



Asamblea General

Distr. general
15 de diciembre de 2009
Español
Original: inglés

Sexagésimo cuarto período de sesiones
Tema 55 c) del programa

Globalización e interdependencia: ciencia y tecnología para el desarrollo

Informe de la Segunda Comisión*

Relatora: Sra. Denise McQuade (Irlanda)

I. Introducción

1. La Segunda Comisión celebró un debate sustantivo sobre el tema 55 del programa (véase A/64/422, párr. 2). En las sesiones 30ª, 33ª, 37ª y 38ª, celebradas los días 3, 10 y 25 de noviembre y 1º de diciembre de 2009, se adoptaron medidas en relación con el subtema c). En las actas resumidas correspondientes se reseña el debate de la Comisión sobre ese subtema (A/C.2/64/SR.30, 33, 37 y 38).

II. Examen de los proyectos de resolución

A. Proyectos de resolución A/C.2/64/L.8 y Rev.1

2. En la 30ª sesión, celebrada el 3 de noviembre, el representante de los Estados Unidos de América, en nombre de Australia, Bulgaria, el Canadá, Estonia, Israel, el Japón, las Islas Marshall, la República de Corea y el Reino Unido de Gran Bretaña e Irlanda del Norte, presentó un proyecto de resolución titulado “Creación de una cultura mundial de seguridad cibernética y examen de las medidas nacionales para proteger las infraestructuras de información esenciales” (A/C.2/64/L.8), cuyo texto era el siguiente:

“La Asamblea General,

Recordando sus resoluciones 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos, 57/239, de 20 de diciembre

* El informe de la Comisión sobre este tema se publicará en cuatro partes, con las signaturas A/64/422 y Add.1 a 3.



de 2002, relativa a la creación de una cultura mundial de seguridad cibernética, y 58/199, 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,

Recordando también sus resoluciones 53/70, de 4 de diciembre de 1998, 54/49, de 1º 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, y 63/37, de 2 de diciembre de 2008, relativas a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,

Recordando además los documentos finales de la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Ginebra del 10 al 12 de diciembre de 2003 (primera fase) y en Túnez del 16 al 18 de noviembre de 2005 (segunda fase), en que los Estados reconocieron que la libertad de expresión y la libre circulación de información, las ideas y los conocimientos son esenciales para la sociedad de la información de hoy y benéficos para el desarrollo, y que, dado que la confianza y la seguridad en la utilización de las tecnologías de la información y las comunicaciones son unos de los pilares más importantes de la sociedad de la información, es necesario fomentar, desarrollar y poner en práctica una firme cultura global de seguridad cibernética,

Reconociendo que la contribución de las tecnologías de la información en red es cada vez más indispensable para la mayoría de las funciones esenciales de la vida cotidiana, el comercio y la prestación de bienes y servicios, la investigación, la innovación y el espíritu empresarial, y para la libre circulación de información entre individuos, organizaciones y gobiernos,

Observando que los gobiernos, las empresas, la sociedad civil y las personas dependen cada vez más de una red mundial de infraestructuras de información, y que esa dependencia aumentará,

Observando también que las lagunas en el acceso a las tecnologías de la información y su uso por los Estados pueden disminuir su prosperidad social y económica, y observando en especial las necesidades de los países menos adelantados en los ámbitos de las mejores prácticas y la capacitación en materia de seguridad cibernética,

Expresando preocupación por que las amenazas para el funcionamiento fiable de las infraestructuras de información esenciales y la integridad de la información transportada por esas redes están aumentando en complejidad y gravedad y afectando el bienestar interno, nacional e internacional,

Afirmando que la seguridad de las infraestructuras de información esenciales es una responsabilidad que los gobiernos deben abordar de manera sistemática y es una esfera en la que deben asumir un papel rector a nivel nacional, en coordinación con los interesados competentes, quienes a su vez deben ser conscientes de los riesgos correspondientes, las medidas de prevención y las respuestas efectivas de manera acorde con sus respectivas funciones,

Reconociendo que las medidas nacionales deben ir apoyadas por el intercambio de información y la colaboración a nivel nacional, regional e internacional a fin de afrontar efectivamente la naturaleza cada vez más transnacional de esas amenazas,

Observando la labor de las organizaciones regionales e internacionales competentes para mejorar la seguridad cibernética, especialmente las que han alentado los esfuerzos nacionales y fomentado la cooperación internacional,

Observando también el informe de la Unión Internacional de Telecomunicaciones publicado en 2009, titulado ‘Seguridad de la información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad’, centrado en un enfoque nacional amplio para la seguridad cibernética compatible con la libertad de expresión, la libre circulación de información y las debidas garantías procesales,

Reconociendo que es beneficioso evaluar periódicamente los progresos en las medidas nacionales para proteger las infraestructuras de información esenciales,

1. *Invita* a los Estados Miembros a que presenten voluntariamente resúmenes de sus principales iniciativas en materia de seguridad cibernética y protección de las infraestructuras de información esenciales, a fin de resaltar los avances y las mejores prácticas nacionales, las experiencias adquiridas y las esferas en las que se deberían adoptar medidas adicionales;

2. *Ofrece* a los Estados Miembros, a este respecto, la encuesta de autoevaluación sobre la seguridad cibernética nacional que se adjunta como posible instrumento para ayudarlos, cuando proceda, a examinar las medidas nacionales relativas a la seguridad cibernética y la protección de infraestructuras de información esenciales;

3. *Invita* a todos los Estados Miembros que hayan elaborado estrategias relativas a la seguridad cibernética y la protección de las infraestructuras de información esenciales a que informen al Secretario General, para el sexagésimo quinto período de sesiones de la Asamblea General, acerca de las mejores prácticas y las medidas que podrían ayudar a otros Estados Miembros, a las organizaciones regionales e internacionales, al sector privado y los interesados de la sociedad civil, en sus iniciativas por crear una cultura mundial de seguridad cibernética.

