organizaciones no gubernamentales pertinentes que estuvieran reconocidas como entidades consultivas por el Consejo Económico y Social, de conformidad con la resolución 1996/31, debían comunicar a la secretaría del Grupo su interés de participar en la labor del Grupo. Las demás organizaciones no gubernamentales pertinentes que tuvieran competencia en el ámbito y la finalidad del Grupo también debían manifestar a la secretaría del Grupo su interés y, de ser así, se las invitaría a participar con arreglo al procedimiento de no objeción, en calidad de observadoras.

E. Organización de los trabajos

9. En la primera sesión de cada período de sesiones sustantivo, que tuvo lugar, respectivamente, el 9 de septiembre de 2019, el 10 de febrero de 2020 y el 8 de marzo de 2021, el Grupo de Trabajo acordó la organización de los trabajos que figura en los documentos A/AC.290/2019/2, A/AC.290/2020/1 y A/AC.290/2021/1.

F. Documentación

10. La lista completa de todos los documentos oficiales, documentos de trabajo, documentos técnicos y otros documentos de que dispuso el Grupo de Trabajo puede consultarse en el siguiente sitio web específico: www.un.org/disarmament/open-ended-working-group/.

G. Labor del Grupo de Trabajo

11. En su primer período de sesiones sustantivo, el Grupo de Trabajo examinó los temas 3 a 5 del programa en sus nueve sesiones plenarias.

12. En su segundo período de sesiones sustantivo, el Grupo de Trabajo siguió examinando el tema 5 del programa en sus nueve sesiones plenarias.

13. En su tercer período de sesiones sustantivo, el Grupo de Trabajo examinó los temas 5 a 7 del programa.

14. A fin de continuar su labor durante la pandemia de enfermedad por coronavirus (COVID-19), el Grupo de Trabajo celebró reuniones virtuales oficiosas el 15, 17 y 19 de junio y el 2 de julio de 2020; del 29 de septiembre al 1 octubre de 2020; del 17 al 19 de noviembre de 2020; del 1 al 3 de diciembre de 2020 y el 18, 19 y 22 de febrero de 2021.

15. El Grupo de Trabajo celebró una reunión consultiva oficiosa entre períodos de sesiones con participación de múltiples partes interesadas del 2 al 4 de diciembre de 2019. A pedido del Presidente del Grupo, la reunión estuvo presidida por el Jefe

Ejecutivo del Organismo de Ciberseguridad de Singapur, David Koh, quien presentó y distribuyó un resumen de los trabajos a los miembros del Grupo[1].

III. Aprobación del informe final

16. El 12 de marzo de 2021, en su tercer período de sesiones sustantivo, el Grupo de Trabajo examinó el tema 7 del programa, titulado “Aprobación del informe final”, y aprobó su informe, que figura en los documentos A/AC.290/2021/L.1, en su forma revisada oralmente, y A/AC.290/2021/CRP.2.

17. Dadas las restricciones impuestas debido a la COVID-19 en la Sede de las Naciones Unidas, por las que se limitó el número de reuniones del Grupo de Trabajo en su tercer período de sesiones sustantivo, se publicará un compendio de las declaraciones en explicación de posición como documento A/AC.290/2021/INF.2.

[1] Puede consultarse en www.un.org/disarmament/open-ended-working-group/.

Anexo I*

Informe sustantivo final

A. Introducción

1. Pese a las transformaciones radicales que el mundo ha vivido desde la fundación de las Naciones Unidas hace 75 años, su propósito y sus ideales atemporales siguen teniendo la misma relevancia que cuando se fundaron. Junto con la reafirmación de su fe en los derechos fundamentales del hombre y el compromiso de promover el progreso económico y social de todos los pueblos y crear condiciones bajo las cuales puedieran mantenerse la justicia y el respeto del derecho internacional, los Estados resolvieron unir sus fuerzas para mantener la paz y la seguridad internacionales[2].

2. Los avances en las tecnologías de la información y las comunicaciones (TIC) tienen repercusiones en los tres pilares de la labor de las Naciones Unidas: la paz y la seguridad, los derechos humanos y el desarrollo sostenible. Las TIC y la conectividad mundial han catalizado el progreso y el desarrollo humanos, han transformado las sociedades y las economías y han ampliado las oportunidades de cooperación.

3. La necesidad de consolidar y mantener la paz, la seguridad, la cooperación y la confianza a nivel internacional en el entorno de la TIC nunca ha sido tan evidente como ahora. Algunas tendencias negativas en el ámbito digital podrían menoscabar la seguridad y estabilidad internacionales, someter a grandes presiones el crecimiento económico y el desarrollo sostenible e impedir el pleno disfrute de los derechos humanos y las libertades fundamentales. Una de estas tendencias es el uso creciente de las TIC con fines malintencionados.

4. La actual crisis sanitaria mundial ha puesto de relieve los beneficios fundamentales de las TIC y nuestra dependencia de ellas, entre otras cosas para prestar servicios gubernamentales vitales, transmitir mensajes de seguridad pública esenciales, desarrollar soluciones innovadoras para garantizar la continuidad de las operaciones, acelerar la investigación y ayudar a asegurar la continuidad de la educación y la cohesión social por medios virtuales. En este momento de incertidumbre, los Estados, el sector privado, los científicos y otros interlocutores han aprovechado la tecnología digital para mantener a las personas y las sociedades conectadas y sanas. Al mismo tiempo, la pandemia de COVID-19 ha puesto en evidencia los riesgos y las consecuencias de las actividades malintencionadas con las que se trata de explotar las vulnerabilidades en momentos en que las sociedades soportan una enorme presión. También ha puesto de manifiesto la necesidad de reducir las brechas digitales, crear resiliencia en todas las sociedades y sectores, y mantener un enfoque centrado en el ser humano.

5. Dado que las TIC pueden usarse con fines incompatibles con el mantenimiento de la paz, la estabilidad y la seguridad internacionales, la Asamblea General ha reconocido[3] que la difusión y la utilización de estas tecnologías repercuten en los intereses de toda la comunidad mundial y que su eficacia óptima se fomenta mediante una amplia cooperación internacional.

6. Habida cuenta de lo anterior, el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, establecido en virtud de la resolución 73/27 de la Asamblea General, brindó la oportunidad de impulsar el examen de esta cuestión fundamental. Además, ofreció una plataforma democrática, transparente e inclusiva para que todos los Estados participaran, expresaran sus opiniones y ofrecieran su

* Publicado sin revisión editorial.

[2] Preámbulo de la Carta de las Naciones Unidas.

[3] Véase, por ejemplo, A/RES/53/70, sexto párrafo del preámbulo.

cooperación con respecto a la dimensión de la seguridad internacional de las TIC. La participación activa de los miembros de las Naciones Unidas y la colaboración de otras partes interesadas pertinentes demuestran la aspiración compartida y el interés colectivo de la comunidad internacional de lograr un entorno pacífico y seguro para todos en el entorno de las TIC y su propósito de cooperar para lograrlo.

7. El Grupo de Trabajo representa un hito significativo en la cooperación internacional hacia el logro de un entorno de la TIC que sea abierto, seguro, estable, accesible y pacífico. Desde 2003 se han establecido grupos de expertos gubernamentales en seis ocasiones para estudiar amenazas reales y potenciales en el ámbito de la seguridad de la información y posibles medidas de cooperación para encararlas[4]. A través de sus tres informes aprobados por consenso (2010, 2013 y 2015[5]), que son de carácter acumulativo, estos Grupos recomendaron 11 normas voluntarias y no vinculantes de comportamiento responsable de los Estados y reconocieron que con el tiempo podrían elaborarse más normas. Además, recomendaron medidas específicas de fomento de la confianza, desarrollo de la capacidad y cooperación. También reafirmaron que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el entorno de las TIC. En la resolución 70/237 de la Asamblea General, los Estados Miembros acordaron por consenso guiarse por el informe de 2015 del Grupo de Expertos Gubernamentales en su uso de las TIC, consolidando así un marco inicial para el comportamiento responsable de los Estados en el uso de dichas tecnologías. A este respecto, el Grupo de Trabajo también señaló las resoluciones de la Asamblea General 73/27 y 73/266.

8. Sobre esta base y reafirmando este marco, el Grupo de Trabajo ha tratado de llegar a un terreno común y un entendimiento mutuo entre todos los Estados Miembros de las Naciones Unidas sobre un tema de trascendencia mundial. De acuerdo con su mandato, el Grupo de Trabajo deliberó sobre las amenazas reales y potenciales en el ámbito de la seguridad de la información y la posibles medidas de cooperación para afrontarlas; el desarrollo ulterior de reglas, normas y principios sobre el comportamiento responsable de los Estados; la aplicación del derecho internacional al uso de las TIC por los Estados; las medidas de fomento de la confianza; la creación de capacidad; y la posibilidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas. En su esfuerzo por lograr el consenso y promover la paz, la seguridad, la cooperación y la confianza internacionales, las deliberaciones del Grupo de Trabajo se guiaron por los principios de inclusión y transparencia.

9. Las Naciones Unidas deberían seguir desempeñando un papel rector en la promoción del diálogo sobre la utilización de las TIC por los Estados. El Grupo de Trabajo reconoce la importancia y complementariedad de los debates especializados sobre aspectos de las tecnologías digitales abordados por otros órganos y foros de las Naciones Unidas.

10. Si bien los Estados tienen la responsabilidad primordial de mantener la paz y la seguridad internacionales, todas las partes interesadas tienen la responsabilidad de utilizar las TIC de forma que no se ponga en peligro la paz y la seguridad. Dado que la dimensión de la seguridad internacional de las TIC abarca múltiples ámbitos y disciplinas, el Grupo de Trabajo ha aprovechado los conocimientos especializados y la experiencia que han aportado los representantes de las organizaciones intergubernamentales, las organizaciones regionales, la sociedad civil, el sector privado, los círculos académicos y la comunidad técnica. La reunión consultiva oficiosa de tres días de duración del Grupo de Trabajo, celebrada en diciembre

[4] A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237, A/RES/73/266.
[5] A/65/201, A/68/98* y A/70/174.

de 2019, dio lugar a un rico debate entre los Estados y una variedad de otras partes interesadas[6]. Además, estas han aportado propuestas y ejemplos concretos de buenas prácticas mediante contribuciones escritas e intercambios oficiosos con el Grupo de Trabajo. Algunas delegaciones también han celebrado consultas con múltiples partes interesadas por propia iniciativa para fundamentar sus contribuciones al Grupo de Trabajo.

11. El Grupo de Trabajo, consciente de las distintas situaciones, capacidades y prioridades de los Estados y las regiones, reconoce que los beneficios de las tecnologías digitales no están distribuidos de manera uniforme y que una prioridad urgente para la comunidad internacional sigue siendo la de reducir las brechas digitales, incluso ampliando el acceso a las TIC y la conectividad.

12. El Grupo de Trabajo acoge con agrado la gran participación de delegadas en sus períodos de sesiones y la prominencia de las perspectivas de género en sus discusiones. Además subraya la importancia de reducir la brecha digital de género y promover la participación eficaz y significativa y el liderazgo de las mujeres en los procesos de toma de decisiones vinculados a la utilización de las TIC en el contexto de la seguridad internacional.

13. El Grupo de Trabajo subraya que los distintos elementos de que se compone su mandato están interrelacionados y se refuerzan mutuamente, y juntos fomentan un entorno de TIC abierto, seguro, estable, accesible y pacífico.

B. Conclusiones y recomendaciones

14. Habiendo examinado los aspectos sustantivos del mandato del Grupo de Trabajo, y recordando que la resolución 73/27 de la Asamblea General acogió con beneplácito la eficaz labor realizada en 2010, 2013 y 2015 por el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y los correspondientes informes finales transmitidos por el Secretario General[7], los Estados llegaron a las siguientes conclusiones y recomendaciones, que incluyen acciones concretas y medidas de cooperación para hacer frente a las amenazas de las TIC y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico.

