Naciones Unidas A/54/213

Asamblea General

Distr. general
10 de agosto de 1999
Español
Original: árabe/español/inglés/ruso

Quincuagésimo cuarto período de sesiones
Tema 71 del programa provisional*
Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional

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

Informe del Secretario General

Índice

* A/54/150.

99-23600 (S) 150999 200999

I. Introducción

1. La Asamblea General, en los párrafos 2 y 3 de su resolución 53/70, de 4 de diciembre de 1998, titulada “Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional”, invitó a todos los Estados Miembros a que hicieran 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 relacionados con la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y los recursos de información; y c) conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información, y pidió al Secretario General que le presentara un informe en su quincuagésimo cuarto período de sesiones.

2. El 19 de marzo de 1999, el Secretario General dirigió una nota verbal a los Estados Miembros en la que les solicitaba que le transmitieran sus opiniones de conformidad con la invitación que les había formulado la Asamblea. A continuación se reproducen las respuestas recibidas de los Gobiernos.

II. Respuestas recibidas de los Gobiernos

Arabia Saudita

[Original: árabe]
[27 de mayo de 1999]

En todos los Estados que dependen cada vez más de los sistemas de información electrónica hay numerosas instituciones gubernamentales y privadas que han logrado progresos en la esfera de la tecnología de la información. Sin embargo, proporcionalmente a ese progreso, ha aumentado el número de actos encaminados a interrumpir, obstaculizar y alterar los sistemas de información que ponen en práctica entidades internacionales con fines destructivos y terroristas. Esos actos producen daños a la economía, la sociedad y la seguridad. Es fundamental establecer principios y normas internacionales para responder a los peligros contra la seguridad de la información y su uso indebido y para combatir y sancionar dichos actos internacionales. Quienes cometan esos actos deben ser juzgados y sancionados por las organizaciones internacionales competentes.

Australia

[Original: inglés]
[2 de junio de 1999]

1. Australia presidió el Grupo de Expertos de la Organización de Cooperación y Desarrollo Económicos (OCDE) que elaboró las Directrices de la OCDE para la seguridad de los sistemas de información. Preside asimismo el Grupo de Trabajo de la OCDE sobre seguridad y confidencialidad de la información, que se ocupa, entre otras cosas, de evaluar la necesidad de la seguridad de la información. Australia participa, en el marco de la Organización Internacional de Normalización (ISO), en la formulación de normas de seguridad para la tecnología de la información. A nivel interno, Australia ha establecido procesos detallados para la seguridad de la información gubernamental y Standards Australia, conjuntamente con Standards New Zealand, ha formulado una norma conjunta para la gestión de la seguridad de la información basada en una norma del Reino Unido. En la actualidad, el Gobierno y la industria de Australia trabajan conjuntamente en la adopción de medidas para proteger la infraestructura nacional de la información. Australia ha promulgado leyes para proteger los sistemas de telecomunicaciones contra la interceptación, injerencia y algunas formas de utilización ilícita.

2. El objetivo de la seguridad de la información, como se define en las Directrices de la OCDE para la seguridad de los sistemas de información y como se aplica en Australia, es “proteger los intereses de los que dependen de los sistemas de información contra los daños derivados de fallas en la disponibilidad, confidencialidad e integridad”.

3. Ante la convergencia de tecnologías, el objetivo se puede extender a aquellos sistemas de telecomunicaciones que son un tipo concreto de sistemas de información. Cualquier injerencia en los sistemas de información o su utilización ilícita afectarán a su disponibilidad, confidencialidad o integridad. En un medio en rápida evolución, se corre el riesgo de establecer definiciones de aplicación a tecnologías concretas.

4. Australia no considera que el Departamento de Asuntos de Desarme de la Secretaría de las Naciones Unidas sea el órgano adecuado para formular principios internacionales sobre la seguridad de los sistemas mundiales de información y telecomunicaciones. La infraestructura de telecomunicaciones e información repercute en aspectos del comercio, el desarrollo económico y el bienestar social, así como en la aplicación de la ley y la seguridad nacional. Ya se han formulado principios y directrices sobre estas cuestiones en otros foros, como la OCDE, la ISO y la Unión Internacional de Telecomunicaciones (UIT), sobre la base de perspectivas más amplias que las que se proponen en la resolución 53/70

de la Asamblea General. Además, organismos internacionales como el Instituto de las Naciones Unidas de Asia y el Lejano Oriente para la prevención del delito y el tratamiento del delincuente (UNAFEI) y el Centro de Prevención Internacional del Delito se están ocupando de cuestiones relacionadas con los delitos en la esfera de la informática. Australia no considera provechoso que algunas instancias de las Naciones Unidas dupliquen la labor que se está realizando en otro ámbito respecto de la seguridad o la utilización ilícita de la informática. Australia estaría de acuerdo en que se creara un centro de información sobre la labor que se realiza en otros foros.