Anexo

Instrumento de autoevaluación de las medidas nacionales para proteger las infraestructuras de información esenciales

Examen de las necesidades y estrategias en materia de seguridad cibernética

1. Evaluar el papel de las tecnologías de la información y las comunicaciones en la economía, la seguridad nacional, las infraestructuras esenciales (como el transporte, el suministro de agua y alimentos, la salud

pública, la energía, las finanzas y los servicios de emergencia) y la sociedad civil de su país.

2. Determinar los riesgos para la economía, la seguridad nacional, las infraestructuras esenciales y la sociedad civil de su país que deban gestionarse en relación con la seguridad cibernética y la protección de las infraestructuras de información esenciales.

3. Comprender las vulnerabilidades de las redes en uso, los niveles relativos de las amenazas a que se enfrenta cada sector en la actualidad y el plan de gestión en curso, y señalar la manera en que los cambios en el entorno económico, las prioridades de seguridad nacional y las necesidades de la sociedad civil afectan a esos cálculos.

4. Determinar los objetivos de su estrategia nacional en materia de seguridad cibernética y protección de las infraestructuras de información esenciales, describir sus objetivos, el nivel de ejecución actual, las medidas existentes para medir los progresos, su relación con otros objetivos de políticas nacionales y la manera en que esa estrategia concuerda con las iniciativas regionales e internacionales.

Funciones y responsabilidades de los interesados

5. Determinar los principales interesados que participen en la seguridad cibernética y la protección de las infraestructuras de información esenciales y describir la función de cada uno de ellos en la elaboración de las políticas y operaciones pertinentes, incluidos:

- Los ministerios u organismos gubernamentales nacionales, señalando los principales puntos de contacto y las responsabilidades de cada uno;
- Otros participantes gubernamentales (locales y regionales);
- Los agentes no gubernamentales, entre ellos la industria, la sociedad civil y los estamentos académicos;
- Las personas a título individual, señalando si los usuarios normales de Internet tienen acceso a capacitación básica para evitar las amenazas en línea y si existe una campaña nacional de concienciación sobre la seguridad cibernética.

Procesos políticos y participación

6. Determinar los medios oficiales y oficiosos que existan en la actualidad para la colaboración entre el gobierno y la industria en la elaboración de políticas y operaciones en materia de seguridad cibernética y protección de las infraestructuras de información esenciales; determinar los participantes, sus funciones y objetivos, los métodos para obtener y utilizar las aportaciones y su idoneidad en el logro de los objetivos pertinentes en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

7. Determinar los foros o estructuras que podrían ser necesarios además para integrar las perspectivas y los conocimientos gubernamentales y no gubernamentales necesarios para lograr los objetivos nacionales en materia

de seguridad cibernética y protección de las infraestructuras de información esenciales.

Cooperación entre el sector público y privado

8. Recopilar todas las medidas y planes adoptados para aumentar la cooperación entre el gobierno y el sector privado, incluyendo todo arreglo para intercambiar información y gestionar los incidentes.

9. Reunir todas las iniciativas actuales y previstas para promover intereses compartidos y abordar desafíos comunes entre los participantes encargados de las infraestructuras esenciales y los agentes del sector privado que dependen de las mismas infraestructuras esenciales interconectadas.

Gestión de los incidentes y recuperación

10. Determinar el organismo gubernamental que coordine la gestión de los incidentes, incluida la capacidad para ejercer funciones de observación, alerta, respuesta y recuperación, los organismos gubernamentales colaboradores, los participantes no gubernamentales colaboradores, incluida la industria y otros asociados, y todo arreglo existente para la cooperación y el intercambio de información confiable.

11. Determinar, separadamente, la capacidad nacional de respuesta ante incidentes informáticos, incluidos los equipos de respuesta ante incidentes informáticos con responsabilidades nacionales y sus funciones y atribuciones, incluidos los instrumentos y procedimientos existentes para la protección de las redes informáticas gubernamentales, y los instrumentos y procedimientos existentes para difundir información sobre la gestión de los incidentes.

12. Determinar las redes y procesos de cooperación internacional que puedan reforzar la respuesta ante los incidentes y la planificación para imprevistos, la identificación de los asociados y los arreglos para la cooperación bilateral y multilateral, cuando proceda.

Marcos jurídicos

13. Examinar y actualizar las autoridades jurídicas (incluidas las relacionadas con los delitos cibernéticos, la privacidad, la protección de los datos, el derecho comercial, las firmas digitales y el cifrado) que puedan estar anticuadas u obsoletas como resultado de la rápida incorporación de las nuevas tecnologías de la información y las comunicaciones y de la dependencia de esas tecnologías, y utilizar en esos exámenes los convenios, arreglos y precedentes regionales e internacionales. Señalar si su Estado es parte en el Convenio de Budapest sobre la Ciberdelincuencia o tiene previsto adherirse a él o aprobar leyes conmensurables.

