



Asamblea General

Distr. limitada
22 de octubre de 2018
Español
Original: inglés

Septuagésimo tercer período de sesiones

Primera Comisión

Tema 96 del programa

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

Angola, Argelia, Azerbaiyán, Belarús, Bolivia (Estado Plurinacional de), Burundi, Camboya, China, Cuba, Eritrea, Federación de Rusia, Kazajstán, Madagascar, Namibia, Nepal, Nicaragua, Pakistán, República Árabe Siria, República Democrática del Congo, República Popular Democrática de Corea, Samoa, Sierra Leona, Suriname, Tayikistán, Uzbekistán, Venezuela (República Bolivariana de) y Zimbabwe: proyecto de resolución

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

La Asamblea General,

Recordando sus resoluciones [36/103](#), de 9 de diciembre de 1981, [43/78 H](#), de 7 de diciembre de 1988, [53/70](#), de 4 de diciembre de 1998, [54/49](#), de 1 de diciembre de 1999, [55/28](#), de 20 de noviembre de 2000, [56/19](#), de 29 de noviembre de 2001, [57/53](#), de 22 de noviembre de 2002, [58/32](#), de 8 de diciembre de 2003, [59/61](#), de 3 de diciembre de 2004, [60/45](#), de 8 de diciembre de 2005, [61/54](#), de 6 de diciembre de 2006, [62/17](#), de 5 de diciembre de 2007, [63/37](#), de 2 de diciembre de 2008, [64/25](#), de 2 de diciembre de 2009, [65/41](#), de 8 de diciembre de 2010, [66/24](#), de 2 de diciembre de 2011, [67/27](#), de 3 de diciembre de 2012, [68/243](#), de 27 de diciembre de 2013, [69/28](#), de 2 de diciembre de 2014, [70/237](#), de 23 de diciembre de 2015, y [71/28](#), de 5 de diciembre de 2016,

Observando que se han logrado considerables progresos en el desarrollo y la aplicación de las tecnologías de la información y los medios de telecomunicación más modernos,

Confirmando que las tecnologías de la información y las comunicaciones son tecnologías de doble uso y pueden utilizarse con fines tanto legítimos como maliciosos,

Expresando su preocupación por el hecho de que varios Estados estén desarrollando capacidades en materia de TIC con fines militares y de que la utilización de las TIC en futuros conflictos entre Estados se está volviendo cada vez más probable,

* Publicado nuevamente por razones técnicas el 24 de octubre de 2018.



Destacando que redunda en interés de todos los Estados promover la utilización de las tecnologías de la información y las comunicaciones con fines pacíficos, con el objetivo de configurar una comunidad de futuro compartido para la humanidad en el ciberespacio, y que los Estados también tienen un interés en prevenir los conflictos que se derivan de emplear las tecnologías de la información y las comunicaciones,

Observando que las Naciones Unidas deberían desempeñar un papel rector en la promoción del diálogo entre los Estados Miembros para llegar a un entendimiento común sobre la seguridad de las TIC y sobre su utilización, así como en la elaboración de un entendimiento común sobre la aplicación del derecho internacional y de las normas, reglas y principios internacionales para el comportamiento responsable de los Estados en esta esfera, alentar los esfuerzos regionales, promover medidas de fomento de la confianza y de transparencia, y prestar apoyo a las actividades de creación de capacidad y de divulgación de las mejores prácticas,

Expresando preocupación por el hecho de que incorporar funciones ocultas perniciosas en las TIC podría hacerse de maneras que afectarían a la utilización segura y fiable de las TIC y a la cadena de suministro de productos y servicios de las TIC, erosionarían la confianza en el comercio y perjudicarían la seguridad nacional,

Considerando que es necesario impedir que los recursos o las tecnologías de la información se utilicen con fines delictivos o terroristas,

Subrayando la necesidad de mejorar la coordinación y la cooperación entre los Estados para combatir el uso indebido de las tecnologías de la información con fines delictivos y, en ese contexto, destacando la función que pueden desempeñar las Naciones Unidas y otras organizaciones internacionales y regionales,

Subrayando la importancia del respeto de los derechos humanos y las libertades fundamentales en el uso de las tecnologías de la información y las comunicaciones,

Acogiendo con beneplácito la eficaz labor del 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 informes pertinentes en que figuran sus conclusiones, remitidos por el Secretario General¹,