Belarús

[Original: inglés]
[25 de mayo de 1999]

1. La República de Belarús apoya plenamente la resolución 53/70 de la Asamblea General, de 4 de diciembre de 1998, titulada "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional". La aplicación resuelta de las nuevas tecnologías de la información y los medios de telecomunicaciones brinda las más amplias oportunidades para el desarrollo acelerado de la civilización mundial. Al mismo tiempo, como señala concretamente la Asamblea en su resolución 53/70, existe "la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la seguridad de los Estados".

2. La aprobación de la resolución 53/70 de la Asamblea es oportuna y pertinente ya que señala a la atención de la comunidad internacional el posible uso de las tecnologías de la información con fines bélicos y la necesidad de evitar la aplicación de las nuevas tecnologías y medios de información en un contexto militar en el que éstos podrían compararse con armas de destrucción en masa. Además, con la aprobación de la resolución 53/70 de la Asamblea General se abre la posibilidad de examinar concretamente el problema de la seguridad internacional de la información, incluida la injerencia no autorizada o la utilización ilícita de los sistemas de información y telecomunicaciones y los recursos de información. Por último, es conveniente formular y acordar un concepto de seguridad internacional de la información y principios jurídicos internacionales con objeto de aumentar la seguridad de los sistemas mundiales de información y telecomunicaciones y prevenir el terrorismo y la delincuencia en la esfera de la información.

Brunei Darussalam

[Original: inglés]
[7 de junio de 1999]

Respecto de la resolución 53/70 de la Asamblea General, de 4 de diciembre de 1998, titulada "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional", la Misión Permanente de Brunei Darussalam tiene el honor de transmitir las siguientes opiniones del Ministerio de Defensa de Brunei Darussalam:

> "El Ministerio de Defensa, en su calidad de ministerio responsable de la defensa nacional, reconoce la importancia de la seguridad de la información en la actual era de la tecnología de la información. El Ministerio considera que cualquier tipo de información cuya utilización y transmisión puedan plantear una amenaza para la seguridad nacional es importante. Sin embargo, atendiendo a sus vínculos con la tecnología de la información y como también esta cuestión es de la competencia de otros ministerios del país, el Ministerio de Defensa cooperará con los organismos pertinentes para responder a la petición formulada en la resolución. A fin de proteger y garantizar la seguridad de las comunicaciones internacionales, debe considerarse que la responsabilidad en ese campo no escapa a la jurisdicción de la Corte Internacional de Justicia".

Cuba

[Original: español]
[28 de junio de 1999]

Evaluación general de los problemas de seguridad de la información

1. La generalización del empleo de las tecnologías de la información, prácticamente en todas las esferas de la actividad humana, lo que se ha dado en llamar "informatización de la sociedad" y a lo que muchos denominan "Era de la información" por el grado de dependencia cada vez mayor que se crea hacia los sistemas de información, plantea nuevos problemas de seguridad que tienen que ser considerados muy seriamente no sólo por cada Estado sino también por toda la comunidad internacional.

2. Por tal motivo, la Organización de las Naciones Unidas es el marco adecuado para emprender un debate que propicie las vías y formas pertinentes para enfrentar los peligros que para la seguridad internacional pudiera tener el uso con fines no pacíficos de las nuevas tecnologías de la información y de las telecomunicaciones.

3. Asimismo, se deben tomar todas las medidas necesarias para que estas tecnologías estén a la disposición del desarro-

llo de todos los Estados, particularmente de los países subdesarrollados que no poseen los recursos suficientes para desarrollarlas por sí mismos.

4. Por otro lado, el concepto de "Globalización" es ya una realidad en el campo de la información y las telecomunicaciones, lo que hace que las distancias ya no sean un obstáculo en los procesos de intercambio de información, al tiempo que se incrementan los riesgos relacionados con la seguridad de los sistemas que propician este intercambio. Es necesario destacar que la "Globalización" conlleva a un nivel de estandarización que facilita la realización de acciones injerencistas contra estos sistemas.