14. Determinar el estado actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las autoridades jurídicas, las dependencias nacionales encargadas de la delincuencia cibernética y el nivel de comprensión de las cuestiones relativas a la delincuencia cibernética entre los fiscales, jueces y legisladores.

15. Evaluar la idoneidad de los códigos jurídicos y las autoridades actuales para hacer frente a los desafíos presentes y futuros de la delincuencia cibernética y del ciberespacio de forma más general.

16. Examinar si su Estado participa en las medidas internacionales para luchar contra la delincuencia cibernética, como la Red 24/7 de puntos de contacto, y establecer en qué medida hacerlo promovería la consecución de los objetivos nacionales en materia de seguridad cibernética.

17. Determinar los requisitos para que sus organismos nacionales de imposición de la ley cooperen con sus homólogos internacionales a fin de investigar los delitos cibernéticos transnacionales en los casos en que la infraestructura esté situada en su territorio nacional o los culpables residan en él pero las víctimas residan en otros lugares.

Creación de una cultura mundial de seguridad cibernética

18. Resumir las medidas y los planes adoptados para crear una cultura nacional de seguridad cibernética a que se hace referencia en las resoluciones de la Asamblea General de las Naciones Unidas 57/239 y 58/199, incluida la ejecución de un plan de seguridad cibernética para los sistemas operados por el gobierno, la ejecución de programas nacionales de concienciación y divulgación dirigidos, entre otros, a los niños y los usuarios individuales, y las necesidades nacionales de capacitación en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.”

3. En su 37ª sesión, celebrada el 25 de noviembre, la Comisión tuvo ante sí un proyecto de resolución revisado titulado “Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales” (A/C.2/64/L.8/Rev.1), presentado por los Estados Unidos en nombre de Alemania, Antigua y Barbuda, Argentina, Australia, Belice, Bulgaria, el Canadá, Chile, Croacia, Eslovenia, España, Estonia, Finlandia, Francia, Hungría, Irlanda, las Islas Marshall, Israel, Italia, el Japón, Letonia, México, Montenegro, Nigeria, Panamá, Polonia, Portugal, el Reino Unido de Gran Bretaña e Irlanda del Norte, la República de Corea, la República Dominicana, la República de Moldova, Rumania, Singapur, Suecia y Ucrania.

4. En la misma sesión se informó a la Comisión de que el proyecto de resolución revisado no tenía consecuencias para el presupuesto por programas.

5. También en la misma sesión, el representante de los Estados Unidos de América, corrigió oralmente el proyecto de resolución.

6. También en la 37ª sesión, Grecia, la India, Jamaica y Lituania se sumaron también a los patrocinadores del proyecto de resolución.

7. La Comisión aprobó el proyecto de resolución A/C.2/64/L.8/Rev.1 en su forma oralmente revisada (véase párr. 14, proyecto de resolución I).

B. Proyectos de resolución A/C.2/64/L.17 y A/C.2/64/L.49

8. En la 33ª sesión, celebrada el 10 de noviembre, la representante del Sudán, en nombre de los Estados Miembros de las Naciones Unidas que son miembros del

Grupo de los 77 y China, presentó un proyecto de resolución titulado “Ciencia y tecnología para el desarrollo” (A/C.2/64/L.17) cuyo texto era el siguiente:

“La Asamblea General,

Recordando sus resoluciones 58/200, de 23 de diciembre de 2003, 59/220, de 22 de diciembre de 2004, 60/205, de 22 de diciembre de 2005 y 62/201, de 19 de diciembre de 2007,

Recordando también su resolución 61/207, de 20 de diciembre de 2006, y la referencia que se hace en ella a la ciencia y la tecnología,

Recordando además la resolución 2006/46 del Consejo Económico y Social, de 28 de julio de 2006,

Reconociendo la función decisiva que la ciencia y la tecnología, incluidas las tecnologías ecológicamente racionales, pueden desempeñar en el desarrollo y la facilitación de los esfuerzos por erradicar la pobreza, lograr la seguridad alimentaria, luchar contra las enfermedades, mejorar la educación, proteger el medio ambiente, acelerar el ritmo de la diversificación y la transformación económicas y mejorar la productividad y la competitividad,

Recordando el Documento Final de la Cumbre Mundial 2005,

Recordando también los resultados de la Cumbre Mundial sobre la Sociedad de la Información,

Reconociendo que el apoyo internacional puede ayudar a los países en desarrollo a beneficiarse de los adelantos tecnológicos y puede aumentar su capacidad productiva,

Recalcando la función que los conocimientos tradicionales pueden desempeñar en el desarrollo tecnológico y en la ordenación y el uso sostenibles de los recursos naturales,

Reconociendo la necesidad urgente de cerrar la brecha digital y ayudar a los países en desarrollo a tener acceso a los beneficios que puedan brindar las tecnologías de la información y las comunicaciones,

Acogiendo con beneplácito la aprobación del Plan Estratégico de Bali para el apoyo tecnológico y la creación de capacidad del Programa de las Naciones Unidas para el Medio Ambiente,

Reafirmando la necesidad de fortalecer los programas de ciencia y tecnología de las entidades pertinentes del sistema de las Naciones Unidas,