Acogiendo con beneplácito también que, al examinar la aplicación del derecho internacional a la utilización de las tecnologías de la información y las comunicaciones por los Estados, el Grupo de Expertos Gubernamentales determinó en su informe de 2015² que era de importancia fundamental la adhesión de los Estados a los siguientes principios de la Carta de las Naciones Unidas y otras fuentes del derecho internacional: la igualdad soberana; la solución de controversias internacionales por medios pacíficos de manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia; la renuncia a recurrir, en las relaciones internacionales, a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas; el respeto de los derechos humanos y las libertades fundamentales; y la no intervención en los asuntos internos de otros Estados.

Confirmando las conclusiones del Grupo de Expertos Gubernamentales, contenidas en sus informes de 2013³ y 2015², de que el derecho internacional y, en particular, la Carta, son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones, que la aplicación de

¹ A/65/201, A/68/98 y A/70/174.

² A/70/174.

³ A/68/98.

normas, reglas y principios de conducta estatal responsable de carácter voluntario y no vinculante en el uso de esas tecnologías puede reducir los riesgos para la paz, la seguridad y la estabilidad internacionales, y que, dadas las características particulares de esas tecnologías, podrían elaborarse normas adicionales con el transcurso del tiempo,

Confirmando también que la soberanía de los Estados y las normas y principios internacionales que de ella dimanar son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio,

Observando que la creación de capacidad es esencial para la cooperación de los Estados y las medidas de fomento de la confianza en la esfera de la seguridad de las TIC,

Destacando la necesidad de que se desplieguen mayores esfuerzos para cerrar la brecha digital facilitando la transferencia de tecnología de la información y la creación de capacidad a los países en desarrollo en los ámbitos de las mejores prácticas y la capacitación en materia de ciberseguridad, de conformidad con lo dispuesto en la resolución 64/211 de la Asamblea General, de 21 de diciembre de 2009, titulada “Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales”,

Destacando también que, si bien los Estados tienen la responsabilidad primordial de mantener un entorno seguro y pacífico en la esfera de la tecnología de la información y las comunicaciones, la cooperación internacional sería más eficaz si se establecieran mecanismos para alentar la participación, según procediera, del sector privado, el mundo académico y las organizaciones de la sociedad civil,

1. *Acoge con beneplácito* el siguiente conjunto de reglas, normas y principios internacionales de comportamiento responsable de los Estados:

1. Los Estados deben cumplir la Carta de las Naciones Unidas y las normas que rigen las relaciones internacionales reconocidas universalmente, que consagran, entre otras cosas, el respeto de la soberanía, la integridad territorial y la independencia política de todos los Estados, el respeto de los derechos humanos y las libertades fundamentales y el respeto de la diversidad de la historia, la cultura y los sistemas sociales de todos los países.
2. 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 tecnologías de la información y las comunicaciones 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.
3. Los Estados no deben utilizar las tecnologías de la información y las comunicaciones y las redes de información y comunicaciones para llevar a cabo actividades contrarias a la tarea de mantener la paz y la seguridad internacionales.
4. Los Estados no deben utilizar las tecnologías de la información y las comunicaciones y las redes de información y comunicaciones para injerirse en los asuntos internos de otros Estados o con el fin de socavar su estabilidad política, económica y social, y tienen el derecho y el deber de combatir, en el marco de sus prerrogativas constitucionales, la difusión de noticias falsas o

distorsionadas que puedan interpretarse como una injerencia en los asuntos internos de otros Estados o como perjudiciales para la promoción de la paz, la cooperación y las relaciones amistosas entre Estados y naciones.

5. Los Estados deben reconocer el deber del Estado de abstenerse de toda campaña de difamación, vilipendio o propaganda hostil que tenga por fin intervenir o injerirse en los asuntos internos de otros Estados.

6. Los Estados deben procurar garantizar a todos los niveles de la cadena de suministro la seguridad de los bienes y servicios de TIC, a fin de impedir que otros Estados aprovechen su posición dominante en materia de TIC, incluida la dominación de los recursos, las infraestructuras críticas, las tecnologías básicas, los bienes y servicios de tecnología de la información y las comunicaciones y las redes de información y comunicaciones, para socavar el derecho de los Estados a ejercer un control independiente de los bienes y servicios de TIC, o para amenazar su seguridad política, económica y social.