Amenazas reales y potenciales

15. Los Estados concluyeron que estaban cada vez más preocupados por las repercusiones del uso malintencionado de las TIC en el mantenimiento de la paz y la seguridad internacionales, y, por ende, en los derechos humanos y el desarrollo. En particular, se expresó preocupación por la posibilidad de que las capacidades de TIC se utilizaran para fines que pudieran menoscabar la paz y la seguridad internacionales. Los incidentes perjudiciales vinculados a la TIC son cada vez más frecuentes y sofisticados, y evolucionan y se diversifican constantemente. La conectividad y la dependencia crecientes de las TIC sin las consiguientes medidas que garanticen su seguridad pueden traer consigo riesgos imprevistos y hacer a las sociedades más vulnerables frente a las actividades malintencionadas de la TIC. Pese a los incalculables beneficios que suponen estas tecnologías para la humanidad, su uso malintencionado puede tener repercusiones negativas de gran alcance.

[6] Véase el resumen de la Presidencia de la reunión consultiva oficiosa entre períodos de sesiones del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, disponible en https://www.un.org/disarmament/open-ended-working-group/.

[7] A/65/201, A/68/98* y A/70/174.

16. Los Estados recordaron que varios Estados están desarrollando capacidades de TIC con fines militares. También recordaron que el uso de las TIC en futuros conflictos entre Estados es cada vez más probable. El aumento continuo de los incidentes de uso malintencionado de las TIC por agentes estatales y no estatales, incluidos terroristas y grupos delictivos, es una tendencia perturbadora. Algunos agentes no estatales han demostrado tener capacidades de TIC que antes solo estaban al alcance de los Estados.

17. Los Estados también concluyeron que cualquier uso de las TIC por los Estados de forma incompatible con las obligaciones que contrajeron en el marco, que incluye normas voluntarias, el derecho internacional y medidas de fomento de la confianza, menoscaba la paz y la seguridad internacionales, la confianza y la estabilidad entre los Estados, y puede aumentar la probabilidad de futuros conflictos entre ellos.

18. Los Estados concluyeron que las actividades malintencionadas de las TIC contra la infraestructura crítica y la infraestructura de información crítica en que se sustentan servicios públicos esenciales pueden tener devastadoras consecuencias económicas, sociales, humanitarias y para la seguridad. Aunque es prerrogativa de cada Estado determinar qué infraestructuras designa como críticas, tales infraestructuras pueden incluir instalaciones médicas, servicios financieros, la energía, el agua, el transporte y el saneamiento. Las actividades malintencionadas de las TIC contra la infraestructura crítica y la infraestructura de información crítica que menoscaban la confianza en los procesos políticos y electorales y las instituciones públicas o que afectan a la disponibilidad general o la integridad de Internet, también son un problema real y creciente. Dichas infraestructuras pueden ser propiedad del sector privado, estar gestionadas o explotadas por él, pueden estar compartidas o conectadas en red con otro Estado o ser explotadas por diferentes Estados. Por eso, la cooperación entre los Estados o entre los sectores público y privado podría ser necesaria para proteger su integridad, funcionamiento y disponibilidad.

19. Los Estados también concluyeron que cualquier actividad de las TIC contraria a las obligaciones contraídas en virtud del derecho internacional que dañe intencionadamente la infraestructura crítica o dificulte de otro modo su utilización y funcionamiento para prestar servicios al público, podría suponer una amenaza no solo para la seguridad sino también para la soberanía de los Estados, así como para el desarrollo económico y los medios de subsistencia y, en última instancia, para la seguridad y el bienestar de las personas.

20. Dado que todos los Estados dependen cada vez más de las tecnologías digitales, estos llegaron a la conclusión de que el desconocimiento y la falta de capacidades adecuadas para detectar las actividades malintencionadas de TIC, defenderse contra ellas o responder a ellas podrían hacerlos más vulnerables. Como se ha observado en la actual emergencia sanitaria mundial, las vulnerabilidades ya existentes pueden agravarse en épocas de crisis.

21. Los Estados concluyeron que las amenazas podían afectar de distinto modo a los Estados en función de sus niveles de digitalización, capacidad, seguridad y resiliencia de la TIC, infraestructura y desarrollo. Las amenazas también pueden afectar de forma distinta a los distintos grupos y entidades, como la juventud, las personas mayores, las mujeres y los hombres, las personas vulnerables, algunas profesiones concretas, las pequeñas y medianas empresas y otros.

22. Habida cuenta de la situación cada vez más preocupante de las amenazas digitales, y reconociendo que ningún Estado está a salvo de ellas, los Estados coincidieron en la urgencia de implantar y seguir desarrollando medidas de cooperación para abordar tales amenazas. También afirmaron que si actuaban unidos y de forma inclusiva, siempre que fuera posible, lograrían resultados más eficaces y

de mayor alcance. En este sentido, se destacó además la importancia de seguir reforzando la colaboración con la sociedad civil, el sector privado, el mundo académico y la comunidad técnica, cuando procediera.

23. Los Estados destacaron las buenas oportunidades económicas y sociales que podían derivarse de las TIC y concluyeron que lo que resultaba preocupante era el uso indebido de las tecnologías y no las tecnologías en sí mismas.

Normas, reglas y principios de comportamiento responsable de los Estados

24. Las normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados pueden reducir los riesgos para la paz, la seguridas y la estabilidad internacionales y contribuyen notablemente a aumentar la previsibilidad y reducir los riesgos de percepciones erróneas y, de este modo, contribuyen a la prevención de los conflictos. Los Estados destacaron que dichas normas reflejaban las expectativas y los estándares de la comunidad internacional en cuanto al comportamiento de los Estados en su utilización de las TIC y permitían a la comunidad internacional evaluar las actividades de los Estados. De conformidad con la resolución 70/237 de la Asamblea General, y reconociendo la resolución 73/27 de la Asamblea General, se pidió a los Estados que evitaran y se abstuvieran de utilizar las TIC de forma que no estuviera en consonancia con las normas de comportamiento responsable de los Estados.

25. Los Estados convinieron en que las normas no sustituían ni alteraban las obligaciones o derechos de los Estados en virtud del derecho internacional, que eran vinculantes, sino que proporcionaban orientación específica adicional sobre lo que constituía comportamiento responsable de los Estados en la utilización de las TIC. Las normas no pretendían limitar o prohibir acciones que de algún modo estuvieran en consonancia con el derecho internacional.

26. Si bien coincidieron en la necesidad de proteger todas las infraestructuras críticas y las infraestructuras de información críticas de que dependen los servicios públicos esenciales, además de esforzarse por garantizar la disponibilidad general y la integridad de Internet, los Estados concluyeron además que la pandemia de COVID-19 había acentuado la importancia de proteger la infraestructura sanitaria, incluidos los servicios y las instalaciones médicas, implementando las normas relativas a la infraestructura crítica como las afirmadas por consenso a través de la resolución 70/237 de la Asamblea General.

27. Los Estados afirmaron la importancia de apoyar e impulsar los esfuerzos para aplicar las normas que los Estados se han comprometido a seguir en los planos mundial, regional y nacional.

28. Los Estados, reafirmando la resolución 70/237 de la Asamblea General y reconociendo la resolución 73/27 de la Asamblea General, deberían: adoptar medidas razonables para garantizar la integridad de la cadena de suministro, incluso formulando medidas de cooperación objetivas, de modo que los usuarios finales puedan confiar en la seguridad de los productos de las TIC; tratar de evitar la proliferación de técnicas e instrumentos malintencionados de las TIC, así como el uso de funciones ocultas perniciosas; y alentar la información responsable sobre las vulnerabilidades.

29. Dadas las características particulares de las TIC, los Estados reafirmaron que, teniendo en cuenta las propuestas sobre normas formuladas en el Grupo de Trabajo, podrían seguir desarrollándose nuevas normas en el futuro. Los Estados también llegaron a la conclusión de que seguir desarrollando normas y aplicar las ya existentes no eran actividades mutuamente excluyentes, sino que podían ocurrir simultáneamente.

El Grupo de Trabajo recomienda lo siguiente:

30. Los Estados, de forma voluntaria, deberían hacer un estudio de los esfuerzos que se realizan a nivel nacional para implementar las normas, adquirir experiencia y compartir buenas prácticas sobre su implementación, y seguir informando al Secretario General de sus opiniones y evaluaciones nacionales al respecto.

31. Los Estados no deberían 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 su utilización y funcionamiento para prestar servicios al público. Además, los Estados deben seguir reforzando las medidas para proteger toda la infraestructura crítica frente a las amenazas de las TIC y aumentar los intercambios de buenas prácticas al respecto.

32. Los Estados, en asociación con las organizaciones pertinentes, incluidas las Naciones Unidas, deben seguir apoyando la implementación y el desarrollo de normas de comportamiento responsable de los Estados. Se debería alentar a los Estados que estén en condiciones de aportar conocimientos o recursos a que lo hagan.

33. Los Estados, recordando la resolución 70/237 de la Asamblea General y reconociendo la resolución 73/27 de la Asamblea General, toman nota de las propuestas formuladas por los Estados sobre la elaboración de reglas, normas y principios de comportamiento responsable de los Estados para futuras discusiones sobre las TIC en las Naciones Unidas, señalando que en la resolución 75/240 se estableció un Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021-2025.

Derecho internacional

34. Reconociendo la resolución 70/237 de la Asamblea General, y reconociendo también la resolución 73/27 de la Asamblea General, por la que se estableció el Grupo de Trabajo, los Estados reafirmaron que el derecho internacional, y en particular la Carta de las Naciones Unidas, era aplicable y esencial para mantener la paz y la estabilidad y promover un entorno de la TIC abierto, seguro, estable, accesible y pacífico. A este respecto, se pidió a los Estados que evitaran y se abstuvieran de adoptar cualquier medida que no estuviera en consonancia con el derecho internacional, y en particular la Carta de las Naciones Unidas. Los Estados también concluyeron que debía haber más entendimiento común sobre el modo en que el derecho internacional era aplicable al uso de las TIC por los Estados.

35. Los Estados también reafirmaron que debía intentarse el arreglo pacífico de controversias por medios pacíficos como la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial y el recurso a organismos o acuerdos regionales, u otros medios pacíficos de su elección.

36. Los Estados convinieron en que, dadas las características particulares del entorno de las TIC, podía llegarse a entendimientos comunes más sólidos sobre el modo en que el derecho internacional era aplicable al uso de las TIC por los Estados intercambiando opiniones al respecto y designando temas específicos del derecho internacional para discutirlos más a fondo en las Naciones Unidas.

37. A fin de que todos los Estados entiendan mejor de qué forma el derecho internacional es aplicable a su uso de las tecnologías de la TIC, y con miras a contribuir a crear consenso y entendimiento común en la comunidad internacional, los Estados convinieron en que era necesario realizar más esfuerzos neutrales y objetivos para desarrollar la capacidad en las esferas del derecho internacional y la legislación y las políticas nacionales.

El Grupo de Trabajo recomienda lo siguiente:

38. Los Estados deberían seguir informando, de forma voluntaria, al Secretario General sobre sus opiniones y evaluaciones a nivel nacional con respecto al modo en que el derecho internacional puede aplicarse a su uso de las TIC en el contexto de la seguridad internacional, y seguir compartiendo voluntariamente sus opiniones y prácticas nacionales por otras vías según corresponda.

39. Los Estados que estén en condiciones de hacerlo deberían seguir apoyando, de forma neutral y objetiva, más iniciativas para desarrollar la capacidad, de acuerdo con los principios incluidos en el párrafo 56 del presente informe, en las esferas del derecho internacional y la legislación y las políticas nacionales, a fin de que todos los Estados contribuyan a generar entendimientos comunes del modo en que el derecho internacional es aplicable a su uso de las TIC y para contribuir a crear consenso en la comunidad internacional.

40. Los Estados deberían seguir estudiando y debatiendo, en el marco de futuros procesos de las Naciones Unidas, cómo se aplica el derecho internacional a su uso de las TIC, como paso clave para aclarar y seguir desarrollando entendimientos comunes sobre la cuestión.

Medidas de fomento de la confianza

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

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

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

44. Además, los Estados coincidieron en que las Naciones Unidas tienen un papel fundamental en la elaboración de medidas de fomento de la confianza y el apoyo a su implementación a nivel mundial. En todos los informes del Grupo de Expertos aprobados por consenso se han recomendado medidas prácticas de fomento de la confianza. Además de estas recomendaciones orientadas específicamente a las TIC, en la resolución 43/78 H, aprobada por consenso, la Asamblea General hizo suyas las

Directrices para las Medidas de Fomento de la Confianza elaboradas en la Comisión de Desarme de las Naciones Unidas, en las que se definían principios, objetivos y características de gran valor para las medidas de fomento de la confianza que pueden tenerse en cuenta al elaborar nuevas medidas específicas para las TIC.