Observando con aprecio la colaboración entre la Comisión de Ciencia y Tecnología para el Desarrollo y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo para establecer una red de centros de excelencia en ciencia y tecnología para los países en desarrollo y para diseñar y realizar exámenes de las políticas de ciencia, tecnología e innovación,

Tomando nota con interés del establecimiento de ONU-Biotech, la red interinstitucional de cooperación en materia de biotecnología descrita en el informe del Secretario General sobre ciencia y tecnología para el desarrollo,

Tomando nota del informe del Secretario General,

Tomando nota también de la resolución 2009/8 del Consejo Económico y Social , de 24 de julio de 2009, sobre ciencia y tecnología para el desarrollo,

1. *Reafirma su compromiso* de:

a) Fortalecer y mejorar los mecanismos existentes y apoyar las iniciativas de investigación y desarrollo, incluso mediante alianzas voluntarias entre el sector público y el privado, a fin de atender las necesidades especiales de los países en desarrollo en las esferas de la salud, la agricultura, la conservación, el uso sostenible de los recursos naturales y la ordenación del medio ambiente, la energía, la silvicultura y los efectos del cambio climático;

b) Promover y facilitar, según proceda, el acceso de los países en desarrollo a la tecnología y también al desarrollo, la transmisión y la difusión de la tecnología, incluida la tecnología ecológicamente racional y los correspondientes conocimientos especializados;

c) Ayudar a los países en desarrollo en sus esfuerzos por promover y elaborar estrategias nacionales de recursos humanos y ciencia y tecnología, que son elementos impulsores fundamentales de la creación de capacidad nacional para el desarrollo;

d) Promover y apoyar un mayor esfuerzo para desarrollar la tecnología necesaria para impulsar las fuentes de energía renovables, como la energía solar, la de la biomasa, la hidroeléctrica, la eólica y la geotérmica;

e) Aplicar políticas a nivel nacional e internacional para atraer inversiones públicas, privadas, nacionales y extranjeras que permitan mejorar los conocimientos, transferir tecnología en condiciones mutuamente convenientes e incrementar la productividad;

f) Apoyar los esfuerzos de los países en desarrollo, tanto individuales como colectivos, para aprovechar las nuevas tecnologías agrícolas a fin de incrementar la productividad agrícola por medios ecológicamente sostenibles;

2. *Reconoce* que la ciencia y la tecnología, incluidas las tecnologías de la información y las comunicaciones, son decisivas para el logro de los objetivos de desarrollo convenidos internacionalmente, incluidos los Objetivos de Desarrollo del Milenio, y para la plena participación de los países en desarrollo en la economía mundial;

3. *Solicita* a la Comisión de Ciencia y Tecnología para el Desarrollo que sirva de foro para continuar ayudando al Consejo Económico y Social a cumplir sus funciones de centro de coordinación del seguimiento de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información a nivel de todo el sistema, y para atender, en el contexto de su mandato y de conformidad con la resolución 2006/46 del Consejo, las necesidades especiales de los países en desarrollo en esferas como la agricultura, el desarrollo rural, las tecnologías de la información y las comunicaciones y la ordenación del medio ambiente;

4. *Alienta* a la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo a que, en colaboración con los asociados pertinentes, siga realizando exámenes de las políticas de ciencia, tecnología e innovación con miras a ayudar a los países en desarrollo y a los países de economía en

transición a determinar las medidas necesarias para integrar las políticas de ciencia, tecnología e innovación en sus estrategias nacionales de desarrollo;

5. *Alienta* a la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo y otras organizaciones pertinentes a que ayuden a los países en desarrollo en sus esfuerzos por integrar las políticas de ciencia, tecnología e innovación en las estrategias nacionales de desarrollo;

6. *Alienta* a los gobiernos a que aumenten y promuevan las inversiones en actividades de investigación y desarrollo de tecnologías ecológicamente racionales y a que fomenten la participación del sector empresarial y el sector financiero en el desarrollo de esas tecnologías, e invita a la comunidad internacional a que respalde esa labor;

7. *Alienta* a que se mantengan los arreglos existentes y se sigan promoviendo los proyectos conjuntos de investigación y desarrollo a nivel regional, subregional e interregional movilizando, cuando sea posible, los recursos científicos y de investigación y desarrollo existentes y creando redes de instalaciones científicas y equipos de investigación avanzados;

8. *Alienta* a la comunidad internacional a que, habida cuenta del diferente nivel de desarrollo de los países, continúe facilitando la difusión adecuada de conocimientos científicos y técnicos y la transferencia, el acceso y la adquisición de tecnología para los países en desarrollo, en condiciones equitativas, transparentes y mutuamente convenidas, de tal manera que favorezcan el bienestar social y económico en interés de la sociedad;

9. *Pide* a las entidades de las Naciones Unidas y otras organizaciones internacionales, la sociedad civil y el sector privado a que sigan colaborando en la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, con miras a poner el potencial de las tecnologías de la información y las comunicaciones al servicio del desarrollo a través de la investigación de políticas sobre la brecha digital y los nuevos desafíos de la sociedad de la información, así como de actividades de asistencia técnica, con la participación de alianzas entre múltiples interesados;

10. *Solicita* al Secretario General que le presente, en su sexagésimo sexto período de sesiones, un informe sobre la aplicación de la presente resolución en el que figuren recomendaciones sobre las medidas complementarias que deberán adoptarse y se dé cuenta de la experiencia adquirida en la integración de las políticas de ciencia, tecnología e innovación en las estrategias nacionales de desarrollo.”

