



Asamblea General

Distr. general
3 de julio de 2001
Español
Original: español/inglés

Quincuagésimo sexto período de sesiones

Tema 81 de la lista preliminar*

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

Índice

	<i>Página</i>
I. Introducción	2
II. Respuestas recibidas de los gobiernos	2
Bolivia	2
Filipinas	2
México	4
Suecia**	6

* A/56/50.

** En nombre de los Estados miembros de la Unión Europea que son Miembros de las Naciones Unidas.

I. Introducción

1. La Asamblea General, en su resolución 55/28, de 20 de noviembre de 2000, sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, invitó a todos los Estados Miembros a que siguieran haciendo llegar al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) evaluación general de los problemas de la seguridad de la información; b) determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de sistemas de información y de telecomunicaciones y de recursos de información; y c) el contenido de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones; y pidió al Secretario General que le presentara un informe en su quincuagésimo sexto período de sesiones sobre la base de las respuestas que recibiera de los Estados Miembros.

2. El 19 de marzo de 2001, el Secretario General dirigió una nota verbal a los Estados Miembros en que les solicitaba que le ofreciesen sus puntos de vista, de conformidad con la invitación de la Asamblea General. Las respuestas recibidas de los gobiernos hasta el 3 de julio de 2001 se reproducen en la sección II del presente informe. Cualesquiera otras respuestas recibidas serán publicadas como adición del presente informe.

II. Respuestas recibidas de los gobiernos

Bolivia

[Original: español]
[14 de junio de 2001]

De acuerdo con la información recibida de la Cancillería boliviana, las fuerzas armadas de Bolivia, en la actualidad, no poseen medios electrónicos adecuados, ni tienen prevista su adquisición o fabricación en el futuro.

Filipinas

[Original: inglés]
[22 de mayo de 2001]

1. Evaluación general de los problemas de la seguridad de la información

1. La complejidad y la amplitud de los problemas y las cuestiones relativos a la seguridad de la información son inmensas, lo que hace de la seguridad de la información una grave cuestión mundial. Las amenazas planteadas por los problemas que se presentan en la actual era de la información están aumentando rápidamente. Cada nuevo avance e innovación tecnológico también crea nuevas oportunidades que se pueden explotar en contra de una buena visión de la humanidad.

2. El problema de la seguridad de la información plantea una amenaza similar a la de las armas de destrucción en masa. Están amenazados todos los aspectos de la existencia humana. Se trata de un problema que ninguna nación o grupo de naciones puede encarar por cuenta propia. En consecuencia, se trata de una inquietud mundial

que requiere, con carácter urgente, una seria respuesta concertada de todas las naciones, sean éstas tecnológicamente avanzadas o no.

2. Determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de sistemas de información y de telecomunicaciones y los recursos de información

3. Los criterios básicos siguientes se podrían definir de la manera siguiente:

a) **Injerencia no autorizada o penetración no aprobada.** i) Un acto de injerencia no gubernamental; o ii) injerencia aprobada por el gobierno que no se encuentre dentro del régimen o los protocolos internacionales establecidos de seguridad de la información;

b) **Injerencia autorizada.** “Injerencia” iniciada por el gobierno de la manera aprobada por los tratados internacionales o dentro de los límites de un régimen o los protocolos internacionales establecidos de seguridad de la información;

c) **Uso no aprobado de la información.** i) Uso de información pública y privada obtenida ilegal y legalmente sin la autorización previa de las fuentes; ii) uso de información vital pública y privada, obtenida ilegal y legalmente por entidades gubernamentales con fines personales, no gubernamentales; iii) uso de información vital, pública y privada, obtenida ilegal y legalmente por el gobierno, fuera del marco de un régimen o de los protocolos internacionales establecidos de seguridad de la información y otros tratados y leyes internacionales conexos;