5. No se debe pasar por alto que estamos hablando de tecnologías que son de países desarrollados, y dentro de éstos, los Estados Unidos, la mayor Potencia hegemónica mundial, particularmente en el campo de la informática y las telecomunicaciones, posee una posición preponderante que le permite imponer patrones tecnológicos que facilitan su potencial empleo como medios de agresión.

6. En contraste con lo anterior, los países subdesarrollados no tienen otra alternativa que aceptar esas tecnologías para poder subsistir en las nuevas condiciones, sin conocer a plenitud la mayor parte de las veces los riesgos asociados a ellas, que con frecuencia dan lugar a una deficiente implementación de protocolos, servicios o mecanismos de seguridad.

7. Cuba aprecia profundamente la oportunidad que se le brinda para analizar el tema en la Asamblea General al presentarse una iniciativa que fuera adoptada por consenso bajo el formato de la resolución 53/70. Nuestro país, consciente de la importancia actual del tema, participará activamente en los análisis que, sobre el particular, se originen en el marco de la resolución.

Determinación de criterios básicos relacionados con la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información

8. El mundo en que vivimos es testigo de un incremento sin precedentes de la utilización de las tecnologías de la información y de las telecomunicaciones, que ha permitido, lamentablemente, que se les utilice también para fines hostiles derivados de políticas agresivas que aplican unos Estados hacia otros.

9. En este mismo sentido es válido destacar que el desarrollo y la popularidad de las redes de alcance global, y en particular "Internet", han sido significativos. A pesar de este crecimiento, los sistemas son aún operados sobre una base meramente colaboracional. Esto es importante para reconocer que en la naturaleza voluntaria de "Internet" radica su fuerza y su mayor fragilidad.

10. El conjunto común de las reglas para una acertada e incrementada seguridad de operación de las redes de alcance global es voluntaria debido a que las leyes de los países no son uniformes respecto al trabajo en redes de datos.

11. Sin embargo, partiendo del hecho de que la asociación a estas redes globales es opcional, es justo argumentar que cualquier regla de conducta de ellas debe formar parte del acuerdo de asociación, y que su violación, independientemente de cualquier infraestructura legal disponible, pudiera ser motivo de sanciones.

12. La seguridad de la información incluye la protección de su confidencialidad — sólo debe ser conocida por quien tiene derecho a ello —, la protección de la información contra modificaciones no autorizadas (integridad), la protección de los sistemas contra denegación de servicios (disponibilidad) y contra accesos no autorizados.

13. En este contexto, existen algunos criterios básicos que deben ser tomados en consideración:

a) Los usuarios son responsables por su propia conducta o lo que es lo mismo, que un acceso no autorizado a una computadora o el uso de una red es explícitamente una violación de las reglas de conducta, independientemente de la fragilidad de la protección de los medios informáticos;

b) Las organizaciones que emplean estas tecnologías son responsables de que sus empleados las usen adecuadamente, y para ello deben definir las políticas de seguridad que lo aseguren, así como las medidas y procedimientos que garanticen su control. De igual modo cada país debe establecer los mecanismos que correspondan para lograr que las organizaciones radicadas en su territorio cumplan estos requerimientos;

c) Los proveedores de servicios de computadoras y redes son responsables del mantenimiento de la seguridad de los sistemas que ellos operan. Son además responsables de notificar a los usuarios sobre sus políticas de seguridad y de cualquier cambio en éstas;

d) Los vendedores y suministradores de sistemas son responsables de proporcionar sistemas sólidos que incorporen adecuados controles de seguridad. Un vendedor o suministrador de sistemas debe evaluar cada uno de ellos en términos de controles de seguridad antes de su introducción en el mercado. Cada producto debe describir los aspectos de seguridad incorporados. Los vendedores y suministradores se sistemas tienen la obligación de reparar los defectos en las

partes relevantes de los sistemas que ellos venden o distribuyen libremente;

e) Los usuarios, los proveedores de servicios y los vendedores de software y hardware son responsables de la colaboración en el suministro de seguridad. Se espera que cada sitio notifique a otro si detecta una penetración en progreso en cualquiera de éstos, y que se ayuden unos a otros para responder a las violaciones de seguridad. Esta asistencia puede incluir trazas de conexiones, rastros de violaciones y asistencia legal.

