Naciones Unidas A/59/116/Add.1*

Asamblea General

Distr. general
28 de diciembre de 2004
Español
Original: español/inglés

Quincuagésimo noveno período de sesiones
Tema 60 del programa
Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General**

Adición

Índice

* Publicado nuevamente por razones técnicas.

** La información contenida en el presente informe se recibió después de que se presentara el informe principal.

04-47514* (S) 100105 100105

Respuestas recibidas de los Estados Miembros

Estados Unidos de América

[Original: inglés]
[13 de julio de 2004]

1. La seguridad efectiva de las redes e infraestructuras informáticas es esencial para garantizar la fiabilidad, disponibilidad e integridad de las redes informáticas nacionales y mundiales de las que dependen cada vez más los Estados y sus ciudadanos para el uso de servicios esenciales y para su seguridad económica. La cuestión que se debe abordar es qué pueden hacer las naciones, individual y colectivamente, para aumentar la seguridad de las redes e infraestructuras informáticas e impedir ataques destructivos.

2. Algunos Estados creen que ese objetivo se puede lograr mediante un convenio internacional que limitaría el desarrollo o la utilización de una amplia variedad de tecnologías de la información. Implícita en esas propuestas estaría la concesión a los gobiernos del derecho de aprobar o prohibir la transmisión al territorio nacional desde fuera de sus fronteras de información considerada de carácter desestabilizador desde el punto de vista político, social o cultural.

3. Los Estados Unidos de América no creen que este enfoque contribuya al objetivo de fortalecer la seguridad de los sistemas mundiales de información y comunicaciones, sino que, a su juicio, contraviene el principio de la libre circulación de información indispensable para el crecimiento y el desarrollo de todos los Estados. Las medidas que se adopten para garantizar la seguridad informática no deben coartar la libertad que todo individuo tiene de buscar, recibir e impartir informaciones e ideas y de difundirlas por cualquier medio de expresión, incluidos los medios electrónicos, y sin limitación de fronteras, como se establece en el artículo 19 de la Declaración Universal de Derechos Humanos.

4. Por el contrario, los Estados Unidos de América creen que la principal amenaza a la seguridad cibernética se origina en los incesantes ataques alevosos de delincuentes organizados, piratas cibernéticos y agentes no estatales, inclusive terroristas. Desde esta perspectiva, la mejor forma de proteger los beneficios del espacio cibernético es mediante la penalización efectiva por parte del Estado del uso indebido de la tecnología de la información y mediante la aplicación sistemática a nivel nacional de medidas encaminadas a prevenir daños a las infraestructuras informáticas esenciales sobre las que se apoya dicha tecnología, sin importar la fuente de la amenaza, algo que los Estados Unidos de América llaman la creación de una cultura global de la seguridad cibernética. En esta visión, todas las partes (gobiernos, empresas y sociedad civil) son conscientes de sus responsabilidades y actúan conforme a sus funciones para garantizar la seguridad cibernética.

5. Con respecto a las aplicaciones militares de la tecnología de la información, no es necesario en absoluto un convenio internacional, pues existe ya el derecho de los conflictos armados y sus principios de necesidad, proporcionalidad y limitación de daños indirectos, que rigen la utilización de dicha tecnología.

La seguridad cibernética mediante la prevención

6. La mejor forma de lograr la seguridad cibernética es mediante la actuación de los Estados a nivel nacional y su cooperación a nivel internacional para garantizar la seguridad de sus propias infraestructuras informáticas esenciales. Cada Estado debería establecer un programa nacional con el fin de:

a) Educar y crear conciencia sobre las mejores prácticas en materia de seguridad de las redes e infraestructuras informáticas;

b) Penalizar efectivamente el uso indebido de la tecnología de la información;

c) Fomentar una alianza entre gobierno e industria para otorgar incentivos con miras a garantizar la seguridad de sus sistemas nacionales;

d) Establecer un mecanismo de alerta y respuesta en caso de incidentes y procedimientos de intercambio de información, tanto a nivel nacional como internacional.

7. Cada Estado debería procurar crear una cultura de la seguridad cibernética entre todas las partes interesadas, es decir, gobierno, empresas y usuarios particulares, y facilitar la cooperación internacional entre los Estados al objeto de crear una cultura global de la seguridad cibernética.