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

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

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

El Grupo de Trabajo recomienda lo siguiente:

48. Los Estados deberían seguir informando al Secretario General, de forma voluntaria, sobre sus opiniones y evaluaciones, incluyendo información adicional sobre las lecciones aprendidas y las buenas prácticas en relación con las medidas de fomento de la confianza pertinentes en los planos bilateral, regional o multilateral.

49. Los Estados deberían determinar y examinar voluntariamente las medidas de fomento de la confianza adecuadas para sus contextos específicos y cooperar con otros Estados en su implementación.

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

51. Los Estados que aún no lo hayan hecho deberían considerar la designación de un punto de contacto nacional en los planos técnico, diplomático y de políticas, teniendo en cuenta las capacidades diferenciadas. Se alienta también a los Estados a que sigan examinando las modalidades para establecer un directorio de estos puntos de contacto a nivel mundial.

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

53. Los Estados deberían seguir estudiando la posibilidad de adoptar medidas de fomento de la confianza a nivel bilateral, regional y multilateral y fomentando las oportunidades para el ejercicio cooperativo de estas medidas.

Desarrollo de la capacidad

54. La capacidad de la comunidad internacional para prevenir o atenuar las repercusiones de las actividades malintencionadas de la TIC depende de la capacidad que tenga cada Estado para prepararse y responder a ellas. Esto es de especial importancia para los Estados en desarrollo, si se quiere facilitar su verdadera participación en las discusiones sobre las TIC en el contexto de la seguridad internacional y su capacidad para abordar las vulnerabilidades de su infraestructura crítica. La creación de capacidad ayuda a desarrollar las aptitudes, los recursos humanos, las políticas y las instituciones necesarias para aumentar la resiliencia y la seguridad de los Estados a fin de que puedan gozar plenamente de los beneficios de las tecnologías digitales. Desempeña una importante función facilitadora para promover el cumplimiento del derecho internacional y la implementación de normas sobre el comportamiento responsable de los Estados, y apoyar la implementación de medidas de fomento de la confianza. En un mundo digitalmente interdependiente, los beneficios del desarrollo de la capacidad se extienden más allá de los beneficiarios iniciales y contribuyen a crear un entorno de la TIC más seguro y estable para todos.

55. Garantizar un entorno de TIC abierto, seguro, estable, accesible y pacífico requiere una cooperación eficaz entre los Estados que permita reducir los riesgos para la paz y la seguridad internacionales. El desarrollo de la capacidad es un aspecto importante de dicha cooperación y un acto voluntario tanto del donante como del receptor.

56. Teniendo en cuenta y debatiendo más a fondo algunos principios ampliamente aceptados, los Estados coincidieron en que el desarrollo de la capacidad en relación con el uso de las TIC por los Estados en el contexto de la seguridad internacional debe guiarse por los siguientes principios:

Proceso y finalidad

- El desarrollo de la capacidad debe ser un proceso sostenible y comprender actividades específicas por y para distintos agentes.

- Determinadas actividades deben tener un objetivo claro y centrarse en el logro de resultados y, al mismo tiempo, apoyar el objetivo común de establecer un entorno de la TIC abierto, seguro, estable, accesible y pacífico.

- Las actividades de desarrollo de la capacidad deben contar con una base empírica y ser políticamente neutrales, transparentes, responsables e incondicionales.

- El desarrollo de la capacidad debe llevarse a cabo respetando plenamente el principio de la soberanía de los Estados.

- Es posible que deba facilitarse el acceso a las tecnologías pertinentes.

Alianzas

- El desarrollo de la capacidad debe basarse en la confianza mutua y en la demanda, corresponder a unas necesidades y prioridades determinadas a nivel nacional y llevarse a cabo reconociendo plenamente la implicación nacional. Los asociados en el desarrollo de la capacidad deben participar voluntariamente.

- Dado que las actividades de desarrollo de la capacidad deben adaptarse a necesidades y contextos específicos, todas las partes son asociados activos en ellas,

con responsabilidades compartidas pero diferenciadas, en particular las de colaborar en el diseño, la ejecución, el seguimiento y la evaluación de dichas actividades.

- Todos los asociados deben proteger y respetar la confidencialidad de las políticas y los planes nacionales.

Las personas

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

- Debe garantizarse la confidencialidad de la información sensible.

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

58. Los Estados concluyeron que el desarrollo de la capacidad debía contribuir a transformar la brecha digital en oportunidades digitales. En particular, debería orientarse a facilitar una auténtica participación de los países en desarrollo en las discusiones y foros pertinentes y reforzar la resiliencia de los países en desarrollo en el entorno de las TIC.

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

60. Además de las competencias técnicas, la creación de instituciones y los mecanismos de cooperación, los Estados concluyeron que hay una necesidad urgente de adquirir conocimientos especializados en los ámbitos diplomático, jurídico, político, legislativo y regulador. En este contexto se destacó la importancia de desarrollar capacidad diplomática para participar en procesos internacionales e intergubernamentales.

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

62. Los Estados concluyeron que hacer balance de los esfuerzos nacionales con respecto a las conclusiones y recomendaciones de este informe, así como de las evaluaciones y recomendaciones que los Estados Miembros acordaron por consenso que servirían de guía, con arreglo a la resolución 70/237, es un ejercicio valioso para determinar los progresos realizados y dónde se necesita mayor desarrollo de capacidades.

El Grupo de Trabajo recomienda lo siguiente:

63. Los Estados deberían guiarse por los principios contenidos en el párrafo 56 en sus actividades de desarrollo de la capacidad relacionada con las TIC en el ámbito de la seguridad internacional, y se debería alentar a otros agentes a que tengan en cuenta estos principios en sus propias actividades de desarrollo de la capacidad.

64. Los Estados deberían seguir informando al Secretario General, de forma voluntaria, sobre sus opiniones y evaluaciones en relación con los avances en el ámbito de las TIC en el contexto de la seguridad internacional e incluyendo información adicional sobre las lecciones aprendidas y las buenas prácticas con respecto a los programas y las iniciativas de desarrollo de la capacidad.

65. Los Estados deberían utilizar de forma voluntaria el modelo de encuesta nacional sobre la implementación de la resolución 70/237 de la Asamblea General de las Naciones Unidas (que estará disponible en línea) para ayudarles a hacerlo. Los Estados Miembros también pueden utilizar el modelo de encuesta, de forma voluntaria, para estructurar la información que deben presentar al Secretario General de sus opiniones y evaluaciones mencionada anteriormente.

66. Debería alentarse a los Estados y otros agentes que estén en condiciones de hacerlo a ofrecer asistencia financiera, técnica o en especie para el desarrollo de la capacidad. Debería seguir facilitándose más coordinación y financiación de las actividades de desarrollo de la capacidad, en particular entre las organizaciones pertinentes y las Naciones Unidas.

67. Los Estados deberían seguir considerando el desarrollo de la capacidad a nivel multilateral, incluido el intercambio de opiniones, información y buenas prácticas.

Diálogo institucional periódico

68. El Grupo de Trabajo establecido en virtud de la resolución 73/27 de la Asamblea General ofreció, por primera vez bajo los auspicios de las Naciones Unidas, una plataforma específica para el diálogo entre todos los Estados sobre los avances de las TIC en el contexto de la seguridad internacional.

69. Además de su objetivo de tratar de lograr entendimientos comunes entre todos los Estados, el Grupo de Trabajo ha fomentado redes diplomáticas y ha alentado la confianza entre sus participantes. La amplia implicación de las partes interesadas no gubernamentales ha demostrado que hay una comunidad más amplia de agentes dispuesta a aprovechar su experiencia para apoyar a los Estados en su objetivo de garantizar un entorno de la TIC abierto, seguro, estable, accesible y pacífico. Las discusiones del Grupo de Trabajo fueron una afirmación de la importancia de mantener discusiones periódicas y estructuradas bajo los auspicios de las Naciones Unidas sobre el uso de las TIC.

70. Los Estados concluyeron también que un diálogo periódico bajo los auspicios de las Naciones Unidas contribuía a los objetivos compartidos de reforzar la paz internacional, la estabilidad y la prevención de los conflictos en el entorno de la TIC. También concluyeron que, dada la dependencia cada vez mayor de las TIC y el alcance de las amenazas que se derivan de su uso malintencionado, era muy necesario

seguir potenciando entendimientos comunes, fomentando la confianza e intensificando la cooperación internacional.

71. Como principales responsables de la seguridad nacional, la seguridad pública y el estado de derecho, los Estados afirmaron la importancia de mantener un diálogo intergubernamental periódico y determinar los mecanismos adecuados para interactuar con otros grupos de partes interesadas en futuros procesos.

72. El examen de los avances de las TIC y la seguridad internacional en las Naciones Unidas se centra en sus dimensiones de paz, estabilidad y prevención de conflictos a nivel internacional. Los Estados concluyeron que el diálogo institucional periódico que se mantenga en el futuro no debería duplicar los mandatos, esfuerzos y actividades existentes de las Naciones Unidas centrados en las dimensiones digitales de otras cuestiones[8]. Concluyeron también que un mayor intercambio entre estos foros y los procesos establecidos por la Primera Comisión podría contribuir a reforzar las sinergias y mejorar la coherencia, respetando al mismo tiempo el carácter o el mandato especializados de cada órgano.

73. Los Estados concluyeron que, en el futuro, el diálogo sobre cooperación internacional en torno a las TIC en el contexto de la seguridad internacional debía, entre otras cosas, crear conciencia, fomentar la confianza y alentar más estudios y debates sobre esferas en que aún no hay entendimiento común. Los Estados reconocieron la utilidad de explorar mecanismos dedicados al seguimiento de la implementación de las normas y reglas acordadas, así como al desarrollo de otras nuevas.

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

El Grupo de Trabajo recomienda lo siguiente:

75. Los Estados deben seguir participando activamente en un diálogo institucional periódico bajo los auspicios de las Naciones Unidas.

76. Los Estados deben asegurar la continuación del 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.

77. Los Estados deben toman nota 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, el Programa de Acción debería seguir elaborándose, incluso en el proceso del Grupo

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

de Trabajo de Composición Abierta establecido en virtud de la resolución 75/240 de la Asamblea General.

78. Los Estados deben considerar las conclusiones y recomendaciones del presente informe en futuros procesos de diálogo institucional periódico bajo los auspicios de las Naciones Unidas.

79. Los Estados que estén en condiciones de hacerlo deben considerar establecer o apoyar programas de patrocinio y otros mecanismos para garantizar una participación amplia en los procesos mencionados de las Naciones Unidas.

C. Observaciones finales

80. Durante todo el proceso del Grupo de Trabajo de Composición Abierta, los Estados participaron de forma constante y activa, lo que dio lugar a un rico intercambio de opiniones. Gracias a este intercambio se presentaron perspectivas diversas, ideas nuevas y propuestas importantes, con las que no todos los Estados estuvieron necesariamente de acuerdo, como la posibilidad de establecer nuevas obligaciones jurídicamente vinculantes. Las diversas perspectivas se reflejan en el anexo al Resumen de la Presidencia de los debates y las propuestas específicas de texto a incluir en relación con el tema del programa titulado “Reglas, normas y principios”. Estas perspectivas deberían seguir considerándose en futuros procesos de las Naciones Unidas, incluido el Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 75/240 de la Asamblea General.

Anexo II*

Resumen de la Presidencia

A. Contexto

1. El Grupo de Trabajo supuso una oportunidad histórica para que todos los Estados interactuaran en pie de igualdad bajo los auspicios de las Naciones Unidas manteniendo discusiones centradas específicamente en asuntos relativos a las TIC en el contexto de la seguridad internacional. Además de los muchos ámbitos de acuerdo reflejados en su informe, con sus debates inclusivos y transparentes el Grupo de Trabajo ha sido un medio valioso de fortalecer la paz y la seguridad internacionales fomentando la confianza y el entendimiento entre los Estados y ayudando a establecer una red diplomática mundial de expertos nacionales. La participación activa y amplia de todas las delegaciones ha demostrado la determinación de los Estados de seguir abordando unidos esta cuestión de importancia fundamental para todos.