14. Entre los principales objetivos de un atacante a redes de datos se encuentran:

a) Obtener, modificar o destruir información. Sin dudas es el principal objetivo de la mayoría de los atacantes;

b) Introducirse en las computadoras ajenas y usarlas como si fueran usuarios de éstas;

c) Lograr un punto de partida para otros ataques. Los sistemas pueden ser invadidos con el único propósito de lanzar nuevos ataques a partir de ellos;

d) Denegación de servicio, esto es, que la información no esté disponible en el momento preciso para alguien que la necesite y tenga derecho a usarla;

e) Obtener publicidad, algo de mucha utilidad en el caso de los servidores “Web”.

15. La utilización ilícita de los sistemas de información y de telecomunicaciones, así como de los recursos de información, sobre todo cuando forman parte de la aplicación de políticas injerencistas de unos Estados contra otros, es un atentado a la soberanía y la independencia de los Estados afectados, creando focos de tensión que pueden desembocar en una seria amenaza a la seguridad internacional.

16. El constante intento de conseguir fines políticos que satisfagan intereses nacionales por parte de los Estados conlleva a la utilización ilícita, según las normas internacionales establecidas, de, entre otros medios, estaciones de radio y televisión para desestabilizar el orden constitucional de otros Estados considerados enemigos.

17. Cuba es un ejemplo de Estado afectado por políticas mencionadas en los párrafos anteriores. Para que sólo se tenga una idea de la gravedad del asunto, nuestro país durante varias décadas se ha visto sometido a la agresión radial y televisiva de los Estados Unidos que responde a la constante política de agresión de la primera Potencia mundial en el orden militar, económico y político con el declarado intento de derrocar al Gobierno de la República de Cuba.

18. Para ello, por ejemplo, hasta abril de este año existían en el territorio de Estados Unidos un total de 17 estaciones que transmitían información subversiva contra Cuba.

19. Se transmitían diariamente entre 288:30 y 306:30 horas de señales radiales por onda media (OM), onda corta (OC) y frecuencia modulada (FM); 2084:30 horas semanales, y si le sumamos también las señales televisivas transmitidas semanalmente eso completaría una cifra de 2089:00 horas en total.

20. En la mayoría de estos casos, la información incita a la desobediencia civil y a la ejecución de actos vandálicos y terroristas.

21. Cuba siempre ha estado dispuesta a solucionar sus diferencias con Estados Unidos en un plano de igualdad y sobre la base del respeto a su soberanía e independencia nacionales y así lo ha expresado públicamente en diferentes ocasiones. Esta posición se mantiene invariable.

Conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información

22. Sin duda el desarrollo de las nuevas tecnologías que actualmente conocemos en materia de información reclama un esfuerzo paralelo de desarrollo progresivo del Derecho Internacional en esta esfera, incluida la elaboración de un marco jurídico adecuado que contribuya al aumento de la seguridad de los sistemas de información.

23. La tarea no será fácil, si tomamos en cuenta de que aún quedan cuestiones que requerirán la concertación de definiciones de amplia aceptación, para de este modo poder facilitar la ulterior codificación de nuevos principios que contribuyan al logro de los objetivos planteados en materia de seguridad.

24. La propia naturaleza de las redes globales sobrepasa los límites jurisdiccionales de cada país que, en muchos casos, imposibilita atenerse a las fronteras geográficas. Asimismo, el desarrollo desigual de los Estados, entre otros factores, dificulta considerablemente el establecimiento de regulaciones internacionales uniformes de aplicación general a todos los países que comparten estas tecnologías.

25. No obstante, no partiríamos de cero ya que existen principios generalmente aceptados e instrumentos jurídicos internacionales concertados entre los Estados, en diferentes foros multilaterales, a lo largo del avance tecnológico que ha logrado la humanidad en los últimos años, que serían de gran utilidad para consolidar y/o desarrollar nuevos postulados

internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información.

26. Por solo mencionar algunos ejemplos relevantes de esos acuerdos, Cuba considera que se deberían tomar en cuenta los siguientes:

a) La resolución 110 (II) de la Asamblea General de 3 de noviembre de 1947, que condena la propaganda destinada a provocar o alentar cualquier amenaza de la paz, quebrantamiento de la paz o acto de agresión;

b) El Convenio Internacional de Comunicaciones de Nairobi de 1982, así como aquellos instrumentos jurídicos, internacionales y pertinentes adoptados en la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura y en la Unión Internacional de Telecomunicaciones;

c) Los Principios, adoptados por la Asamblea General, que han de regir la utilización por los Estados de Satélites artificiales de la tierra para las transmisiones internacionales directas por televisión, que establece que dichas actividades deberán realizarse de conformidad con el derecho internacional y desarrollarse de manera compatible con el fomento del entendimiento mutuo y el fortalecimiento de las relaciones de amistad y cooperación entre los Estados y pueblos con miras al mantenimiento de la paz y seguridad internacionales;

d) La Convención sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y sobre su destrucción, la cual posee en su anexo disposiciones sobre la protección de la información confidencial, que pudieran servir también de útil referencia para la elaboración de los principios señalados anteriormente.