8. En el informe del Grupo de Expertos Gubernamentales deberían subrayarse los aspectos contenidos en las resoluciones de la Asamblea General 55/63, de 4 de diciembre de 2000, 56/121, de 19 de diciembre de 2001, ambas tituladas “Lucha contra la utilización de la tecnología de la información con fines delictivos”, y 57/239, de 20 de diciembre de 2002, titulada “Creación de una cultura mundial de seguridad cibernética”. El informe podría aprovechar dichos aspectos para incorporar referencias específicas a medidas para fomentar los principios de seguridad cibernética que los Miembros ya han aprobado. Dichos esfuerzos se podrían inspirar en actividades multilaterales llevadas a cabo recientemente para potenciar la seguridad cibernética a nivel regional, como las del Foro de Telecomunicaciones de la Cooperación Económica en Asia y el Pacífico, la Organización de los Estados Americanos, la Cumbre Mundial sobre la Sociedad de la Información y el Grupo de los Ocho.

9. Las costosas amenazas a la integridad y la disponibilidad de las infraestructuras informáticas nacionales y mundiales se derivan en su inmensa mayoría del uso indebido con fines delictivos. Desde la perspectiva de los Estados Unidos de América, es mucho más importante que los gobiernos adopten medidas para investigar y enjuiciar efectivamente a los individuos que participan en esas actividades. Por esta razón, los Estados Unidos de América y otros 34 Estados han firmado el Convenio sobre el Delito Cibernético del Consejo de Europa, de 23 de noviembre de 2001, en el cual figuran directrices para la promulgación de legislación nacional y para la cooperación transfronteriza entre las autoridades encargadas de velar por el cumplimiento de la ley. El Consejo de Europa espera abrir el Convenio a la adhesión de países que no son miembros del Consejo, de conformidad con su práctica habitual y con lo dispuesto en el artículo 37 del Convenio. De hecho, todos los países, sean o no parte en el Convenio, pueden utilizarlo inmediatamente como modelo para elaborar leyes nacionales eficaces contra el delito cibernético.

10. Además, independientemente del origen o de la motivación de un ataque, los instrumentos utilizados y el daño sufrido por los sistemas informáticos son de carácter similar. Así pues, es más importante que todas las naciones adopten medidas sistemáticas para reducir la vulnerabilidad de sus sistemas y educar a sus ciudadanos

en una cultura de la seguridad cibernética, es decir, un conjunto de prácticas y hábitos de seguridad concebidos para salvaguardar sus infraestructuras informáticas.

11. La protección efectiva de las redes e infraestructuras informáticas esenciales pasa por la reducción de la vulnerabilidad de dichas infraestructuras a cualquier tipo de ataque, a fin de reducir al mínimo el daño y el tiempo de recuperación en caso de que se produzcan daños.

12. La protección efectiva también hace necesaria la comunicación, la coordinación y la cooperación a nivel nacional e internacional entre todas las partes interesadas, es decir, la industria, los círculos académicos, el sector privado y las entidades gubernamentales, sin olvidar los organismos encargados de proteger las infraestructuras y velar por el cumplimiento de la ley. Dichas actividades deben realizarse teniendo debidamente en cuenta la seguridad de la información y la legislación vigente en materia de asistencia judicial recíproca y protección de la privacidad. Al objeto de alcanzar esos objetivos, se debe alentar a los Estados a que, al formular su estrategia para reducir los riesgos a sus infraestructuras informáticas esenciales, apliquen los 11 principios enunciados por los expertos de los países miembros del Grupo de los Ocho en protección de las infraestructuras informáticas esenciales y aprobados por los ministros de justicia e interior de esos países en mayo de 2003:

a) Los países deberían disponer de redes de alerta en caso de emergencia ante posibles vulnerabilidades, amenazas e incidentes de carácter cibernético;

b) Los países deberían concienciar a las partes interesadas para facilitar su comprensión de la naturaleza y el alcance de sus infraestructuras informáticas esenciales, y de la función que les corresponde a la hora de proteger dichas infraestructuras;