2. Todos los períodos de sesiones del Grupo de Trabajo estuvieron caracterizados por intercambios interactivos sustantivos entre los Estados, así como con la sociedad civil, el sector privado, el mundo académico y la comunidad técnica. El compromiso demostrado por los Estados y otras partes interesadas durante toda la labor del Grupo de Trabajo, con su participación cada vez mayor, incluso cuando algunas de sus reuniones pasaron a formato virtual, es muestra innegable de la importancia cada vez más universal de los temas que examina, así como del reconocimiento creciente de que urge afrontar colectivamente las amenazas que representa para la seguridad internacional el uso malintencionado de las TIC.

3. Este resumen se publica bajo la responsabilidad de la Presidencia y refleja su entendimiento de los principales puntos que se debatieron durante las sesiones del Grupo de Trabajo. Es posible que no refleje la totalidad de las contribuciones de todas las delegaciones y no debe considerarse que refleja la opinión consensuada de los Estados sobre ninguno de los puntos específicos que se tratan en él. El compendio completo de las declaraciones y propuestas nacionales que se presentaron para su difusión está disponible en https://www.un.org/disarmament/open-ended-working-group.

B. Sinopsis de las discusiones

4. El proceso del Grupo de Trabajo permitió a todos los Estados expresar sus opiniones, preocupaciones y aspiraciones de manera democrática, transparente e inclusiva. Si bien el Grupo de Trabajo trató de establecer ámbitos de convergencia y consenso, sus discusiones también fueron reflejo de la diversidad de perspectivas, ideas y propuestas de los Estados Miembros, y pueden ser una base útil para seguir trabajando en pos de entendimientos comunes sobre el uso de las TIC por los Estados en el contexto de la seguridad internacional.

5. En sus deliberaciones en el Grupo de Trabajo, los Estados subrayaron los vínculos y las sinergias entre cada uno de los elementos de su mandato: el derecho internacional rige las acciones y las relaciones entre los Estados y las normas voluntarias y no vinculantes proporcionan orientación adicional sobre lo que constituye el comportamiento responsable de los Estados. Estos dos elementos reflejan las expectativas de comportamiento en el uso de las TIC por los Estados en el contexto de la seguridad internacional. De este modo, también contribuyen a fomentar la confianza al aumentar la transparencia y la cooperación entre los Estados y a reducir el riesgo de conflicto. A su vez, el desarrollo de la capacidad permite que

* Publicado sin revisión editorial.

todos los Estados contribuyan a aumentar la estabilidad y la seguridad a nivel mundial. Conjuntamente, estos elementos constituyen un marco mundial de medidas de cooperación para hacer frente a amenazas reales o potenciales en el ámbito de las TIC. El diálogo institucional periódico brindará la oportunidad de seguir desarrollando y aplicando este marco mediante el fomento de entendimientos comunes, el intercambio de las lecciones aprendidas y las buenas prácticas de aplicación, el fomento de la confianza y el aumento de la capacidad entre los Estados.

Amenazas reales y potenciales

6. En sus discusiones en el Grupo de Trabajo, los Estados mencionaron una amplia gama de amenazas reales y potenciales, lo que puso de manifiesto que estos pueden percibir de formas distintas las amenazas procedentes del entorno de las TIC. El formato inclusivo del Grupo de Trabajo ofreció a los Estados la oportunidad de profundizar su comprensión del modo en que otros perciben las acciones y los comportamientos en el entorno de la TIC y escuchar a otros sobre lo que consideran las amenazas y los riesgos más significativos.

7. Algunos Estados expresaron su preocupación por el desarrollo o uso de las capacidades de las TIC para fines incompatibles con el objetivo de mantener la paz y la seguridad internacionales. Algunos expresaron su preocupación por el hecho de que las características del entorno de las TIC puedan alentar medidas unilaterales en lugar de la solución de controversias por medios pacíficos. Algunos Estados señalaron su preocupación por el desarrollo de capacidades de TIC para fines militares y de otro tipo que puedan socavar la paz y la seguridad internacionales. Otros Estados señalaron que la amenaza radica en que un Estado utilice esas capacidades de forma contraria a sus obligaciones en virtud del derecho internacional. También se expresó inquietud por la acumulación de vulnerabilidades y la falta de transparencia y de procesos definidos para comunicarlas, la explotación de funciones ocultas perniciosas, la integridad de las cadenas de suministro mundiales de TIC y la garantía de la seguridad de los datos. Algunos Estados expresaron preocupación por la posibilidad de que las TIC se pudieran utilizar para interferir en sus asuntos internos, entre otras cosas mediante operaciones de información y campañas de desinformación. Se expresó especial preocupación por los esfuerzos encaminados a aumentar la automatización y la autonomía en las operaciones de TIC y por las actividades que pudieran dar lugar a una reducción o interrupción de la conectividad, a una intensificación no deseada de la tensión o a repercusiones negativas para terceros. Algunos Estados también indicaron la falta de claridad sobre las responsabilidades del sector privado como motivo de preocupación en sí mismo.

8. Se subrayó que las medidas para promover un comportamiento responsable de los Estados deben seguir siendo tecnológicamente neutrales y que lo que resultaba preocupante era el uso indebido de las tecnologías y no las tecnologías en sí mismas. Se reconoció que, si bien los avances tecnológicos y las nuevas aplicaciones pueden ofrecer oportunidades de desarrollo, también pueden ampliar los ámbitos de ataque, aumentar las vulnerabilidades en el entorno de la TIC o utilizarse para realizar nuevas actividades malintencionadas. En este sentido, se destacaron determinadas tendencias y avances tecnológicos, como el progreso en el aprendizaje automático y la informática cuántica; la ubicuidad de los dispositivos conectados (“Internet de las cosas”); los nuevos modos de almacenar y acceder a los datos mediante registros descentralizados y la computación en la nube; y la expansión de los macrodatos y los datos personales digitalizados.

Derecho internacional

9. Guiados por el mandato del Grupo, y con el objetivo de mantener la paz y la estabilidad y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico, así como de promover entendimientos comunes, los Estados mantuvieron un intercambio de opiniones sobre la forma en que el derecho internacional es pertinente a la dimensión de la seguridad internacional de las TIC.

10. En sus discusiones, los Estados recordaron que el derecho internacional, y en particular la Carta de las Naciones Unidas en su totalidad, era aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en el entorno de la TIC. A este respecto, los Estados subrayaron la necesidad de tomar las disposiciones necesarias para evitar que se adopte cualquier medida que no esté en consonancia con la Carta de las Naciones Unidas y el derecho internacional, que entorpezca el desarrollo social y económico pleno de la población de los países afectados y menoscabe su bienestar. Asimismo, se destacó la necesidad de comprender mejor la forma en que el derecho internacional era aplicable al uso de la TIC por los Estados.

11. Los principios específicos del derecho internacional que se reafirmaron incluyen, entre otros, la soberanía de los Estados; 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 renuncia a recurrir, en las relaciones internacionales, a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o de 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.

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

13. También se observó que en virtud del derecho internacional consuetudinario, las responsabilidades de los Estados con respecto a los hechos internacionalmente ilícitos se extienden a su uso de las TIC.

14. Se recordó también que los Estados no deben recurrir a intermediarios para cometer actos internacionalmente ilícitos utilizando las TIC, y deben tratar de que ningún agente no estatal, siguiendo instrucciones de un Estado o bajo su control, utilice su territorio para cometer esos actos. También se aludió a la responsabilidad de los Estados con respecto a las entidades que son propiedad de otro Estado o están bajo el control de este.

15. Se recordó 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 podría ser insuficiente en sí mismo para atribuir la actividad a ese Estado, y que las acusaciones vertidas contra los Estados de que han organizado y llevado a cabo hechos ilícitos deben fundamentarse. Algunos Estados destacaron la importancia de las pruebas auténticas, fiables y adecuadas en este contexto.

16. Algunos Estados expresaron la opinión de que el derecho internacional vigente, complementado por las normas voluntarias no vinculantes que reflejan el consenso entre los Estados, es suficiente en la actualidad para abordar el uso de las TIC por los

Estados. También se propuso que los esfuerzos se centraran en llegar a un entendimiento común sobre cómo se aplica el marco normativo ya acordado mediante la formulación de orientación adicional y puede ponerse en práctica si mejora la implementación por todos los Estados. Al mismo tiempo, otros Estados opinaron que, debido a que el entorno de las amenazas evolucionaba rápidamente y el riesgo era considerable, se necesitaba un marco jurídicamente vinculante y convenido internacionalmente sobre las TIC. También se sugirió que un marco vinculante de ese tipo permitiría una implementación más eficaz de los compromisos a nivel mundial y una base más firme para que los agentes rindieran cuentas de sus actos. Los Estados subrayaron que el desarrollo de un marco jurídico internacional en el que abordar las cuestiones relacionadas con el uso de las TIC con repercusiones en la paz y la seguridad internacionales se debería hacer teniendo en cuenta las preocupaciones e intereses de todos los Estados, alcanzarse por consenso, y todo ello en el seno de las Naciones Unidas con la participación activa y en pie de igualdad de todos los Estados.

17. Se destacó que, si bien los instrumentos de derecho internacional vigentes no contienen referencias específicas al uso de las TIC en el contexto de la seguridad internacional, el derecho internacional puede desarrollarse progresivamente, entre otras cosas mediante la *opinio iuris* y la práctica de los Estados. Se mencionó la posibilidad de desarrollar paulatinamente medidas complementarias vinculantes de forma simultánea a la implementación de normas. Asimismo, se propuso un compromiso político como una posible vía para avanzar.

18. Al tiempo que se recordó que el derecho internacional, y en particular la Carta de las Naciones Unidas, era aplicable en el uso de las TIC, se destacó que aún no se han aclarado del todo ciertas cuestiones sobre dicha aplicación. Algunos Estados propusieron que dichas cuestiones incluyeran, entre otras, el tipo de actividad relacionada con las TIC que podría ser interpretada por otros Estados como una amenaza o uso de la fuerza (Artículo 2, 4) de la Carta) o que podría dar pie a un Estado a invocar su derecho inmanente de legítima defensa (Artículo 51 de la Carta). También incluyen cuestiones relacionadas con el modo en que los principios del derecho internacional humanitario, como los principios de humanidad, necesidad, proporcionalidad, distinción y precaución, son aplicables a las operaciones de la TIC. En este sentido, algunos Estados observaron que las discusiones sobre la aplicabilidad del derecho internacional humanitario al uso de las TIC por los Estados debían abordarse con prudencia. Los Estados señalaron que era necesario seguir estudiando estos importantes temas en futuras discusiones.

19. Por otra parte, en cuanto al camino a seguir, se propuso, como primer paso clave para aclarar y seguir desarrollando entendimientos comunes, que los Estados aumentaran sus intercambios y discusiones a fondo sobre el modo en que se aplica el derecho internacional al uso de las TIC por los Estados. Se señaló que esos intercambios en sí mismos podían ser una importante medida de fomento de la confianza. Además, algunos Estados propusieron varias formas de compartir voluntariamente sus posturas nacionales sobre la aplicabilidad del derecho internacional, en particular utilizando el informe anual del Secretario General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional[9], el Cyber Policy Portal del Instituto de las Naciones Unidas de Investigación sobre el Desarme o una encuesta sobre la práctica nacional en la aplicación del derecho internacional. También se destacó el progreso alcanzado en los acuerdos regionales y de otra índole para intercambiar opiniones y desarrollar percepciones comunes sobre el modo de aplicar el derecho internacional.

[9] A/RES/75/32.

20. Desde la óptica del mantenimiento de la paz y la prevención de los conflictos, los Estados afirmaron la necesidad de solucionar las controversias por medios pacíficos y abstenerse de la amenaza o el uso de la fuerza. En este contexto, los Estados recordaron los órganos, mecanismos e instrumentos existentes para la prevención y el arreglo pacífico de controversias. Algunos Estados sugirieron que la elaboración de un enfoque y un entendimiento comunes y universalmente aceptados, a nivel técnico, en torno a las causas de los incidentes vinculados a la TIC, bajo los auspicios de las Naciones Unidas y mediante el intercambio de buenas prácticas, teniendo en cuenta el respeto al principio de la soberanía de los Estados, podría aumentar la rendición de cuentas y la transparencia y contribuir a apoyar el recurso jurídico para las personas perjudicadas por actos malintencionados.