9. En su 38ª sesión, celebrada el 1º de diciembre, la Comisión tuvo ante sí un proyecto de resolución titulado “Ciencia y tecnología para el desarrollo” (A/C.2/64/L.49), presentado por el Vicepresidente de la Comisión, Sr. Mohamed Cherif Diallo (Guinea), sobre la base de las consultas oficiosas celebradas en relación con el proyecto de resolución A/C.2/64/L.17.

10. En la misma sesión, la Comisión convino en no aplicar, a propuesta de la Presidencia, la disposición pertinente del artículo 120 del reglamento de la Asamblea General y procedió a adoptar medidas sobre el proyecto de resolución A/C.2/64/L.49.

11. También en la misma sesión, se informó a la Comisión de que el proyecto de resolución A/C.2/64/L.49 no tenía consecuencias para el presupuesto por programas.
12. También en la 38ª sesión, la Comisión aprobó el proyecto de resolución A/C.2/64/L.49 (véase párr. 14, proyecto de resolución II).
13. Habida cuenta de la aprobación del proyecto de resolución A/C.2/64/L.49, el proyecto de resolución A/C.2/64/L.17 fue retirado por sus patrocinadores.

III. Recomendación de la Segunda Comisión

14. La Segunda Comisión recomienda a la Asamblea General que apruebe los siguientes proyectos de resolución:

Proyecto de resolución I
Creación de una cultura mundial de seguridad cibernética
y balance de las medidas nacionales para proteger las
infraestructuras de información esenciales

La Asamblea General,

Recordando sus resoluciones 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos, 57/239, de 20 de diciembre de 2002, relativa a la creación de una cultura mundial de seguridad cibernética, y 58/199, 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,

Recordando también sus resoluciones 53/70, de 4 de diciembre de 1998, 54/49, de 1º 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, y 63/37, de 2 de diciembre de 2008, relativas a los avances con respecto a las tecnologías de la información en el contexto de la seguridad internacional,

Recordando además los documentos finales de la Cumbre Mundial sobre la Sociedad de la Información celebrada en 2003 (primera fase) y en 2005 (segunda fase)¹,

Reconociendo que la confianza y la seguridad en la utilización de las tecnologías de la información y las comunicaciones son unos de los pilares más importantes de la sociedad de la información, y que es necesario alentar, fomentar, desarrollar y poner en práctica resueltamente una sólida cultura global de seguridad cibernética,

Reconociendo también la contribución cada vez mayor de las tecnologías de la información en red a muchas de las funciones esenciales de la vida cotidiana, el comercio y la prestación de bienes y servicios, la investigación, la innovación y la actividad empresarial, y a la libre circulación de información entre individuos y organizaciones, gobiernos, empresas y la sociedad civil,

Reconociendo además que, cada uno en su papel, los gobiernos, las empresas, otras organizaciones y los propietarios y usuarios individuales de las tecnologías de la información deben asumir sus responsabilidades y adoptar medidas para mejorar la seguridad de esas tecnologías de la información,

Reconociendo la importancia del mandato del Foro para la Gobernanza de Internet, como un diálogo entre múltiples interesados sobre diversos asuntos, entre ellos cuestiones de política pública relativas a elementos clave de la gobernanza de

¹ Véanse A/C.2/59/3 y A/60/687.

Internet a fin de fomentar la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet, y reiterando que todos los gobiernos deben tener igual cometido y responsabilidad respecto de la gobernanza de Internet y de la estabilidad, la seguridad y la continuidad de Internet,

Reafirmando la necesidad constante de una mayor cooperación que permita a los gobiernos cumplir en igualdad de condiciones su papel y responsabilidades en cuestiones de política pública internacional relativas a Internet, pero no en los asuntos técnicos y operacionales cotidianos que no repercutan en las cuestiones de política pública internacional,

Reconociendo que cada país determinará sus propias infraestructuras de información esenciales,

Reafirmando la necesidad de aprovechar el potencial de las tecnologías de la información y las comunicaciones para promover el logro de los objetivos de desarrollo internacionalmente convenidos, entre ellos los Objetivos de Desarrollo del Milenio, reconociendo que las lagunas en el acceso a las tecnologías de la información y su uso por los Estados pueden disminuir su prosperidad económica, y reafirmando también la eficacia de la cooperación para combatir la utilización de la tecnología de la información con fines delictivos y crear una cultura mundial de seguridad cibernética,

Destacando la necesidad de que se desplieguen mayores esfuerzos para cerrar la brecha digital con el fin de lograr el acceso universal a las tecnologías de la información y las comunicaciones y proteger las infraestructuras de información esenciales facilitando la transferencia de tecnología de la información y fomentando la capacidad de los países en desarrollo, en especial los países menos adelantados, en los ámbitos de las mejores prácticas y la capacitación en materia de seguridad cibernética,

Expresando preocupación porque las amenazas para el funcionamiento fiable de las infraestructuras de información esenciales y la integridad de la información transmitida por esas redes están aumentando en complejidad y gravedad y afectando al bienestar interno, nacional e internacional,