d) **Uso ilícito de sistemas de información y telecomunicaciones.** i) Uso de recursos de información y telecomunicaciones, incluso las infraestructuras conexas, con fines dolosos; y ii) todo uso no aprobado de la información;

e) **Recursos de información.** Datos no procesados y procesados (por ejemplo, estadísticas, hechos, cifras, registros, etc.), programas informáticos, equipo técnico/cibernético (por ejemplo, computadoras personales, computadoras portátiles, escáneres y otras formas de tecnología nuevas y adelantadas), tecnología de la información y otros servicios conexos (por ejemplo, torres de transmisión, discos de satélite, torres/edificios de control), expertos y profesionales de tecnología de la información (por ejemplo, programadores de computadoras, analistas de sistemas, etc.), incluso redes y sistemas de información y cibernéticos (Internet);

f) **Armas de información.** Recursos de información elaborados o creados estratégicamente para la guerra de información o para causar daños, confusión, desventajas y cualquier otra forma de actividad dolosa;

g) **Guerra de información.** i) Actividades encaminadas a lograr superioridad en materia de información mediante la ejecución de medidas orientadas a explotar, corromper, destruir, desestabilizar o dañar la información del enemigo y sus funciones; ii) actividades encaminadas a proteger los recursos de información y los sistemas de telecomunicaciones propios; iii) actividades encaminadas a explotar los recursos de información y los sistemas de telecomunicaciones propios para el logro de metas e intereses, por ejemplo, guerra cibernética (guerra de información en el contexto de la defensa y militar), guerra en la Internet (guerra de la información en el contexto más amplio de la sociedad);

h) **Terrorismo de la información.** Actos de terrorismo en el contexto de la seguridad de la información;

i) **Delitos cibernéticos o delitos de la información.** i) Actos criminales relacionados con elementos de la seguridad de la información; ii) actos dolosos dirigidos contra recursos de información (por ejemplo, vandalismo técnico, intrusión técnica, destrucción indiscriminada de archivos electrónicos); iii) toda injerencia no autorizada o penetración no aprobada;

j) **Delincuentes técnico/cibernético.** i) Personas que cometen actos en violación de los regímenes o protocolos internacionales establecidos sobre seguridad de la información; ii) personas cuyos actos criminales entrañan el uso de la seguridad de la información o dependen en gran medida de ella; iii) personas que repetidamente cometen actos dirigidos contra los recursos de la información (se debería exceptuar a los menores de ser condenados como tecnodelincuentes);

k) **Colonización de la información.** i) Actos cometidos por un Estado contra otro Estado para dominar y controlar el ámbito de la información e impedir el acceso a la tecnología de la información más moderna y crear una situación en que otros Estados queden en situación de dependencia tecnológica en la esfera de la información; ii) actos de expansión de la información y adquisición de un monopolio sobre la infraestructura de la información y las telecomunicaciones nacional de otro Estado, creando así condiciones de dependencia y control;

l) **Naciones tecnológicamente adelantadas.** i) Países cuya economía está conectada electrónicamente en más del 50%; ii) en general podrá referirse a los países desarrollados.

3. **El contenido de los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones mencionados en el párrafo 2 de la resolución 55/28**

4. La propuesta de establecer un régimen internacional sobre seguridad de la información es sumamente crucial en este momento. En las propuestas de ese tipo se debería velar por la rendición de cuentas por parte de los Estados que violen dichos protocolos sobre la seguridad de la información. También se debería establecer un equilibrio entre las naciones tecnológicamente avanzadas y las que no lo son. En el régimen se debería estudiar a las naciones tecnológicamente avanzadas que ya están realizando su propia forma de “injerencia” contra las naciones que se encuentran en desventaja. Por último, en el régimen se debería considerar seriamente que el “cumplimiento de la ley” es un factor vital en el mejoramiento de la seguridad de la información a escala internacional. Ello se podía poner en práctica mediante la creación de un centro internacional que coordine a las dependencias encargadas del cumplimiento de la ley de las distintas naciones para rastrear a los sospechosos, así como ayudar a dichas naciones en sus operaciones internas.