Normas, reglas y principios de comportamiento responsable de los Estados

21. En sus discusiones en el Grupo de Trabajo, los Estados recordaron que las normas voluntarias no vinculantes sobre el comportamiento responsable de los Estados no alteran ni sustituyen el derecho internacional, sino que deben considerarse compatibles con él y con los propósitos y principios de las Naciones Unidas, incluidos el mantenimiento de la paz y la seguridad internacionales y la promoción de los derechos humanos. Los Estados también recordaron la resolución 2131 (XX) de la Asamblea General, de 1965, titulada “Declaración sobre la inadmisibilidad de la intervención en los asuntos internos de los Estados y protección de su independencia y soberanía”.

22. Los Estados recordaron que la resolución 73/27 de la Asamblea General presenta un conjunto de 13 reglas, normas y principios para el comportamiento responsable de los Estados y, entre otras cosas, también afirma las 11 normas voluntarias y no vinculantes “consagradas en los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2013 y 2015, aprobados por consenso y recomendados en la resolución 71/28”[10].

23. Se subrayó la necesidad de dar a conocer las normas vigentes y apoyar su puesta en práctica paralelamente al desarrollo de nuevas normas. Los Estados destacaron la necesidad de ofrecer orientación sobre la puesta en práctica de las normas. A ese respecto, los Estados pidieron que se compartieran y difundieran las buenas prácticas y experiencias sobre la implementación de las normas. Se propusieron distintos enfoques de cooperación, como una hoja de ruta elaborada por los Estados, para contribuir a sus actividades de implementación, así como encuestas voluntarias para compartir experiencias y buenas prácticas.

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

25. En las discusiones se formularon propuestas para seguir desarrollando las normas vigentes. Los Estados reiteraron que era igualmente importante proteger todas las infraestructuras críticas que apoyan los servicios esenciales para el público, que deben incluir las instalaciones médicas y sanitarias. También llamaron la atención

[10] A/RES/73/27, párrafo 1.

sobre la importancia de cooperar para proteger infraestructuras críticas por las que se prestan servicios a través de las fronteras o jurisdicciones, dado el impacto potencial de cualquier daño a dichas infraestructuras, así como la importancia de garantizar la disponibilidad e integridad general de Internet. Además, se recordó la resolución 64/211 de la Asamblea General, titulada "Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales"[11]. Los Estados también propusieron que se siguiera velando por la integridad de la cadena de suministro de las TIC, expresando su preocupación por la creación de funciones ocultas perniciosas en los productos de las TIC y la responsabilidad de notificar a los usuarios cuando se detecten vulnerabilidades importantes. Además, los Estados expresaron su preocupación por la acumulación de vulnerabilidades. Algunos Estados propusieron formular reglas y normas internacionales objetivas sobre la seguridad de la cadena de suministro.

26. Atendiendo a lo expuesto en el párrafo anterior, las propuestas escritas formuladas por los Estados en el Grupo de Trabajo sobre la elaboración de las normas existentes, la orientación sobre su aplicación y las normas nuevas figuran en anexo al presente resumen.

27. También se señaló la propuesta, presentada en 2015, de crear un código de conducta internacional para la seguridad de la información[12].

28. Algunos Estados reconocieron la necesidad de alentar y apoyar más iniciativas regionales y alianzas con otras partes interesadas, como el sector privado y la comunidad técnica, sobre la implementación de normas. Estas alianzas podrían establecerse, por ejemplo, para garantizar iniciativas sostenibles de desarrollo de la capacidad con el fin de reducir las diferencias en las capacidades de implementación. A este respecto, los Estados recordaron el párrafo 1.13 de la resolución 73/27 de la Asamblea General, que, entre otras cosas, destaca que "los Estados deben alentar al sector privado y a la sociedad civil a desempeñar un papel adecuado para aumentar la seguridad de las TIC y en su utilización, incluida la seguridad de la cadena de suministro de productos y servicios de las TIC". Los Estados señalaron la importancia de las medidas de divulgación y cooperación para asegurar que las distintas partes interesadas, incluidos los sectores público y privado y la sociedad civil, cumplan sus responsabilidades en el uso de las TIC.

Medidas de fomento de la confianza

29. En sus discusiones en el Grupo de Trabajo, los Estados señalaron que las medidas de fomento de la confianza recomendadas en los informes del Grupo de Expertos aprobados por consenso siguen siendo pertinentes. Además destacaron varias de ellas que requerían atención prioritaria, como el diálogo y los intercambios de información voluntarios de carácter periódico sobre las amenazas actuales y emergentes, las políticas nacionales, los marcos legislativos, la doctrina nacional, las opiniones nacionales sobre el modo en que el derecho internacional es aplicable al uso de las TIC por los Estados y los enfoques nacionales a la hora de definir la infraestructura crítica y categorizar los incidentes vinculados a la TIC. Se sugirió que el intercambio de buenas prácticas en los enfoques de la ciencia forense digital y la investigación de los ciberincidentes malintencionados podrían contribuir a aumentar la cooperación y desarrollar la capacidad. También se destacó la importancia de desarrollar una percepción común de los conceptos y la terminología como medida práctica para impulsar la cooperación internacional y fomentar la confianza. Entre

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

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

otras medidas de este tipo figuraban el desarrollo de orientación sobre la aplicación de las medidas de fomento de la confianza, la capacitación del cuerpo diplomático, el intercambio de lecciones aprendidas sobre el establecimiento y el ejercicio de vías de comunicación seguras para las crisis, los intercambios de personal, los ejercicios basados en situaciones en el ámbito de las políticas y los ejercicios operacionales en el plano técnico entre los equipos informáticos de respuesta de emergencia o los equipos de respuesta a incidentes de ciberseguridad. Las medidas nacionales de transparencia, como la de compartir voluntariamente las respuestas a una encuesta sobre la aplicación o la emisión de declaraciones nacionales de adhesión al marco para el comportamiento responsable de los Estados se sugirieron como vías alternativas para fomentar la confianza con respecto a las intenciones y los compromisos de los Estados.

30. Teniendo en cuenta las experiencias de los órganos regionales en el establecimiento y mantenimiento de redes de puntos de contacto, y sobre la base de las redes ya existentes, se debatió la viabilidad de establecer un directorio mundial central de puntos de contacto. Al mismo tiempo, se observó que la seguridad de este directorio, así como sus modalidades operacionales, serían fundamentales para su eficacia, como también lo era evitar que los acuerdos se duplicaran o fueran excesivamente detallados. Asimismo, se destacó la importancia de realizar ejercicios periódicos en una red de puntos de contacto, ya que puede ayudar a mantener la preparación y la capacidad de respuesta y garantizar que los directorios de puntos de contacto se mantengan al día.

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

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

Creación de capacidad

33. En sus discusiones en el Grupo de Trabajo, los Estados pusieron de relieve la importancia que podía tener el desarrollo de la capacidad a la hora de empoderar a todos los Estados a participar plenamente en las deliberaciones internacionales sobre el marco para el comportamiento responsable de los Estados y, al mismo tiempo, contribuir a alcanzar compromisos comunes, como la Agenda 2030 para el Desarrollo

Sostenible [13]. En este sentido, los Estados destacaron la necesidad de asignar suficientes recursos financieros y humanos a los programas de desarrollo de la capacidad.

34. Se destacó la importante labor que han realizado otros agentes, incluidas las organizaciones internacionales, los órganos regionales y subregionales, la sociedad civil, el sector privado, el mundo académico y los órganos técnicos especializados, para desarrollar la capacidad en materia de TIC, y alentaron a reflexionar sobre el modo de fomentar la cooperación, la sostenibilidad, la eficacia y la reducción de la duplicación entre estas actividades.

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

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

37. Los Estados llamaron la atención sobre la brecha digital de género y pidieron medidas específicas en los planos nacional e internacional para abordar las cuestiones de la igualdad de género y la participación significativa de las mujeres en los debates y los programas de desarrollo de la capacidad internacionales relativos a las TIC y la

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

seguridad internacional, en particular recopilando datos desglosados por género. Se reconocieron los programas que han facilitado la participación de las mujeres en debates multilaterales sobre la seguridad de la TIC. Asimismo, se hizo hincapié en la necesidad de reforzar los vínculos entre este tema y la agenda de las Naciones Unidas sobre las mujeres, la paz y la seguridad.

38. Los Estados señalaron que había muchos obstáculos que impiden el desarrollo de la capacidad o reducen su eficacia, e indicaron como aspectos especialmente preocupantes la coordinación y complementariedad insuficientes a la hora de determinar y ejecutar las actividades de desarrollo de la capacidad. También se expresaron preocupaciones prácticas en lo relativo a la determinación de las necesidades de desarrollo de la capacidad, la rapidez de la respuesta a las solicitudes de asistencia para el desarrollo de la capacidad y el diseño, la ejecución, la sostenibilidad y la accesibilidad de las actividades de desarrollo de la capacidad, así como la falta de criterios específicos para medir su repercusión. En muchos contextos, la falta de recursos humanos, financieros y técnicos suficientes impide las actividades de creación de capacidad y el progreso necesario para reducir la brecha digital. Una vez que se ha desarrollado la capacidad, algunos países se enfrentan al reto de retener el talento en un mercado competitivo para los profesionales de las TIC. Los Estados mencionaron que otra dificultad era la falta de acceso a las tecnologías relacionadas con la seguridad de la TIC.

Diálogo institucional periódico

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

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

41. Algunos Estados formularon una propuesta concreta sobre el establecimiento de un programa de acción que promueva un comportamiento responsable de los Estados en el ciberespacio con miras a crear un foro permanente de las Naciones Unidas para examinar el uso de las TIC por los Estados en el contexto de la seguridad internacional. Se propuso que el programa de acción constituyera un compromiso político de los Estados con las recomendaciones, normas y principios acordados; se organizaran reuniones periódicas centradas en la implementación; permitiera intensificar la cooperación técnica y la creación de capacidad entre los Estados; y se celebraran conferencias periódicas de examen. En la propuesta de programa de acción también se previeron la participación y las consultas amplias.

42. Los Estados tomaron nota de la creación, mediante la resolución 75/240, de 31 de diciembre de 2020, de un nuevo grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021-2025, que iniciará sus actividades una vez concluida la labor del Grupo de Trabajo de

Composición Abierta establecido en virtud de la resolución 73/27 y examinará sus resultados.

43. Los Estados también expresaron su deseo de que la comunidad internacional vuelva en última instancia a un proceso único basado en el consenso bajo los auspicios de las Naciones Unidas. A este respecto, observaron que los distintos formatos propuestos para el diálogo no eran necesariamente excluyentes entre sí. Se sugirió que los distintos formatos podían ser complementarios o fusionarse para aprovechar las características particulares de cada uno y reducir la duplicación de esfuerzos.

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

45. Si bien los Estados reconocieron su función y responsabilidad particulares en relación con la seguridad nacional e internacional, también subrayaron la importante contribución que supone el comportamiento responsable de otros agentes al logro de un entorno abierto, seguro, accesible y pacífico en la esfera de la TIC. A ese respecto, se señaló que aumentar la cooperación y las alianzas entre múltiples partes interesadas puede facilitar la creación de un entorno más resiliente y seguro para estas tecnologías.

Anexo al resumen de la Presidencia

Propuestas específicas de texto a incluir en relación con el tema del programa titulado “Reglas, normas y principios” presentadas por escrito por las delegaciones

Teniendo en cuenta que en sus contribuciones escritas muchas delegaciones hicieron referencia a normas existentes, lo que sigue solo refleja las propuestas adicionales.

Armenia

- Los Estados se abstendrán de realizar cualquier acción que pueda suponer un intento de disrupción de la integridad de las infraestructuras críticas y las actividades gubernamentales, y ofrecerán por canales seguros las aclaraciones oportunas para evitar una posible escalada.

Australia, Estados Unidos de América, Estonia, Japón, Kazajstán y Chequia

Texto de orientación sobre la implementación de las normas 13 f) y g) de 2015

- Al proporcionar orientación para la implementación de estas normas, los Estados deben tener en cuenta que al destacar determinados sectores como infraestructura crítica no se pretende establecer una lista exhaustiva ni afecta a la designación o no a nivel nacional de ningún otro sector, ni se aprueba implícitamente la actividad malintencionada contra una categoría no especificada.