Afirmado que la seguridad de las infraestructuras de información esenciales es una responsabilidad que los gobiernos deben asumir de manera sistemática y una esfera en la que deben desempeñar un papel rector a nivel nacional, en coordinación con los interesados competentes, quienes a su vez deben ser conscientes de los riesgos correspondientes, las medidas de prevención y las respuestas efectivas de manera acorde con sus respectivas funciones,

Reconociendo que las medidas nacionales deben ir apoyadas por el intercambio de información y la colaboración a nivel internacional a fin de afrontar de manera efectiva el carácter cada vez más transnacional de esas amenazas,

Observando la labor realizada por las organizaciones regionales e internacionales competentes para mejorar la seguridad cibernética, y reiterando su función de alentar los esfuerzos nacionales y fomentar la cooperación internacional,

Observando también el informe de la Unión Internacional de Telecomunicaciones publicado en 2009 sobre la seguridad de la información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad, que se centra en un enfoque nacional amplio de la seguridad cibernética compatible

con la libertad de expresión, la libre circulación de información y las debidas garantías procesales,

Reconociendo que es beneficioso evaluar periódicamente los progresos en las medidas nacionales para proteger las infraestructuras de información esenciales,

1. *Invita* a los Estados Miembros a utilizar, siempre y cuando lo consideren procedente, el instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales que figura en el anexo a fin de contribuir a la evaluación de sus esfuerzos por proteger sus infraestructuras de información esenciales y fortalecer su seguridad cibernética de manera que se resalten los ámbitos en que se necesiten medidas adicionales con el objetivo de ampliar la cultura mundial de seguridad cibernética;

2. *Alienta* a los Estados Miembros y a las organizaciones regionales e internacionales pertinentes que hayan elaborado estrategias de seguridad cibernética y de protección de las infraestructuras de información esenciales a que compartan las mejores prácticas y las medidas que puedan ayudar a otros Estados Miembros en sus esfuerzos por facilitar el logro de la seguridad cibernética proporcionando esa información al Secretario General para que la recopile y la difunda entre los Estados Miembros.

Anexo

Instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales²

Balance de las necesidades y estrategias en materia de seguridad cibernética

1. Evaluar el papel de las tecnologías de la información y las comunicaciones en la economía, la seguridad nacional, las infraestructuras esenciales (como el transporte, el suministro de agua y alimentos, la salud pública, la energía, las finanzas y los servicios de emergencia) y la sociedad civil de su país.
2. Determinar los riesgos para la economía, la seguridad nacional, las infraestructuras esenciales y la sociedad civil de su país que deban gestionarse en el ámbito de la seguridad cibernética y la protección de las infraestructuras de información esenciales.
3. Comprender las vulnerabilidades de las redes en uso, los niveles relativos de riesgo a que se enfrenta cada sector en la actualidad y el plan de gestión en vigor, y señalar la manera en que los cambios en el entorno económico, las prioridades de seguridad nacional y las necesidades de la sociedad civil afectan a esos cálculos.
4. Determinar los objetivos de la estrategia nacional en materia de seguridad cibernética y protección de las infraestructuras de información esenciales; describir sus objetivos, el nivel de ejecución actual, las medidas existentes para medir los progresos, su relación con otros objetivos de política nacionales y la manera en que esa estrategia concuerda con las iniciativas regionales e internacionales.

² Instrumento voluntario que los Estados Miembros pueden utilizar, en parte o íntegramente, siempre y cuando consideren procedente como contribución a sus esfuerzos por proteger sus infraestructuras de información esenciales y fortalecer su seguridad cibernética.

Funciones y responsabilidades de los interesados

5. Determinar los principales interesados que participen en la seguridad cibernética y la protección de las infraestructuras de información esenciales y describir la función de cada uno de ellos en la elaboración de las políticas y operaciones pertinentes, incluidos:

- Los ministerios u organismos gubernamentales nacionales, señalando los principales puntos de contacto y las responsabilidades de cada uno;
- Otros participantes gubernamentales (locales y regionales);
- Los agentes no gubernamentales, entre ellos la industria, la sociedad civil y los estamentos académicos;
- Los particulares, señalando si el usuario medio de Internet tiene acceso a capacitación básica para evitar los riesgos en línea y si existe una campaña nacional de concienciación sobre la seguridad cibernética.

Procesos políticos y participación

6. Determinar los medios oficiales y oficiosos que existan en la actualidad para la colaboración entre el gobierno y la industria en la elaboración de políticas y operaciones en materia de seguridad cibernética y protección de las infraestructuras de información esenciales; determinar los participantes, sus funciones y objetivos, los métodos para obtener y utilizar las aportaciones y su idoneidad para el logro de los objetivos pertinentes en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

7. Determinar otros foros o estructuras que podrían necesitarse para integrar las perspectivas y los conocimientos gubernamentales y no gubernamentales necesarios para lograr los objetivos nacionales en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

Cooperación entre el sector público y el privado

8. Recopilar todas las medidas y planes adoptados para aumentar la cooperación entre el gobierno y el sector privado, incluyendo todo arreglo para intercambiar información y gestionar los incidentes.

9. Reunir todas las iniciativas actuales y previstas para promover intereses compartidos y enfrentar desafíos comunes entre los participantes encargados de las infraestructuras esenciales y los agentes del sector privado que dependan de las mismas infraestructuras esenciales interconectadas.