7. Los Estados deben reafirmar los derechos y responsabilidades de todos los Estados, de conformidad con las normas y reglas pertinentes, en lo que respecta a la protección jurídica de su espacio de información y su infraestructura de información crítica contra los daños resultantes de amenazas, interferencias, ataques y sabotajes.

8. Los Estados deben reconocer que los derechos de una persona en el entorno fuera de línea también deben protegerse en el entorno en línea; y respetar plenamente los derechos y libertades en el espacio informativo, incluido el derecho y la libertad de buscar, recibir y difundir informaciones, teniendo en cuenta el hecho de que el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos⁴ establece que ese derecho entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) El respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas;

9. Todos los Estados deben desempeñar el mismo papel y asumir la misma responsabilidad en la gobernanza internacional de Internet, su seguridad, continuidad y estabilidad de funcionamiento, y su desarrollo de manera que promueva el establecimiento de mecanismos internacionales multilaterales, transparentes y democráticos de gobernanza de Internet que garanticen una distribución equitativa de los recursos, faciliten el acceso de todas las personas y aseguren un funcionamiento estable y seguro de Internet.

10. Los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional. Sin embargo, la indicación de que una actividad de tecnología de la información y las comunicaciones se ha iniciado o se origina en el territorio u objetos de la infraestructura de tecnología de la información y las comunicaciones de un Estado puede ser insuficiente por sí sola para atribuir la actividad a ese Estado. Los Estados deben observar que las acusaciones contra los Estados de organizar y llevar a cabo actos ilícitos deben fundamentarse. En el caso de incidentes relacionados con las tecnologías de la información y las comunicaciones, los Estados deben tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el

⁴ Véase la resolución 2200 A (XXI), anexo.

hecho, los problemas que plantea la atribución en el entorno de estas tecnologías y la naturaleza y el alcance de las consecuencias.

11. Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando tecnologías de la información y las comunicaciones. Los Estados no deben recurrir a terceros para cometer actos internacionalmente ilícitos utilizando las tecnologías de la información y las comunicaciones, y deben tratar de garantizar que su territorio no sea utilizado por agentes no estatales para cometer esos actos.

12. Los Estados deben estudiar la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, enjuiciar la utilización de las tecnologías de la información y las comunicaciones con fines terroristas y delictivos y poner coto a la difusión de información que incite al terrorismo, el separatismo o el extremismo o que exacerbe el odio por motivos étnicos, raciales o religiosos, y aplicar otras medidas de cooperación para hacer frente a esas amenazas. Quizás los Estados deberían considerar si es necesario elaborar nuevas medidas a este respecto.

13. Para garantizar la seguridad de uso de las tecnologías de la información y las comunicaciones, los Estados deben acatar las resoluciones del Consejo de Derechos Humanos [20/8](#), de 5 de julio de 2012⁵, y [26/13](#), de 26 de junio de 2014⁶, relativas a la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones de la Asamblea General [68/167](#), de 18 de diciembre de 2013, y [69/166](#), de 18 de diciembre de 2014, relativas al 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.

14. Un Estado no debe realizar ni apoyar a sabiendas actividades en la esfera de las tecnologías de la información y las comunicaciones contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañen intencionadamente infraestructuras fundamentales que prestan servicios al público o dificulten de otro modo su utilización y funcionamiento.

15. Los Estados deben tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las tecnologías de la información y las comunicaciones, teniendo en cuenta la resolución [58/199](#) de la Asamblea General, de 23 de diciembre de 2003, relativa a la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales, y otras resoluciones pertinentes.

16. Los Estados deben atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales sean objeto de actos malintencionados en los que se empleen tecnologías de la información y las comunicaciones. Los Estados también deben atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las tecnologías de la información y las comunicaciones originada en su territorio que esté dirigida contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía.

17. 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 tecnologías de la información y las comunicaciones, y el derecho de los Estados a un control independiente de

⁵ Véase *Documentos Oficiales de la Asamblea General, sexagésimo séptimo período de sesiones, Suplemento núm. 53* y corrección ([A/67/53](#) y [A/67/53/Corr.1](#)), cap. IV, secc. A.