México

[Original: español]
[16 de mayo de 2001]

1. México considera necesario dirigir mayores esfuerzos hacia el fomento de las aplicaciones civiles de los avances científicos y tecnológicos y de los medios de información. México apoyó las resoluciones 53/70, de 4 de diciembre de 1998, y 54/49,

de 1° de diciembre de 1999, de la Asamblea General, tituladas “Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”.

2. Actualmente, las principales percepciones sobre problemas de seguridad se enmarcan en la posible vulnerabilidad de los sistemas de información que regulan los programas de defensa de algunos países, así como el riesgo de la utilización de la informática y de las telecomunicaciones por terroristas o con fines de disuasión.

3. Al respecto, sólo la cooperación internacional y el derecho internacional constituyen las vías para evitar que las medidas que se establezcan respecto a los problemas de seguridad de la información mermen en alguna medida la libertad de información y de comunicación.

4. Es indudable la importancia de este campo. Sin embargo, deberán tenerse también presentes los desarrollos y discusiones efectuadas en el marco de las otras comisiones de la Asamblea General, que podrían contribuir de manera importante a la definición y precisión de conceptos que podrían emplearse para el examen de los problemas relacionados con la seguridad de la información.

5. Por lo que respecta a la cuestión relativa a la determinación de criterios o conceptos internacionales básicos relacionados con la seguridad de la información, México considera 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.

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

7. En relación con la necesidad de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales, es preciso subrayar que dichos principios no sólo deberán aumentar la seguridad de los sistemas sino garantizarla legalmente de una manera más eficaz.

8. Asimismo, es conveniente realizar un examen riguroso de las disposiciones relevantes contenidas en instrumentos internacionales adoptados a lo largo de los años tanto por la Asamblea General como por otras organizaciones internacionales —verbigracia la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura— en materia de seguridad internacional, terrorismo internacional e información con el objeto de identificar y evaluar los principios existentes pertinentes de aplicación en este campo.

9. México coincide al respecto, con la resolución 51/210, de 17 de diciembre de 1996, relativa a las medidas para eliminar el terrorismo internacional, particularmente el párrafo 3 c) de la parte I en que se hace alusión a los peligros de la utilización de los sistemas de comunicación, electrónicos, de redes de datos en actos terroristas, así como a la necesidad de encontrar medios consistentes con el derecho internacional, promover la cooperación para prevenir dicha criminalidad.

10. Durante el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado en Viena, del 10 al 17 de abril de 2000, la Secretaría elaboró un documento titulado “Delitos relacionados con las redes informáticas” (A/CONF.187/10), el cual señala que para combatir y prevenir

eficazmente los delitos cibernéticos es necesario un enfoque internacional coordinado a diferentes niveles.

11. En el ámbito interno, la investigación de esos delitos requiere expertos, conocimientos especializados y procedimientos adecuados. Se alienta a los Estados a considerar la posibilidad de crear mecanismos que permitan obtener oportunamente datos exactos de los sistemas y redes informáticas cuando estos datos se requieren como prueba en procedimientos judiciales.

12. A nivel internacional, la investigación eficaz de los delitos cibernéticos requiere una actuación oportuna, facilitada por la coordinación entre los organismos nacionales de aplicación de la ley y la autoridad legal pertinente.

Suecia*

[Original: inglés]
[26 de junio de 2001]

1. En el quincuagésimo quinto período de sesiones de la Asamblea General de las Naciones Unidas, los Estados miembros de la Unión Europea respaldaron el consenso en relación con la resolución 55/28 de la Asamblea, titulada “Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”. Los Estados miembros de la Unión Europea desean presentar la siguiente respuesta común al párrafo 3 de la resolución, en que se invita a los Estados Miembros de las Naciones Unidas a que hagan llegar al Secretario General sus opiniones y observaciones.