- El Grupo de Trabajo preparó su informe en el contexto de la pandemia de COVID-19. En esas circunstancias, el Grupo de Trabajo subrayó que todos los Estados consideraban que los servicios y las instalaciones médicas eran infraestructuras críticas a efectos de las normas f) y g).

Belarús

• Los Estados deben reafirmar sus compromisos con el principio de que cesarán la militarización de las TIC existentes y la creación de nuevas TIC específicamente diseñadas para dañar los recursos de información, la infraestructura y las instalaciones críticas de otros países.

Canadá

Texto orientativo de normas propuesto para incluir en el párrafo 41

Mientras que las normas del Grupo de Expertos de 2015 articulan las acciones que los Estados deben o no deben tomar, los Estados subrayaron la necesidad de orientar sobre cómo ponerlas en práctica, y ofrecieron la siguiente orientación sobre estas normas. El Grupo de Trabajo entiende que tanto las normas como las orientaciones se entienden sin perjuicio de los derechos y obligaciones de los Estados en virtud del derecho internacional, y no los modifican ni reducen en modo alguno.

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 (2015 ¶13 a)).

i. Esta norma es de carácter general. La implementación de toda la variedad de normas, así como la orientación específica que se ofrece a continuación, contribuirá a la puesta en práctica de esta norma. Los Estados deben adoptar un enfoque de colaboración mutua y con las partes interesadas no gubernamentales, incluidas la industria, el mundo académico y la sociedad civil.

ii. Para ello, los Estados deben, según el caso, y cuando sea posible:

- Adoptar e implementar estrategias nacionales de ciberseguridad amplias. Siempre que sea posible, promover la cooperación internacional en materia de ciberseguridad

- Establecer y mantener funciones de respuesta a incidentes, por ejemplo, equipos informáticos de respuesta de emergencia, que sean capaces de coordinar, compartir buenas prácticas y cooperar en la respuesta a incidentes de TIC.

- Publicar declaraciones de que actuarán de conformidad con el marco de comportamiento responsable de los Estados en el ciberespacio, como se articula en el informe del Grupo de Trabajo de 2015

- Participar en iniciativas regionales y bilaterales destinadas a desarrollar e implementar medidas de fomento de la confianza.

iii. Se alentará a los Estados miembros a que recopilen y simplifiquen la información que presenten sobre su implementación de las normas aceptadas.

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 (2015 ¶13 b)).

i. Los Estados podrían establecer las estructuras, las políticas, los procesos y los mecanismos de coordinación nacionales necesarios para facilitar un examen minucioso de los incidentes graves relacionados con las TIC y determinar las respuestas adecuadas.

ii. Una vez que esas estructuras y procesos estén en marcha, los Estados podrían elaborar plantillas de la gravedad de los incidentes de TIC con el fin de evaluar y valorar dichos incidentes.

iii. La transparencia y la armonización de estas plantillas por parte de las organizaciones regionales podría garantizar la homogeneidad en la forma en que los Estados consideran los incidentes de TIC y mejorar la comunicación entre los Estados. En la medida de lo posible, las plantillas deberían ajustarse a las prácticas existentes y evitar la duplicación.

iv. Al considerar toda la información pertinente en el caso de un incidente de TIC, los Estados deberían investigar los posibles efectos en función del género, y trabajar de forma inclusiva con todas las partes interesadas para comprender el contexto más amplio de un incidente relacionado con las TIC, incluido su impacto en el disfrute de los derechos de las mujeres y la comunidad LGBT.

v. Los Estados deberían considerar el efecto de los incidentes relacionados con las TIC en los derechos humanos, incluidos los derechos a la libertad de expresión, asociación y reunión pacífica, el derecho a no sufrir injerencias arbitrarias o ilegales en la vida privada, así como los derechos de las personas con discapacidad.

vi. Los Estados deberían reconocer que las respuestas a los incidentes de seguridad suelen requerir la participación de diversas partes interesadas, no solo de los equipos informáticos de respuesta de emergencia y de respuesta a incidentes de ciberseguridad nacionales, y mejorar la colaboración mediante la formación y el desarrollo de capacidades con todos los grupos interesados. Además deberían fomentar la capacitación en seguridad digital y otras actividades de creación de capacidad y asistencia por parte de las partes interesadas, incluida la sociedad civil, con el fin de prevenir incidentes de seguridad, en particular en las comunidades vulnerables y otros usuarios en riesgo.

c. Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC (2015 ¶13 c)).

i. Con respecto a la implementación de esta norma:

- Si un Estado detecta ciberactividad malintencionada procedente del territorio o de la ciberinfraestructura de otro Estado, el primer paso podría ser notificar a dicho Estado. Los equipos informáticos de respuesta de emergencia son cruciales para detectar este tipo de actividades.

- Dado que los incidentes relacionados con las TIC pueden provenir o implicar a terceros Estados, se entiende que la notificación a un Estado no implica que dicho Estado sea responsable del incidente.

- El Estado notificado debe acusar recibo a través del punto de contacto nacional correspondiente.

- Cuando un Estado tenga conocimiento de que su territorio o su ciberinfraestructura se está utilizando para cometer un hecho internacionalmente ilícito mediante el uso de las TIC que pueda tener consecuencias adversas graves en un Estado, el primer Estado debería intentar adoptar medidas razonables, disponibles

y practicables dentro de su territorio y sus capacidades, de conformidad con sus obligaciones en virtud del derecho interno y el derecho internacional, para que cese el hecho internacionalmente ilícito o para mitigar sus consecuencias.

- Un Estado puede tener conocimiento de un acto de ese tipo tras la notificación de un Estado afectado. Dicha notificación debe realizarse de buena fe y debe ir acompañada de información justificativa. Dicha información puede consistir en compartir posibles indicadores de compromiso, como la dirección IP y los ordenadores utilizados para los actos malintencionados de las TIC e información sobre el programa malicioso.

- Se debe alentar a los Estados a que se aseguren de que los agentes no estatales, incluido el sector privado, no realicen actividades malintencionadas con las TIC para sus propios fines o los de los agentes estatales o no estatales en detrimento de terceras partes, incluidas las situadas en el territorio de otro Estado. Este objetivo podría alcanzarse trabajando con el sector privado para definir las acciones permitidas utilizando un enfoque basado en los riesgos y desarrollar herramientas concretas como procesos de certificación, guías de mejores prácticas, mecanismos de respuesta a incidentes y, según proceda, normativas nacionales.

- Esta norma no debería interpretarse como la exigencia de que un Estado controle de forma proactiva todas las TIC en su territorio, o que tome otras medidas preventivas.

ii. Un Estado que tenga conocimiento de actividades perjudiciales de TIC procedentes de su territorio, pero que carezca de capacidad de respuesta, puede optar por solicitar asistencia a otros Estados, incluso a través de los modelos estándar de solicitud de asistencia.

- En tales casos, se puede solicitar la asistencia de otros Estados o de una entidad privada, que si se proporciona debe hacerse con arreglo a la legislación nacional y el derecho internacional de los derechos humanos.

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. Los Estados tal vez podrían considerar si es necesario elaborar nuevas medidas a este respecto (2015 ¶13 d))

i. Al aplicar esta norma, los Estados deben:

- Considerar, según proceda, prestar apoyo a la labor de la Comisión de Prevención del Delito y Justicia Penal de las Naciones Unidas, incluso renovando el mandato del Grupo de Expertos intergubernamental de composición abierta, y apoyando los esfuerzos que está realizando para estudiar de manera exhaustiva el problema de la ciberdelincuencia.

- Apoyar los esfuerzos de la Oficina de las Naciones Unidas contra la Droga y el Delito para que continúe prestando a los Estados Miembros, cuando se le solicite y con arreglo a las necesidades nacionales, asistencia técnica y creación sostenible de capacidad para hacer frente a la ciberdelincuencia, por conducto del Programa Mundial contra el Delito Cibernético y, entre otras cosas, sus oficinas regionales, en relación con la prevención, detección, investigación y enjuiciamiento de la ciberdelincuencia en todas sus formas, reconociendo que la cooperación con los Estados Miembros, las organizaciones internacionales y regionales pertinentes, el

sector privado, la sociedad civil y otras partes interesadas pertinentes puede facilitar esta actividad.

- Implementar las medidas existentes de forma coherente con sus obligaciones y considerar la adopción de nuevas medidas, como la aprobación de legislación nacional para combatir la ciberdelincuencia, de conformidad con las obligaciones de los Estados en materia de derechos humanos y asegurando las garantías judiciales.

e. Los Estados, para garantizar la utilización segura de las TIC, deben respetar 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 (2015 ¶13 e))

i. Los Estados deben:

- Cumplir con sus obligaciones en virtud del derecho nacional e internacional, al considerar, elaborar o aplicar las políticas o la legislación nacional en materia de ciberseguridad o al diseñar y poner en marcha iniciativas o estructuras relacionadas con la ciberseguridad, incluidas medidas para garantizar la protección de todos los derechos humanos.

- Al hacerlo, incorporar las perspectivas de todas las partes interesadas y afectadas en las primeras etapas de la elaboración e implementación de las políticas de ciberseguridad con el fin de salvaguardar una consideración holística de las repercusiones de las medidas de ciberseguridad.

- Asegurar la intervención especialmente importante de la sociedad civil dado su papel de agente clave en la promoción del cumplimiento por los Estados de sus obligaciones y compromisos en materia de derechos humanos.

- Tener en cuenta que las personas tienen los mismos derechos en línea que fuera de ella, y que las mujeres y las personas pertenecientes a minorías y grupos vulnerables pueden experimentar amenazas diferentes en el contexto de los derechos humanos.

- Llevar a cabo auditorías de género de las políticas de ciberseguridad nacionales o regionales para determinar áreas de mejora.

- Considerar la incorporación de medidas para abordar las repercusiones de las TIC en los derechos humanos en sus planes de acción nacionales sobre empresas y derechos humanos.

f. Ningún Estado debería realizar o apoyar a sabiendas actividades de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que perjudiquen intencionadamente las infraestructuras críticas o dificulten de otro modo su utilización y funcionamiento que permita prestar servicios al público (2015 ¶13 f)).

i. Cada Estado determina qué infraestructuras o sectores considera críticos, de conformidad con las prioridades nacionales y los métodos de categorización de las infraestructuras críticas. Algunos ejemplos de sectores de infraestructuras críticas que prestan servicios públicos esenciales pueden ser la energía, el agua, el saneamiento, la salud, la educación, las finanzas, el transporte, las telecomunicaciones y las organizaciones de respuesta a las crisis. La infraestructura crítica también puede incluir la infraestructura técnica esencial para las elecciones, los referendos o los

plebiscitos y la infraestructura técnica esencial para la disponibilidad o integridad general de Internet. El hecho de que tales infraestructuras se citen como ejemplos no excluye en absoluto la designación por los Estados de otras infraestructuras críticas, ni aprueba las actividades malintencionadas contra las categorías de infraestructuras críticas no especificadas anteriormente.

ii. Los Estados deberían considerar los efectos potencialmente perjudiciales de sus actividades de TIC en la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet.