27. Por último, y como parte del papel primario que debe tener la Organización de Naciones Unidas en los análisis que se pudieran hacer en torno a estos temas, Cuba considera que la Organización debe, entre otras cosas, reconocer que cada país tiene el derecho a proteger sus sistemas de información y de telecomunicaciones con sistemas de protección seguros; recomendar a los Estados Miembros el establecimiento de leyes que sancionen el desarrollo y diseminación de virus informáticos y otros programas dañinos. Asimismo, en el marco de la Organización se pudieran buscar acuerdos multilaterales y jurídicamente vinculantes que prohíban la agresión contra los sistemas de información y de telecomunicaciones. De igual modo, se buscarían acuerdos que garanticen la utilización para fines pacíficos y al alcance de todos los Estados de las nuevas tecnologías en desarrollo.

Estados Unidos de América

[Original: inglés]
[20 de mayo de 1999]

Consideraciones generales acerca de las cuestiones relativas a la seguridad de la información y definición de conceptos básicos

1. Los Estados Unidos de América consideran que la seguridad de la información es un tema amplio y complejo que incluye numerosos factores y afecta a actividades de distinto tipo de los particulares, grupos y gobiernos. Aunque el tema general incluye aspectos que guardan relación con la paz y la seguridad internacionales (trabajo que compete a la Primera Comisión), también incluye aspectos técnicos relacionados con las comunicaciones en el plano mundial, así como cuestiones técnicas vinculadas con la cooperación económica y el comercio, los derechos de propiedad intelectual, la aplicación de la ley, la cooperación antiterrorista y otras cuestiones que son consideradas en la Segunda Comisión y en la Sexta Comisión. Las medidas y programas de los gobiernos no son en modo alguno la única forma adecuada de abordar problema, ya que la seguridad de la información también afecta a intereses importantes de particulares, asociaciones, empresas y otras organizaciones del sector privado.

Aspectos relativos a la seguridad internacional

2. Durante los conflictos armados, las naciones han empleado diversas técnicas asociadas con la seguridad de la información. La interferencia de las frecuencias radioeléctricas y las contramedidas electromagnéticas son dos ejemplos evidentes y son técnicas de larga data. En el futuro, será importante que las fuerzas militares protejan sus propios enlaces de datos y otros sistemas relacionados con las computadoras. Además, los Estados Miembros necesitan contar con la capacidad de restaurar sistemas de información esenciales en caso de que debido a desastres naturales o emergencias catastróficas se interrumpan servicios clave de comunicaciones u otras redes de datos en los sectores público y privado. La seguridad de la información también incluye la protección de la información relacionada con las capacidades militares y otros aspectos de la seguridad nacional.

Factores económicos, comerciales y técnicos

3. La seguridad de la información incluye la necesidad de proteger la investigación científica de carácter comercial, así como la tecnología de la producción y otros tipos de datos objeto de derechos de propiedad industrial (por ejemplo,

planes de comercialización y la información sobre los servicios prestados a los consumidores).

4. La seguridad de la información también está asociada a la necesidad de hacer cumplir los acuerdos internacionales sobre la propiedad intelectual (por ejemplo, los relativos a los materiales de vídeo y de audio, así como a los programas informáticos), con el fin de protegerla de la copia y venta no autorizadas. La protección de la intimidad es otro aspecto de la seguridad de la información, es decir, velar por la seguridad de la información personal y comercial que se transmite por medio de la red pública internacional o de enlaces de datos privados.

5. En el plano técnico, el reglamento de la Unión Internacional de Telecomunicaciones y las actividades de las contrapartes nacionales velan por la compatibilidad de las señales electrónicas, la utilización adecuada del espectro electromagnético y la fiabilidad de la red internacional. Esas funciones se aplican asimismo a los satélites que proporcionan numerosos servicios, como la retransmisión telefónica y de datos, los datos de localizadores y otra información utilizada en la navegación aérea y marítima y en los servicios de búsqueda y rescate. Además, las normas de diseño y seguridad proporcionan garantías fundamentales a los fabricantes y usuarios de dispositivos electrónicos, incluidas las computadoras. Dentro de un concepto amplio de la seguridad de la información es posible incluir todas esas funciones normativas y administrativas.