⁶ *Ibid.*, sexagésimo noveno período de sesiones, Suplemento núm. 53 ([A/69/53](#)), cap. V, secc. A.

los bienes y servicios de las tecnologías de la información y las comunicaciones no debe verse menoscabado, ni su seguridad política, económica y social amenazada.

18. Los Estados deben tratar de evitar la proliferación de técnicas e instrumentos malignos en la esfera de las tecnologías de la información y las comunicaciones, así como el uso de funciones ocultas perniciosas.

19. Los Estados deben alentar la divulgación responsable de información sobre las vulnerabilidades relacionadas con las tecnologías de la información y las comunicaciones y compartir la información conexas sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las tecnologías de la información y las comunicaciones o las infraestructuras dependientes de esas tecnologías.

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

21. Los Estados deben alentar al sector privado y a la sociedad civil a desempeñar un papel adecuado para aumentar la seguridad de las tecnologías de la información y las comunicaciones y en su utilización, incluida la seguridad de la cadena de suministro de productos y servicios de las tecnologías de la información y las comunicaciones. *Los Estados deben cooperar con el sector privado y las organizaciones de la sociedad civil en el ámbito de la aplicación de normas de comportamiento responsable en el espacio de la información con respecto a su posible función.

22. Los Estados deben elaborar medidas de fomento de la confianza encaminadas a aumentar la previsibilidad y reducir la probabilidad de malentendidos y el riesgo de conflictos. * Esas medidas incluirán, entre otras cosas, el intercambio voluntario de información sobre las estrategias nacionales y las estructuras organizativas para garantizar la seguridad de la información de un Estado, la publicación de libros blancos y el intercambio de las mejores prácticas, siempre que sea práctico y aconsejable.

23. Los Estados deben ayudar a los países en desarrollo en sus esfuerzos por mejorar la creación de capacidad en materia de seguridad de la información y por cerrar la brecha digital.

24. Los Estados deben reforzar la cooperación bilateral, regional e internacional y promover un papel destacado para las Naciones Unidas en esferas como el fomento de la elaboración de normas jurídicas internacionales para la seguridad de la información, el arreglo pacífico de controversias internacionales y la mejora cualitativa de la cooperación internacional en la esfera de la seguridad de la información; y mejorar la coordinación entre las organizaciones internacionales pertinentes.

25. Los Estados deben resolver por medios pacíficos cualquier controversia resultante de la aplicación del presente conjunto de reglas, normas y principios internacionales de comportamiento responsable de los Estados y abstenerse de recurrir a la amenaza o al uso de la fuerza;

2. *Exhorta* a los Estados Miembros a seguir promoviendo a nivel multilateral el examen de las amenazas reales y potenciales en la esfera de la seguridad de la información y de posibles estrategias para encarar las amenazas que surjan en esa

esfera, de manera compatible con la necesidad de preservar la libre circulación de la información;

3. *Considera* que el propósito de esas medidas podría promoverse continuando el examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones;

4. *Invita* a todos los Estados Miembros, teniendo en cuenta las evaluaciones y recomendaciones que figuran 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 Internacional¹¹, a seguir comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

- a) La evaluación general de los temas relacionados con la seguridad de la información;
- b) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en ese ámbito;
- c) El contenido de los conceptos mencionados en el párrafo 3;
- d) Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial;

5. *Solicita*, con miras a que el proceso de negociación de las Naciones Unidas sobre la seguridad en la utilización de las tecnologías de la información y las comunicaciones sea más democrático, inclusivo y transparente, al Secretario General que, con la asistencia de un grupo de trabajo de composición abierta, que se establecerá en 2019 y actuará por consenso, siga elaborando con carácter prioritario las normas, reglas y principios de comportamiento responsable de los Estados enunciados en el párrafo 1, así como las modalidades de aplicación correspondientes; que, de ser necesario, les introduzca cambios o elabore reglas de comportamiento adicionales; que estudie la posibilidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas; y que siga 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 aplica 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 los conceptos a que se hace referencia en el párrafo 3, y en su septuagésimo quinto período de sesiones le presente un informe sobre los resultados del estudio, y que ofrezca la posibilidad de que se celebren, dentro de los límites de los recursos existentes y 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;

6. *Decide* incluir en el programa provisional de su septuagésimo cuarto período de sesiones el tema titulado “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.