Gestión de incidentes y recuperación

10. Determinar el organismo gubernamental que coordine la gestión de los incidentes, incluida la capacidad para ejercer funciones de observación, alerta, respuesta y recuperación, los organismos gubernamentales colaboradores, los participantes no gubernamentales, incluidos la industria y otros asociados, y todo arreglo existente para la cooperación y el intercambio de información confiable.

11. Determinar, separadamente, la capacidad nacional de respuesta ante incidentes informáticos, incluidos los equipos de respuesta ante incidentes informáticos con responsabilidades nacionales y sus funciones y atribuciones, incluidos los instrumentos y procedimientos existentes para la protección de las redes

informáticas gubernamentales, y los instrumentos y procedimientos existentes para difundir información sobre la gestión de los incidentes.

12. Determinar las redes y los procesos de cooperación internacional que puedan reforzar la respuesta ante los incidentes y la planificación para imprevistos, la identificación de los asociados y los arreglos de cooperación bilateral y multilateral, cuando proceda.

Marcos jurídicos

13. Examinar y actualizar las autoridades jurídicas (incluidas las relacionadas con los delitos cibernéticos, la privacidad, la protección de los datos, el derecho comercial, las firmas digitales y el cifrado) que puedan estar anticuadas u obsoletas como resultado de la rápida incorporación de las nuevas tecnologías de la información y las comunicaciones y de la dependencia de esas tecnologías, y utilizar en esos exámenes los convenios, arreglos y precedentes regionales e internacionales. Determinar si su país ha elaborado la legislación necesaria para la investigación y el enjuiciamiento de la delincuencia cibernética, indicando los marcos existentes, por ejemplo, las resoluciones de la Asamblea General 55/63 y 56/121 relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos e iniciativas regionales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

14. Determinar la situación actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las competencias legales y las dependencias nacionales encargadas de las cuestiones relativas a la delincuencia cibernética, y el nivel de comprensión de esas cuestiones entre los fiscales, jueces y legisladores.

15. Evaluar la idoneidad de los códigos jurídicos y las autoridades actuales para hacer frente a los desafíos presentes y futuros de la delincuencia cibernética y del ciberespacio de forma más general.

16. Examinar la participación nacional en las iniciativas internacionales para luchar contra la delincuencia cibernética, como la Red permanente de puntos de contacto.

17. Determinar los requisitos para que los organismos nacionales de imposición de la ley cooperen con sus homólogos internacionales a fin de investigar los delitos cibernéticos transnacionales en los casos en que la infraestructura o los autores del delito se encuentren en el territorio nacional pero las víctimas residan en otros lugares.

Creación de una cultura mundial de seguridad cibernética

18. Resumir las medidas y los planes adoptados para crear la cultura nacional de seguridad cibernética a que se hace referencia en las resoluciones de la Asamblea General de las Naciones Unidas 57/239 y 58/199, incluida la ejecución de un plan de seguridad cibernética para los sistemas operados por el gobierno, de programas nacionales de concienciación y divulgación dirigidos, entre otros, a los niños y los usuarios individuales, y de actividades nacionales de capacitación en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

Proyecto de resolución II Ciencia y tecnología para el desarrollo

La Asamblea General,

Recordando sus resoluciones 58/200, de 23 de diciembre de 2003, 59/220, de 22 de diciembre de 2004, 60/205, de 22 de diciembre de 2005, y 62/201, de 19 de diciembre de 2007,

Recordando también su resolución 61/207, de 20 de diciembre de 2006, y la referencia que se hace en ella a la ciencia y la tecnología,

Tomando nota de las resoluciones del Consejo Económico y Social 2006/46 de 28 de julio de 2006, y 2009/8, de 24 de julio de 2009,

Reconociendo la función decisiva que la ciencia y la tecnología, incluidas las tecnologías ecológicamente racionales, pueden desempeñar en el desarrollo y la facilitación de los esfuerzos por erradicar la pobreza, lograr la seguridad alimentaria, luchar contra las enfermedades, mejorar la educación, proteger el medio ambiente, acelerar el ritmo de la diversificación y la transformación económicas y mejorar la productividad y la competitividad,

Recordando el Documento Final de la Cumbre Mundial 2005¹,

Recordando también los resultados de la Cumbre Mundial sobre la Sociedad de la Información²,

Reconociendo que el apoyo internacional puede ayudar a los países en desarrollo a beneficiarse de los adelantos tecnológicos y puede aumentar su capacidad productiva,

Recalcando la función que los conocimientos tradicionales pueden desempeñar en el desarrollo tecnológico y en la ordenación y el uso sostenibles de los recursos naturales,

Reconociendo la necesidad urgente de cerrar la brecha digital y ayudar a los países en desarrollo a tener acceso a los beneficios que puedan brindar las tecnologías de la información y las comunicaciones,

Alentando a perseverar en los esfuerzos por aplicar el Plan Estratégico de Bali para el apoyo tecnológico y la creación de capacidad del Programa de las Naciones Unidas para el Medio Ambiente³,

Reafirmando la necesidad de fortalecer los programas de ciencia y tecnología de las entidades pertinentes del sistema de las Naciones Unidas,

Observando con aprecio la colaboración entre la Comisión de Ciencia y Tecnología para el Desarrollo y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo para establecer una red de centros de excelencia en ciencia y tecnología para los países en desarrollo y para diseñar y realizar exámenes de las políticas de ciencia, tecnología e innovación,

¹ Véase la resolución 60/1.