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 (2015 ¶13 g)).

i. Con el fin de contribuir a una cultura global de ciberseguridad, los Estados deben considerar, según proceda, el intercambio de información sobre las mejores prácticas para proteger las infraestructuras críticas, incluidos todos los elementos determinados en esta resolución y los siguientes:

- Requisitos de seguridad de referencia
- Procedimientos de notificación de incidentes;
- Herramientas y metodologías de gestión de incidentes;
- Resiliencia ante emergencias; y
- Enseñanzas extraídas de incidentes anteriores.

ii. Las medidas de creación de capacidad y de otro tipo para construir una cultura mundial de ciberseguridad deben elaborarse de forma inclusiva y tratar de abordar las dimensiones de género de la ciberseguridad.

iii. Dada la naturaleza variada y distribuida de la propiedad de las infraestructuras críticas, los Estados deben, según proceda, y en consulta con las partes interesadas pertinentes, promover normas mínimas para la seguridad de las infraestructuras críticas y fomentar la cooperación con el sector privado, el mundo académico y la comunidad técnica en los esfuerzos de protección de la infraestructura crítica.

iv. Los Estados deben, según proceda, participar en iniciativas voluntarias de evaluación de riesgos y planificación de la continuidad de las operaciones (resiliencia, recuperación y contingencias) que impliquen a otras partes interesadas y que tengan por objeto mejorar la seguridad y la resiliencia de la infraestructura crítica que proporciona servicios a nivel regional o internacional frente a las amenazas existentes y emergentes.

v. Los esfuerzos para proteger la infraestructura crítica de información deben llevarse a cabo teniendo en cuenta las leyes nacionales aplicables relativas a la protección de la privacidad y otra legislación pertinente.

vi. Al proporcionar orientación para la implementación de las normas f) y g), los Estados señalan que al destacar determinados sectores como infraestructura crítica no se pretende establecer una lista exhaustiva ni afecta a la designación o no a nivel nacional de ningún otro sector, ni se aprueba implícitamente la actividad malintencionada contra una categoría no especificada.

vii. El Grupo de Trabajo subrayó que todos los Estados consideraban que la infraestructura sanitaria, los servicios y las instalaciones médicas eran

infraestructuras críticas a efectos de las normas f) y g). La necesidad de afirmar la protección de la infraestructura sanitaria cobró relevancia dado que el Grupo de Trabajo elaboró su informe en el contexto de la pandemia de COVID-19.

h. Los Estados deben atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales sean 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 (2015 ¶13 h)).

i. La implementación de esta norma supone examinar las solicitudes de asistencia apropiadas y considerar la naturaleza de la asistencia que puede ofrecerse en el momento oportuno. Los Estados que reciban una solicitud de asistencia apropiada tras un incidente de TIC deben considerar, cuando sea posible, las siguientes medidas razonables y apropiadas:

- Acusar recibo a través del punto de contacto nacional correspondiente.

- Determinar, en el momento oportuno, si tiene la capacidad y los recursos para prestar la asistencia solicitada. Esto puede incluir seleccionar expertos en el país de una serie de partes interesadas.

- En su respuesta inicial, indicar la naturaleza, el alcance y las condiciones de la asistencia que podría prestarse, incluido un plazo para hacerlo.

- En caso de que se acuerde la asistencia, prestarla rápidamente.

- Garantizar que las solicitudes de asistencia, incluidos los procesos y recursos pertinentes, como marcos y plantillas, y las respuestas sean acordes con las obligaciones en materia de derechos humanos.

ii. La implementación de esta norma se vería facilitada por la existencia previa de estructuras y mecanismos nacionales, incluido un punto de contacto nacional, plantillas para las solicitudes de asistencia y confirmación de la asistencia que se ha de prestar, y por la creación de capacidades y asistencia técnica específicas. Las iniciativas de cooperación bilateral y multilateral, las organizaciones y los foros internacionales y regionales pueden desempeñar una función en su desarrollo.

Los enfoques que podrían contribuir positivamente a la implementación de esta norma podrían incluir: una mayor colaboración de los sectores público y privado y las organizaciones de la sociedad civil, a nivel nacional e internacional, especialmente para tomar medidas preventivas; la mejora de la capacidad de los equipos de respuesta a incidentes mediante un enfoque adaptado al desarrollo de la cibercapacidad; y formación especializada para crear cibercapacidad a todos los niveles de los Estados y la sociedad.

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. También 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 (2015 ¶13 i)).

i. Para aplicar esta norma, los Estados deben:

- Adoptar medidas, incluso a través de los foros existentes, para evitar la proliferación de herramientas y técnicas de TIC malintencionadas. Para ello, los Estados deben fomentar las actividades legítimas de las comunidades de investigación, el mundo académico, la industria, las fuerzas del orden, los equipos informáticos de respuesta de emergencia y de respuesta a incidentes de ciberseguridad y otros organismos de ciberprotección al garantizar la seguridad de sus sistemas de TIC.

- Considerar el intercambio de información sobre las vulnerabilidades relacionadas con las TIC y/o las funciones ocultas perniciosas en los productos de las TIC.

- Trabajar para implementar controles de seguridad, basados en la gestión de riesgos.

j. Los Estados deben alentar la divulgación responsable de información sobre las vulnerabilidades de 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 (2015 ¶13 j)).

i. Para aplicar esta norma, los Estados deberían:

- Establecer estructuras nacionales que permitan una notificación y gestión responsables de las vulnerabilidades de las TIC;

- Fomentar mecanismos de coordinación adecuados entre las entidades de los sectores público y privado.

ii. Además, y para evitar malentendidos o interpretaciones erróneas, incluidas las derivadas de la no divulgación de información sobre vulnerabilidades de las TIC potencialmente perjudiciales, se alienta a los Estados a compartir, según proceda, en la mayor medida posible, la información técnica sobre incidentes graves de TIC, utilizando los mecanismos existentes de coordinación entre equipos informáticos de respuesta de emergencia, así como los mecanismos establecidos por las organizaciones regionales (como las redes de puntos de contacto). Los Estados deben garantizar que dicha información se gestiona de forma responsable y en coordinación con otras partes interesadas, según corresponda.

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 debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada. (2015 ¶13 k)).

China

• Los Estados deben comprometerse a no utilizar las TIC y las redes de TIC para llevar a cabo actividades contrarias a la tarea de mantener la paz y la seguridad internacionales.

La soberanía del Estado en el ciberespacio

- Los Estados deben ejercer su jurisdicción sobre la infraestructura y los recursos de las TIC, así como sobre las actividades relacionadas con estas dentro de sus territorios.

- Los Estados tienen derecho a elaborar políticas públicas relacionadas con las TIC en consonancia con las circunstancias nacionales para gestionar sus propios asuntos de TIC y proteger los intereses legítimos de sus ciudadanos en el ciberespacio.

- Los Estados deben abstenerse de utilizar las TIC para interferir en los asuntos internos de otros Estados y socavar su estabilidad política, económica y social.

- Los Estados deben participar en la gestión y distribución de los recursos internacionales de Internet en igualdad de condiciones.

Protección de infraestructura crítica

- Los Estados tienen derechos y responsabilidades en cuanto a la protección jurídica de sus infraestructuras críticas de TIC contra los daños resultantes de amenazas, interferencias, ataques y sabotajes.

- Los Estados deben comprometerse a que se abstendrán de lanzar ciberataques contra las infraestructuras críticas de otros Estados.

- Los Estados no deben valerse de ventajas políticas y técnicas para socavar la seguridad e integridad de las infraestructuras críticas de otros Estados.

- Los Estados deben aumentar los intercambios de normas y mejores prácticas en materia de protección de infraestructuras críticas y alentar a las empresas a realizar dichos intercambios.

Seguridad de los datos

- Los Estados deben adoptar un enfoque equilibrado con respecto al avance técnico, el desarrollo empresarial y la salvaguarda de la seguridad nacional y los intereses públicos.

- Los Estados tienen el derecho y la obligación de garantizar la seguridad de la información personal y los datos importantes para su seguridad nacional, el orden público, la seguridad económica y la estabilidad social.

- Los Estados no realizarán ni apoyarán el espionaje facilitado por las TIC de otros Estados, incluida la vigilancia a gran escala y el robo de datos importantes e información personal.

- Los Estados deben prestar la misma atención al desarrollo que a la seguridad, y promover el flujo de datos legal, ordenado y libre. Los Estados deben facilitar el intercambio de buenas prácticas y la cooperación en este sentido.

Seguridad de la cadena de suministro

- Los Estados no deben explotar su posición dominante en las TIC, que incluye el dominio de los recursos, las infraestructuras críticas y las tecnologías básicas de TIC, los bienes y servicios de las TIC, para socavar el derecho de otros Estados al control independiente de los bienes y servicios de las TIC, así como su seguridad.

• Los Estados deben prohibir a los proveedores de bienes y servicios de TIC la obtención ilegal de datos de los usuarios, y el control y la manipulación de los dispositivos y sistemas de los usuarios mediante la instalación de puertas traseras en los bienes. Los Estados deben prohibir también a los proveedores de bienes y servicios de TIC perseguir intereses ilegítimos aprovechándose de la dependencia de los usuarios de sus productos, u obligando a los usuarios a actualizar sus sistemas y dispositivos. Además, deben solicitar a los proveedores de bienes y servicios de TIC que se comprometan a que sus asociados en la cooperación y los usuarios sean notificados a tiempo si se detectan vulnerabilidades graves en sus productos.

• Los Estados deben comprometerse a mantener un entorno empresarial equitativo, justo y no discriminatorio. Los Estados no deben utilizar la seguridad nacional como pretexto para restringir el desarrollo y la cooperación de las TIC y limitar el acceso al mercado de los productos de las TIC y la exportación de productos de alta tecnología.

Lucha contra el terrorismo

• Los Estados deben prohibir que las organizaciones terroristas utilicen Internet para crear sitios web, foros en línea y blogs para llevar a cabo actividades terroristas, incluida la elaboración, publicación, almacenamiento y difusión de documentos de audio y vídeo terroristas, la difusión de retórica e ideología terrorista violenta, la recaudación de fondos, el reclutamiento, la incitación a actividades terroristas, etc.

• Los Estados deben llevar a cabo intercambios de información y cooperación de los órganos de orden público para combatir el terrorismo. Por ejemplo, un Estado debe almacenar y recopilar oportunamente los datos y las pruebas en línea pertinentes a petición de otros Estados para casos de ciberterrorismo, prestar asistencia en la investigación y dar una respuesta rápida.

• Los Estados deben desarrollar una alianza de cooperación con las organizaciones internacionales, las empresas y los ciudadanos en la lucha contra el ciberterrorismo.

• Los Estados deben solicitar a los proveedores de servicios de Internet que corten el canal de difusión en línea de contenidos terroristas cerrando los sitios web y las cuentas de propaganda y borrando los contenidos terroristas y de extremismo violento.

Croacia, Eslovenia, Finlandia y Francia

• Se debe alentar a los Estados a que tomen medidas para evitar que los agentes no estatales, incluido el sector privado, realicen actividades de TIC para sus propios fines o los de otros agentes no estatales en detrimento de terceras partes, incluidas las situadas en el territorio de otro Estado.

• Este objetivo podría alcanzarse trabajando con el sector privado para definir las acciones permitidas utilizando un enfoque basado en los riesgos y desarrollar herramientas concretas como procesos de certificación, guías de mejores prácticas, mecanismos de respuesta a incidentes y, según proceda, normativas nacionales.

Cuba

Esta situación exige la implementación de regulaciones específicas complementarias al derecho internacional, dirigidas, entre otros, a los siguientes elementos igualmente importantes

- Impedir la aplicación de medidas unilaterales y contra los Estados que obstaculicen el acceso universal a los beneficios que ofrecen las TIC.
- Mitigar los efectos maliciosos de la atribución ante los ciberataques.
- Evitar la militarización del ciberespacio.
- Proteger mejor los datos privados de los ciudadanos promoviendo regulaciones internacionales al respecto.
- Complementar la legislación sobre ciberterrorismo para hacer frente a los incidentes y problemas de ciberseguridad, como los ciberataques. Definir por consenso lo que se entiende por ciberataque.
- Poner en marcha la aplicación, con mayor objetividad, de los principios del derecho internacional en este ámbito.

Chequia

- Los Estados no llevarán a cabo ni apoyarán a sabiendas cualquier ciberactividad que perjudique a los servicios o las instalaciones médicas, y deben adoptar medidas para proteger los servicios médicos de cualquier perjuicio[14].
- Es necesario cumplir con las obligaciones contraidas en virtud del derecho internacional de los derechos humanos al considerar, desarrollar y aplicar las políticas y la legislación nacional sobre ciberseguridad[15].
- Es necesario incorporar las perspectivas de todas las partes interesadas y afectadas en la primera etapa de la elaboración de las políticas de ciberseguridad con el fin de asegurar una consideración holística de las repercusiones de las medidas de ciberseguridad en los derechos humanos[16].

Ecuador

- Orientación sobre la norma 13 b) del Grupo de Expertos 2015[17]:

i) Los Estados podrían establecer las estructuras, las políticas, los procesos y los mecanismos de coordinación nacionales necesarios para facilitar un examen minucioso de los incidentes graves relacionados con las TIC y determinar las respuestas adecuadas;

ii) Seguidamente, los Estados podrían elaborar plantillas de la gravedad de los incidentes de TIC con el fin de evaluar y valorar dichos incidentes;

[14] https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-buildinternational-law.

