Naciones Unidas A/C.2/58/L.74

Asamblea General

Distr. limitada
10 de diciembre de 2003
Español
Original: inglés

Quincuagésimo octavo período de sesiones
Segunda Comisión
Tema 91 b) del programa
Cuestiones de política macroeconómica: ciencia y tecnología para el desarrollo

Proyecto de resolución presentado por el Vicepresidente de la Comisión, Sr. Henri S. Raubenheimer (Sudáfrica) tras las consultas oficiosas celebradas en relación con el proyecto de resolución A/C.2/58/L.19

Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales

La Asamblea General,

Recordando sus resoluciones 57/239, de 20 de diciembre de 2002, sobre la creación de una cultura mundial de seguridad cibernética, 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, sobre el establecimiento de la base jurídica para luchar contra la utilización de las tecnologías de la información con fines delictivos, y 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, y 57/53, de 22 de noviembre de 2002, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,

Reconociendo que los gobiernos, las empresas, otras organizaciones y los usuarios particulares conceden cada vez más importancia a las tecnologías de la información para la promoción del desarrollo socioeconómico y el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información,

Observando también que cada vez hay más vínculos entre las infraestructuras esenciales de la mayoría de los países —como las utilizadas para, entre otras cosas, la generación, transmisión y distribución de energía, el transporte aéreo y marítimo, los servicios bancarios y financieros, el comercio electrónico, el suministro de agua, la distribución de alimentos y la salud pública— y las infraestructuras de información esenciales que interconectan y afectan cada vez más sus operaciones,

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

Reconociendo que esa creciente interdependencia tecnológica se basa en una red compleja de componentes de las infraestructuras de información esenciales,

Observando que, como resultado de la creciente interconectividad, las infraestructuras de información esenciales están hoy expuestas a un número cada vez mayor y más variado de amenazas y vulnerabilidades que plantean nuevos problemas de seguridad,

Observando que la protección efectiva de las infraestructuras esenciales consiste, entre otras cosas, en determinar las amenazas y reducir la vulnerabilidad a que están expuestas las infraestructuras de información esenciales, reducir al mínimo los daños y el tiempo de recuperación en caso de daño o ataque, e identificar la causa del daño o la fuente del ataque,

Reconociendo que la protección efectiva exige comunicación y cooperación a nivel nacional e internacional entre todos los interesados y que los esfuerzos que se realizan a nivel nacional deberían ir apoyados por una cooperación efectiva y sustantiva a nivel internacional y regional entre los interesados,

Reconociendo también que las disparidades entre los Estados en el acceso a las tecnologías de la información y en su utilización pueden reducir la eficacia de la cooperación para combatir la utilización de las tecnologías de la información con fines delictivos y crear una cultura mundial de seguridad cibernética, y teniendo en cuenta la necesidad de facilitar la transferencia de las tecnologías de la información, en particular a los países en desarrollo,

Reconociendo además la importancia de la cooperación internacional para lograr la seguridad cibernética y la protección de las infraestructuras de información esenciales mediante el apoyo de los esfuerzos realizados a nivel nacional para mejorar la capacidad humana, crear más oportunidades de aprendizaje y empleo, mejorar los servicios públicos y elevar la calidad de vida aprovechando unas tecnologías y redes de información y comunicaciones avanzadas, fiables y seguras y promoviendo el acceso universal,

Observando también la labor que realizan las organizaciones internacionales y regionales pertinentes para mejorar la seguridad de las infraestructuras de información esenciales,

Reconociendo que deberían hacerse esfuerzos para proteger las infraestructuras de información esenciales teniendo debidamente en cuenta las leyes nacionales aplicables a la protección de la privacidad y otra legislación pertinente,

1. *Toma nota* de los elementos enunciados en el anexo de la presente resolución para proteger las infraestructuras de información esenciales;

2. *Invita* a todas las organizaciones internacionales pertinentes, incluidos los órganos de las Naciones Unidas competentes, a que consideren como corresponda esos elementos, entre otras cosas, para proteger las infraestructuras de información esenciales en toda labor futura en materia de seguridad cibernética o de protección de infraestructuras esenciales;

3. *Invita* a los Estados Miembros a que consideren , entre otras cosas, esos elementos al desarrollar sus estrategias para reducir los riesgos que afectan a las infraestructuras de información esenciales, de conformidad con las leyes y reglamentos nacionales;

4. *Invita* a los Estados Miembros y a todas las organizaciones internacionales pertinentes a que en los preparativos de la segunda fase de la Cumbre Mundial

sobre la Sociedad de la Información que se celebrará en Túnez en 2005 tengan en cuenta, entre otras cosas, esos elementos y la necesidad de proteger las infraestructuras de información esenciales;

5. *Alienta* a los Estados Miembros y a las organizaciones regionales e internacionales pertinentes que hayan elaborado estrategias de seguridad cibernética y protección de infraestructuras de información esenciales que compartan las mejores prácticas y medidas que puedan ayudar a otros Estados Miembros en sus esfuerzos por facilitar la seguridad cibernética;

6. *Subraya* la necesidad de que se hagan más esfuerzos para acabar con las disparidades de acceso a las tecnologías de la información y las comunicaciones, lograr acceso universal a éstas y proteger las infraestructuras de información esenciales facilitando la transferencia de tecnologías de la información y creación de capacidad, en particular a los países en desarrollo, especialmente los países menos adelantados, para que todos los Estados puedan beneficiarse plenamente de las tecnologías de la información y las comunicaciones para su desarrollo socioeconómico.

Anexo
Elementos para la protección de las infraestructuras de información esenciales

1. Contar con redes de alerta de emergencia en relación con las vulnerabilidades, las amenazas y los incidentes cibernéticos.

2. Crear más conciencia para que los interesados entiendan la naturaleza y el alcance de sus infraestructuras de información esenciales y la función que debe desempeñar cada uno en su protección.

3. Examinar las infraestructuras y determinar las interdependencias de éstas, mejorando así su protección.

4. Promover alianzas entre las partes interesadas, tanto públicas como privadas, para compartir y analizar información sobre las infraestructuras esenciales a fin de prevenir e investigar los daños y los ataques contra dichas infraestructuras, y responder a ellos.

5. Crear y mantener redes de comunicación para casos de crisis y probarlas para asegurarse de que seguirán siendo estables y seguras en situaciones de emergencia.

6. Garantizar que en las políticas sobre disponibilidad de datos se tenga en cuenta la necesidad de proteger las infraestructuras de información esenciales.

7. Facilitar el rastreo de los ataques contra las infraestructuras de información esenciales y, cuando corresponda, revelar la información recabada a otros Estados.

8. Ofrecer capacitación y hacer prácticas para mejorar las capacidades de respuesta y probar planes de continuidad y contingencia en el caso de un ataque contra las infraestructuras de información, y alentar a las partes interesadas a emprender actividades similares.

9. Contar con leyes sustantivas y de procedimiento adecuadas y personal capacitado para que los Estados puedan investigar los ataques contra las infraestructuras de información esenciales y enjuiciar a los responsables, y coordinar dichas investigaciones con otros Estados, cuando corresponda.

10. Cooperar a nivel internacional, cuando corresponda, para proteger las infraestructuras de información esenciales, incluso desarrollando y coordinando sistemas de alerta de emergencia, compartiendo y analizando información sobre vulnerabilidades, amenazas e incidentes y coordinando las investigaciones sobre los ataques contra dichas infraestructuras de conformidad con las leyes nacionales.

11. Promover la investigación y el desarrollo a nivel nacional e internacional y alentar la aplicación de tecnologías de seguridad que cumplan las normas internacionales.