² Véanse A/60/687 y A/C.2/59/3, anexo, cap.I.

³ UNEP/GC.23/6/Add.1 y Corr.1, anexo.

Tomando nota con interés del establecimiento de ONU-Biotech, la red interinstitucional de cooperación en materia de biotecnología descrita en el informe del Secretario General sobre ciencia y tecnología para el desarrollo⁴,

Tomando nota del informe del Secretario General,

Alentando la puesta en marcha de iniciativas orientadas a promover la participación del sector privado en la transferencia de tecnología y la cooperación tecnológica y científica,

1. *Reafirma su compromiso* de:

a) Fortalecer y mejorar los mecanismos existentes y apoyar las iniciativas de investigación y desarrollo, incluso mediante alianzas voluntarias entre el sector público y el privado, a fin de atender las necesidades especiales de los países en desarrollo en las esferas de la salud, la agricultura, la conservación, el uso sostenible de los recursos naturales y la ordenación del medio ambiente, la energía, la silvicultura y los efectos del cambio climático;

b) Promover y facilitar, según proceda, el acceso de los países en desarrollo a la tecnología y también al desarrollo, la transmisión y la difusión de la tecnología, incluida la tecnología ecológicamente racional y los correspondientes conocimientos especializados;

c) Ayudar a los países en desarrollo en sus esfuerzos por promover y elaborar estrategias nacionales de recursos humanos y ciencia y tecnología, que son elementos impulsores fundamentales de la creación de capacidad nacional para el desarrollo;

d) Promover y apoyar un mayor esfuerzo por desarrollar las fuentes de energía renovables, incluida la tecnología necesaria;

e) Aplicar políticas a nivel nacional e internacional para atraer inversiones públicas y privadas, nacionales y extranjeras, que permitan mejorar los conocimientos, transferir tecnología en condiciones mutuamente convenientes e incrementar la productividad;

f) Apoyar los esfuerzos que hacen los países en desarrollo, individual y colectivamente, para aprovechar las nuevas tecnologías agrícolas a fin de incrementar la productividad agrícola por medios ecológicamente sostenibles;

2. *Reconoce* que la ciencia y la tecnología, incluidas las tecnologías de la información y las comunicaciones, son decisivas para el logro de los objetivos de desarrollo convenidos internacionalmente, incluidos los Objetivos de Desarrollo del Milenio, y para la plena participación de los países en desarrollo en la economía mundial;

3. *Solicita* a la Comisión de Ciencia y Tecnología para el Desarrollo que sirva de foro para continuar ayudando al Consejo Económico y Social a cumplir sus funciones de centro de coordinación del seguimiento de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información² a nivel de todo el sistema, y para atender, en el contexto de su mandato y de conformidad con la resolución 2006/46 del Consejo, las necesidades especiales de los países en

⁴ A/64/168.

desarrollo en esferas como la agricultura, el desarrollo rural, las tecnologías de la información y las comunicaciones y la ordenación del medio ambiente;

4. *Alienta* a la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo a que, en colaboración con los asociados pertinentes, siga realizando exámenes de las políticas de ciencia, tecnología e innovación con miras a ayudar a los países en desarrollo y a los países de economía en transición a determinar las medidas necesarias para integrar las políticas de ciencia, tecnología e innovación en sus estrategias nacionales de desarrollo;

5. *Alienta* a la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo y a otras organizaciones pertinentes a que ayuden a los países en desarrollo en sus esfuerzos por integrar las políticas de ciencia, tecnología e innovación en las estrategias nacionales de desarrollo;

6. *Alienta* a los gobiernos a que aumenten y promuevan las inversiones en actividades de investigación y desarrollo de tecnologías ecológicamente racionales y a que fomenten la participación del sector empresarial y el sector financiero en el desarrollo de esas tecnologías, e invita a la comunidad internacional a que respalde esa labor;

7. *Alienta* a que se mantengan los arreglos existentes y se sigan promoviendo los proyectos conjuntos de investigación y desarrollo a nivel regional, subregional e interregional movilizando, cuando sea posible, los recursos científicos y de investigación y desarrollo existentes y creando redes de instalaciones científicas y equipos de investigación avanzados;

8. *Alienta* a la comunidad internacional a que, habida cuenta del diferente nivel de desarrollo de los países, continúe facilitando la difusión adecuada de conocimientos científicos y técnicos y la transferencia, el acceso y la adquisición de tecnología para los países en desarrollo, en condiciones equitativas, transparentes y mutuamente convenidas, de manera que favorezcan el bienestar social y económico en interés de la sociedad;

9. *Pide* a las entidades de las Naciones Unidas y otras organizaciones internacionales, la sociedad civil y el sector privado que sigan colaborando en la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, con miras a poner el potencial de las tecnologías de la información y las comunicaciones al servicio del desarrollo mediante la investigación de políticas sobre la brecha digital y los nuevos desafíos de la sociedad de la información, así como mediante actividades de asistencia técnica, con la participación de alianzas entre múltiples interesados;

10. *Solicita* al Secretario General que en su sexagésimo sexto período de sesiones le presente un informe sobre la aplicación de la presente resolución en el que figuren recomendaciones sobre las medidas complementarias que deberán adoptarse y se dé cuenta de la experiencia adquirida en la integración de las políticas de ciencia, tecnología e innovación en las estrategias nacionales de desarrollo.