1. Observaciones generales sobre las cuestiones relativas a la seguridad de la información

2. La tecnología de la información y las telecomunicaciones facilita enormemente la libre circulación de la información y redundante en considerables beneficios para los particulares, las empresas y los gobiernos de todo el mundo. Además, promueve la democracia y la libertad de expresión, así como el adelanto de la sociedad civil. La Unión Europea considera que es importante fomentar y lograr el mayor desarrollo posible de la tecnología de la información y las telecomunicaciones, y fortalecer al mismo tiempo el principio de la libertad de la información. La Unión Europea reconoce que puede haber una injerencia no autorizada o un uso indebido que pongan en peligro los sistemas de información y telecomunicaciones, la integridad de las infraestructuras basadas en la información y los recursos de información de particulares, empresas, instituciones educativas o médicas y otras organizaciones del sector privado, así como de los gobiernos.

3. La seguridad de la información y de las redes debe garantizar la identidad de los remitentes y los receptores, proteger la información contra cambios no autorizados y contra el acceso no autorizado y brindar un suministro fiable de equipo, servicios e información.

4. La seguridad de la información comprende la protección de la información relativa a la capacidad militar y otros aspectos de la seguridad nacional. La falta de

* En nombre de los Estados miembros de la Unión Europea que son Miembros de las Naciones Unidas.

protección de los recursos de información y de los sistemas de información y telecomunicaciones vitales puede constituir una amenaza a la seguridad internacional.

2. Posible contenido de conceptos internacionales pertinentes encaminados a reforzar la seguridad de los sistemas mundiales de información y telecomunicaciones

5. Como punto de partida, la Unión Europea desearía hacer hincapié en que, si bien la cooperación internacional es esencial para luchar de manera efectiva contra las cuestiones novedosas y complejas relacionadas con la seguridad de la información, corresponde a cada país el derecho y la responsabilidad de proteger su información y sus sistemas basados en la información.

6. La Unión Europea considera que hoy en día el peligro puede venir de cualquier país y que las tecnologías que permiten la vulneración de los sistemas de información y telecomunicaciones son ampliamente accesibles a todos. Todas las economías dependen de la libre circulación de la información y del uso pacífico de las tecnologías de la información. Toda medida preventiva encaminada a contener posibles ataques criminales o terroristas, incluso el peligro a la seguridad internacional, debería tener en cuenta la protección de los recursos de información y los sistemas basados en la información.

7. En la actualidad se están realizando varias actividades de cooperación internacional en la esfera de la seguridad de la información, por ejemplo, por el Consejo de Europa; el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, 10 a 17 de abril de 2000 (véase A/CONF.187/15); la Comisión de Prevención del Delito y Justicia Penal, de las Naciones Unidas; el Grupo de Trabajo sobre Informática del Consejo Económico y Social; el Grupo de Tareas sobre la tecnología de la información y las comunicaciones, de las Naciones Unidas; la Organización de Cooperación y Desarrollo Económicos (OCDE); la Unión Internacional de Telecomunicaciones (UIT); el Grupo de Delitos de Alta Tecnología del Grupo de los Ocho y la Organización de los Estados Americanos (OEA).

8. En consecuencia, la Unión Europea considera que los Estados Miembros de las Naciones Unidas deberían supervisar la labor realizada en éstos y otros foros, con miras a evaluar en su debido momento el tipo de medidas sustantivas que podrían constituir una contribución útil en esa esfera. La Unión Europea no considera que, en el contexto de la Asamblea General, la Primera Comisión deba ser el principal foro para debatir la cuestión de la seguridad de la información. Como esa cuestión esencialmente abarca temas distintos del desarme y la seguridad internacional, la Unión Europea considera que hay otras comisiones que están en mejores condiciones de abordar por lo menos algunos de los aspectos de la cuestión.