c) Los países deberían examinar sus infraestructuras y determinar las interdependencias existentes entre ellas, a fin de garantizar un mayor grado de protección de dichas infraestructuras;

d) Los países deberían promover alianzas entre las partes interesadas, tanto de carácter público como privado, al objeto de compartir y analizar información relativa a sus infraestructuras esenciales y así prevenir, investigar y hacer frente a daños o ataques a dichas infraestructuras;

e) Los países deberían crear y mantener redes de comunicación para situaciones de crisis y ponerlas a prueba para verificar su seguridad y estabilidad en situaciones de emergencia;

f) Los países deberían asegurarse de que en sus políticas de disponibilidad de datos se tenga en cuenta la necesidad de proteger las estructuras informáticas esenciales;

g) Los países deberían facilitar la localización de ataques a las infraestructuras informáticas esenciales y, según proceda, la divulgación a otros países de información relativa a dicha localización;

h) Los países deberían impartir capacitación y llevar a cabo ejercicios para aumentar su capacidad de respuesta y poner a prueba sus planes de continuidad y contingencias, en previsión de un ataque a las infraestructuras informáticas, y deberían alentar a las partes interesadas a que realicen actividades similares;

i) Los países deberían asegurarse de que cuentan con leyes sustantivas y de procedimiento adecuadas, como las descritas en el Convenio sobre el Delito Cibernético del Consejo de Europa, y de que disponen de personal debidamente preparado para investigar y castigar ataques a las infraestructuras informáticas esenciales, además de coordinar dichas investigaciones con otros países, según proceda;

j) Los países deberían cooperar a nivel internacional, según proceda, para proteger las infraestructuras informáticas esenciales, entre otras cosas perfeccionando y coordinando sus sistemas de alerta en caso de emergencia, compartiendo y analizando información sobre vulnerabilidades, amenazas e incidentes y coordinando las investigaciones de ataques a dichas infraestructuras de conformidad con las leyes nacionales;

k) Los países deberían promover la investigación y el desarrollo a nivel nacional e internacional y alentar la aplicación de tecnologías de seguridad certificadas conforme a criterios internacionales.

13. La seguridad efectiva de las redes e infraestructuras informáticas se puede apoyar por medios tecnológicos y potenciar mediante actividades de divulgación y capacitación, desarrollo normativo y legislativo y cooperación internacional.

14. Se debería apoyar a las Naciones Unidas y a otras organizaciones multilaterales en sus esfuerzos por alentar a los Estados Miembros a que:

a) Evalúen la seguridad de sus redes e infraestructuras informáticas esenciales, y comprendan sus vulnerabilidades e interdependencias;

b) Eduquen y creen conciencia a nivel nacional sobre las mejores prácticas en materia de seguridad de las redes e infraestructuras informáticas;

c) Penalicen efectivamente el uso indebido de la tecnología de la información y faciliten las investigaciones transfronterizas de delitos cibernéticos;

d) Fomenten una alianza entre gobierno e industria para otorgar incentivos al objeto de garantizar la seguridad de sus sistemas nacionales;

e) Establezcan un mecanismo nacional de alerta y respuesta en caso de incidentes y procedimientos de intercambio de información tanto a nivel nacional como internacional.

México

[Original: español]
[18 de agosto de 2004]

1. La era actual, caracterizada por un sorprendente desarrollo de los sistemas de información y de las telecomunicaciones, ha sensibilizado a la comunidad internacional respecto del hecho de que, paralelamente a tal adelanto, se ha consolidado una interconexión de usuarios de dichos sistemas de tal magnitud y de diversa naturaleza que las fronteras territoriales y jurídicas de los Estados han sido traspasadas.

2. Tal nivel de interrelación ha propiciado a su vez un grado directamente proporcional de vulnerabilidad en el ámbito de la seguridad nacional e internacional, confirmando con ello que la información y los sistemas de telecomunicaciones son

rubros estratégicos que inciden de manera importante en las condiciones de paz y seguridad internacionales.