[15] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

[16] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

[17] 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.

iii) La transparencia y la armonización de estas plantillas por parte de las organizaciones regionales podría garantizar que los Estados consideren del mismo modo los incidentes de TIC y mejorar la comunicación entre los Estados.

iv) Al considerar toda la información pertinente en el caso de un incidente de TIC, los Estados deberían investigar los posibles efectos en función del género, y trabajar de forma inclusiva con todas las partes interesadas para comprender el contexto más amplio de un incidente relacionado con las TIC, incluido su impacto en el disfrute de los derechos de las mujeres.

- Se propone la siguiente orientación para la implementación de la norma 13 c)[18]:

i) Si un Estado detecta ciberactividad malintencionada procedente del territorio o de la ciberinfraestructura de otro Estado, el primer paso podría ser notificar a dicho Estado. Los equipos informáticos de respuesta de emergencia son cruciales para detectar este tipo de actividades;

ii) Dado que los incidentes relacionados con las TIC pueden provenir o implicar a terceros Estados, se entiende que la notificación a un Estado no implica que dicho Estado sea responsable del incidente;

iii) El Estado notificado debería acusar recibo a través del punto de contacto nacional correspondiente;

iv) Cuando un Estado tenga conocimiento de que su territorio o su ciberinfraestructura se está utilizando para cometer un hecho internacionalmente ilícito que pueda tener consecuencias adversas graves en otro Estado, el primer Estado debería intentar adoptar medidas razonables, disponibles y practicables dentro de su territorio y sus capacidades, de conformidad con sus obligaciones en virtud del derecho interno y el derecho internacional, para que cese el hecho internacionalmente ilícito o para mitigar sus consecuencias;

v) Esta norma no debería interpretarse como la exigencia de que un Estado controle de forma proactiva todas las TIC en su territorio, o que tome otras medidas preventivas;

vi) Un Estado que tenga conocimiento de actividades perjudiciales de TIC procedentes de su territorio, pero que carezca de capacidad de respuesta, puede optar por solicitar asistencia a otros Estados, incluso a través de los modelos estándar de solicitud de asistencia;

vii) En tales casos se puede solicitar la ayuda de otros Estados, o de una entidad privada, de conformidad con el derecho interno. El compromiso de los Estados de cooperar con otras naciones y ayudarlas en caso de crisis es fundamental, y debe hacerse especial hincapié en las diferentes consecuencias que un incidente de TIC puede tener en una infraestructura específica de un país en desarrollo;

- El proyecto también debería incluir nuevas normas, como la siguiente:

“Los Estados no deben llevar a cabo operaciones de TIC con la intención de lograr la disrupción de la infraestructura técnica esencial para procesos políticos, como elecciones, referendos o plebiscitos.”

[18] Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC.

India

• (Sobre el párr. 39): Propuesta de nueva norma relacionada con la necesidad de acordar un estandar de seguridad esencial en el ciberespacio sobre las formas más efectivas de optimizar las nuevas tecnologías a la vez que se protege al público. Para tal fin, los Estados apoyarán firmemente la adopción generalizada y la implementación verificada de prácticas de ciberhigiene básica.

• La protección de las infraestructuras de información críticas es lo que constituye comportamiento responsable de los Estados. Las amenazas a dichas infraestructuras pueden menoscabar la integridad de la información y perjudicar la economía y el desarrollo económico de una nación. Los Estados deben considerar la protección de las infraestructuras de información críticas mediante alianzas entre los sectores público y privado. Los Estados no deben llevar a cabo operaciones relacionadas con la TIC con el fin de provocar la disrupción de dichas infraestructuras. Los Estados no deben crear funciones perniciosas en los productos de TIC. Los Estados deben encargarse de notificar a los usuarios cuando se detecten vulnerabilidades significativas y notificar a los proveedores para que les pongan remedio. Los Estados deben colaborar con las infraestructuras de información críticas, intercambiar información sobre las amenazas y compartir las herramientas y técnicas de mitigación.

República Islámica del Irán

• Las funciones de los Estados, que son los principales responsables de mantener un entorno de TIC seguro y fiable, deberían reforzarse en la gobernanza del entorno de las TIC a nivel mundial, incluidas la elaboración de políticas y la toma de decisiones. La gobernanza prevista debe llevarse a cabo de forma que refuerce la soberanía estatal y no afecte al derecho de los Estados a elegir sus modelos de desarrollo, gobernanza y legislación en el entorno de las TIC.

• Los Estados se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de otro Estado dentro del entorno de las TIC o valiéndose de él.

• Ningún Estado tiene derecho a intervenir por medios informáticos, directa o indirectamente y por motivo alguno, en los asuntos internos o externos de otros Estados. Se condenará y evitará toda forma de intervención e interferencia o intento de amenaza contra los sistemas político, económico, social y cultural, así como contra las infraestructuras de información críticas de los Estados. (Resolución 2131 (XX) de la Asamblea General, de 21 de diciembre de 1965)

• Los Estados no utilizarán los adelantos de las TIC como instrumentos para adoptar medidas coercitivas económicas, políticas o de cualquier otro tipo, incluidas medidas de restricción y bloqueo contra los Estados. (Resolución 2131 (XX) de la Asamblea General, de 21 de diciembre de 1965)

• Los Estados deben garantizar medidas apropiadas dirigidas a que el sector privado con actividades de ámbito extraterritorial, incluidas las plataformas, rinda cuentas de su comportamiento en el entorno de las TIC. Los Estados deben ejercer el debido control sobre las empresas y plataformas de TIC bajo su jurisdicción, o de lo contrario serán responsables de violar a sabiendas la soberanía nacional, la seguridad y el orden público de otros Estados.

• Los Estados deben abstenerse de aprovechar las cadenas de suministro de las TIC desarrolladas bajo su control y jurisdicción para crear o ayudar al desarrollo de vulnerabilidades en los productos, servicios y mantenimiento que puedan

comprometer la soberanía y la protección de datos de los Estados, y deben evitar que eso ocurra.

Japón

El Japón propone al Grupo de Trabajo que se añada el texto siguiente como orientación para la implementación de la norma 13 i) sobre la garantía de la integridad de la cadena de suministro:

- “Los Estados tienen el derecho y la responsabilidad de garantizar el uso de proveedores de confianza para los equipos y sistemas de TIC, en particular para abordar cuestiones de seguridad nacional y protección de la privacidad. Como medidas razonables se podría adoptar legislación o medidas administrativas para garantizar la seguridad de la cadena de suministro, apoyar el desarrollo de tecnología fiable y una industria de confianza, y diversificar los proveedores”.

Países Bajos

- “Los agentes estatales y no estatales no deben llevar a cabo ni permitir a sabiendas actividades que perjudiquen intencionadamente y de forma sustancial la disponibilidad o integridad general del núcleo público de Internet, y por ende la estabilidad del ciberespacio” [sería] una orientación para la implementación de la recomendación 13 f) del informe del Grupo de Trabajo de 2015 y, por lo tanto, también se podría aplicar a la recomendación 13 g)

- “Los agentes estatales y no estatales no deben llevar a cabo, apoyar ni permitir las ciberoperaciones destinadas a perturbar la infraestructura técnica esencial para las elecciones, los referendos o los plebiscitos”, [sería] una orientación para la implementación de la recomendación 13 f) del informe del Grupo de Trabajo de 2015 y, por lo tanto, también se podría aplicar a la recomendación 13 g).

Movimiento de Países No Alineados

- Los Estados Miembros deberían recopilar y racionalizar la información que presentaron sobre su implementación de las normas internacionales y la propuesta pertinente de depósito, con el fin de regular aspectos específicos del uso de las TIC por los Estados desde la perspectiva de la seguridad internacional y determinar ámbitos de interés mutuo.

- Los Estados miembros no deben llevar a cabo ni apoyar a sabiendas ninguna actividad de TIC que perjudique o impida intencionadamente el uso y funcionamiento de las infraestructuras críticas de otros Estados miembros, contraviniendo el derecho internacional.

- Se debe instar a los Estados Miembros a que consideren el intercambio de información sobre las vulnerabilidades relacionadas con las TIC y las funciones ocultas perniciosas de los productos de las TIC y notifiquen a los usuarios cuando se detecten vulnerabilidades importantes.

- Los Estados miembros también deberán tener en cuenta lo dispuesto en la resolución 73/27 de la Asamblea General en la realización de todas las actividades relacionadas con las TIC.

- El Movimiento de Países No Alineados reitera su profunda preocupación por el hecho de que se recurra cada vez más al unilateralismo y, en ese contexto, subraya que el multilateralismo y las soluciones acordadas multilateralmente, de conformidad con la Carta de las Naciones Unidas, proporcionan el único método sostenible de abordar las cuestiones relacionadas con la seguridad internacional.

- Además, reitera que todos los Estados deben abstenerse de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de otro Estado dentro del entorno de las TIC o valiéndose de él.

- También pide que se intensifiquen los esfuerzos para evitar que el ciberespacio se convierta en un escenario de conflicto y asegurar, en cambio, los usos exclusivamente pacíficos que permitan la plena realización del potencial de las TIC para contribuir al desarrollo social y económico.

- El Movimiento de Países No Alineados subraya la importancia de evitar restricciones indebidas, incluso mediante medidas coercitivas unilaterales, a los usos pacíficos de las TIC, la cooperación internacional o la transferencia de tecnología.

- Insiste además en que los Estados tienen la responsabilidad primordial de mantener un entorno de TIC abierto, seguro, estable, accesible y pacífico.

- También subraya que ningún Estado debe realizar o apoyar a sabiendas actividades de TIC contrarias a sus obligaciones en virtud del derecho internacional que perjudiquen o impidan intencionadamente el uso y funcionamiento de las infraestructuras críticas.

Pakistán

- Se debe alentar a los Estados Miembros a que sigan considerando, según proceda, la posible aprobación de uno o varios instrumentos jurídica y políticamente vinculantes para regular aspectos específicos del uso de las TIC por los Estados en el contexto de la seguridad internacional.

- Debe alentarse a los Estados miembros a que convengan en una definición común de lo que constituye infraestructura crítica, con el fin de acordar la prohibición de las actividades de las TIC que, a sabiendas o intencionadamente, perjudiquen la infraestructura crítica o impidan de otro modo su uso y funcionamiento.

- Los Estados Miembros deberían cooperar para llegar a un acuerdo sobre la prohibición de crear funciones ocultas perniciosas o acumular vulnerabilidades en los productos de las TIC, así como comprometerse a informar de forma responsable y oportuna sobre las vulnerabilidades de las TIC y compartir la información asociada sobre las soluciones disponibles para dichas vulnerabilidades.

- Los Estados Miembros deben tratar de facilitar la cooperación con los proveedores de productos y servicios de TIC para evitar la explotación o el uso indebido de los datos y la privacidad de los usuarios.

- Los Estados miembros deben comprometerse a no utilizar las TIC para llevar a cabo actividades contrarias al mantenimiento de la paz y la seguridad internacionales, y abstenerse de utilizar las TIC para interferir de cualquier manera en los asuntos internos de otros Estados.

- Los Estados Miembros deben cooperar para hacer frente a los problemas relacionados con la atribución en el entorno de las TIC. El desarrollo de un enfoque común de la atribución en un entorno universal bajo los auspicios de las Naciones Unidas sigue siendo la forma más eficaz de avanzar en este sentido.

• Debe instarse a los Estados Miembros a que lleguen a un acuerdo sobre la prohibición de las actividades de las TIC que tengan por finalidad la disrupción de la infraestructura técnica esencial para las elecciones, los referendos o los plebiscitos.

• Los Estados Miembros deben elaborar e implementar las normas de manera que se eviten restricciones indebidas a los usos pacíficos de las TIC, a la cooperación internacional en este ámbito o a la transferencia de tecnología.

República de Corea

Sugerencia de orientación para el párrafo 13 c) del informe del Grupo de Expertos de 2015:

• Cuando un Estado afectado notifica con información cualificada a otro Estado que los incidentes de las TIC se han originado en su territorio o lo involucran de algún modo, el Estado notificado debe, con arreglo al derecho internacional e interno y dentro de su capacidad, tomar todas las medidas razonables dentro de su territorio para hacer que estas actividades cesen, o para mitigar sus consecuencias.

• Debe entenderse que dicha notificación no implica la responsabilidad del Estado notificado por el incidente.

• El requisito mínimo de información cualificada puede incluir el Indicador de Compromiso (IoC), como la dirección IP, la ubicación de los autores y los ordenadores utilizados para los actos malintencionados de las TIC y la información sobre el programa malicioso.