3. Es por ello que México considera que las medidas a adoptar para limitar las amenazas que surjan en este ámbito, además de ser consistentes con la necesidad de preservar la libre circulación de la información y promover el desarrollo con fines pacíficos de estos elementos, debe de aportar beneficios tangibles a favor del desarme y la no proliferación, del acercamiento entre las naciones, así como propiciar una mayor cooperación internacional en la materia.

4. Se estima que el campo de la información y de las telecomunicaciones debe ser examinado bajo una óptica dinámica, y de prospectiva, dado que de por sí el ritmo de progreso del desarrollo científico y tecnológico ha propiciado un desfase entre las normas a observar y las capacidades reales de tales sistemas, con lo que de forma inmediata se incrementan las amenazas potenciales y reales en el campo de la seguridad de la información.

5. Dada la actualidad de este tema y la relevancia del examen de los conceptos que permitirán referirnos con mayor precisión a este fenómeno a fin de enfrentarlo debidamente, México alienta la labor que en febrero de este año inició con el propósito de establecer un grupo de expertos gubernamentales que colaborará con el Secretario General de las Naciones Unidas en la elaboración de un estudio relativo al examen de las amenazas reales y potenciales en el ámbito de la seguridad de la información, y de las posibles medidas de cooperación para hacerles frente, así como de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones, como se indica en los párrafos dispositivos 4 y 2 de la resolución 58/32. En este sentido espera que el informe que sea presentado a la Asamblea General de las Naciones Unidas en su sexagésimo período de sesiones contenga recomendaciones sustantivas y logre avances en la definición conceptual y jurídica del tema.

6. En tal propósito, México considera que serán de utilidad los desarrollos y discusiones sobre el tema efectuados en el marco de las otras comisiones de la Asamblea General, disposiciones relevantes contenidas en instrumentos internacionales vigentes, así como los avances logrados por otras organizaciones internacionales. —verbigracia la UNESCO— en materia de seguridad internacional, terrorismo internacional e información y sociedad de la información.

7. En cuanto al párrafo dispositivo 3, sobre la determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada en los sistemas de información, en particular la injerencia no autorizada en los sistemas de información y de telecomunicaciones y los recursos de información o la utilización ilícita de esos sistemas y recursos México insiste en que el concepto de injerencia no autorizada puede dar lugar a confusiones no deseadas, ya que tiene una connotación vinculada a acciones emprendidas por ciertos Estados que, invocando discutibles razones humanitarias u otras, intervienen de manera individual o concertada en asuntos de otros Estados.

8. En este sentido, bien podría omitirse tal concepto y sustituirse por “acceso no permitido” o únicamente “acceso ilegal” para referirse a los actos que realizan algunas personas o entidades en los sistemas de información.

9. Ante la evidente preocupación sobre los problemas de seguridad que se enmarcan en la posible vulnerabilidad de los sistemas de información que regulan los programas de defensa de algunos países, así como del riesgo de la utilización de la informática y de las telecomunicaciones por terroristas o con fines de disuasión, México reafirma que sólo el diálogo, la negociación, la cooperación internacional y el derecho internacional constituyen las vías para evitar que las medidas qué se establezcan respecto de los problemas de seguridad de la información medren en alguna medida la libertad de información y de comunicación.

Venezuela

[Original: español]
[28 de junio de 2004]

1. El Gobierno de la República Bolivariana de Venezuela considera que toda violación a la seguridad de la información es contraria al derecho de los Estados de ejercer plena y legítimamente su soberanía, y en ese sentido, el empleo de los medios y tecnologías de información con fines de desestabilización política y económica es contrario a los valores fundamentales de la democracia.

2. La seguridad de la información tiene entonces un doble carácter, por una parte lo relativo a la garantía de su resguardo y protección; y por la otra, el buen empleo y veracidad de la misma. Tanto la utilización ilícita como la no utilización deliberada de los sistemas de información y de telecomunicaciones o de los recursos de información, con fines desestabilizadores, constituye un factor perturbador en el contexto de la seguridad internacional.

3. La República Bolivariana de Venezuela comparte la elaboración de principios internacionales que propenden a aumentar la seguridad de los sistemas de información y telecomunicaciones mundiales que permitan o faciliten la lucha contra el terrorismo y la delincuencia en la esfera de la información, sin menoscabo de la soberanía de los Estados.