Cooperación para la aplicación de la ley y la lucha contra el terrorismo

6. La dependencia generalizada en las tecnologías basadas en la información ha dado lugar a un nivel de interdependencia y conexión mundiales sin precedentes, como resultado de lo cual su uso ilícito por delincuentes o terroristas podría teóricamente poner en peligro numerosos aspectos de la actividad nacional e internacional, tanto del sector público como del privado.

7. Si bien el grado de dependencia de las tecnologías de la información puede variar de un Estado a otro, la gama de actividades que dependen de esas comunicaciones, a saber, económicas, comerciales, industriales, educacionales y jurídicas, determinan que todos los Estados sean potencialmente vulnerables a las consecuencias de una explotación delictiva. Además, cabe esperar que esa dependencia aumente en la medida que esas tecnologías se conviertan cada vez más en elementos fundamentales para el funcionamiento estable de los gobiernos y para el mantenimiento de los sistemas mundiales de comercio y comunicaciones que sustentan la interacción entre los Estados.

8. Por tanto, los Estados Unidos consideran que la utilización ilícita de la tecnología de la información constituye un peligro para los intereses de todos los Estados y comparten las preocupaciones expresadas por otros que tratan de promover, de forma unilateral y multilateral, medios adecuados para asegurar la integridad de sus recursos que dependen de la tecnología de la información.

9. Asimismo los Estados Unidos consideran cualquier injerencia ilícita o intento de interrumpir o alterar cualquier aspecto de sus sistemas nacionales de información como un peligro potencial para su infraestructura nacional esencial y, por tanto, como una amenaza a sus intereses nacionales. Los Estados Unidos, que reconocen la posible gravedad de ese peligro, han iniciado a nivel nacional programas públicos y privados a largo plazo destinados a salvaguardar sus infraestructura nacional esencial. No obstante, los Estados Unidos también reconocen que, con la creciente interdependencia mundial de gran parte de esa infraestructura esencial, el éxito de sus iniciativas nacionales para salvaguardar sus sistemas basados en la información dependerá, en parte, en última instancia del nivel de seguridad que proporcionen los sistemas con que está conectado más allá de sus fronteras.

10. Por tanto, los Estados Unidos consideran que todos los Estados deben adoptar las medidas nacionales necesarias para asegurar la integridad de sus sistemas nacionales de información y que debe aplicarse todo el peso de la ley a los delincuentes o terroristas internacionales que traten de alterar esos sistemas desde dentro de sus fronteras nacionales. Corresponde a cada Estado adoptar medidas para asegurar que sus sistemas de información sean fiables y estén protegidos al máximo contra el uso ilícito, que no se interrumpa la prestación de servicios y que los sistemas de información puedan restaurarse rápidamente en caso de producirse interrupciones.

11. La legislación penal de los Estados Unidos prohíbe la injerencia en las infraestructuras nacionales de información. Los Estados Unidos instan a todos los Estados a que revisen su marco jurídico nacional y verifiquen que se contemple adecuadamente el ejercicio de la acción penal contra toda actividad relacionada con el uso de los sistemas de información con fines ilícitos o terroristas. Los Estados Unidos han considerado necesario enmendar reiteradas veces sus estatutos relacionados con las computadoras a fin de mejorarlos y responder a nuevos problemas.

Conveniencia de elaborar principios internacionales

12. Como ya se ha señalado, la seguridad de la información es un tema amplio y complejo con numerosas dimensiones que se relacionan entre sí de maneras extremadamente complicadas. Dada la evidente necesidad de analizar todos

los aspectos de la seguridad de la información y llegar a una comprensión cabal acerca de la forma en que interactúan, sería prematuro formular principios generales relativos a la seguridad de la información en todos sus aspectos. Por el contrario, la comunidad internacional debe analizar cuidadosa y sistemáticamente la cuestión antes de dar nuevos pasos. Para facilitar ese análisis, los Estados Miembros deben recabar ideas y criterios de expertos de diversos campos en sus respectivos gobiernos y sociedades.

13. Sin embargo, ya es evidente que la cooperación internacional es esencial para combatir eficazmente los nuevos y complejos problemas que plantean el terrorismo y la delincuencia en la esfera de la información. Actualmente hay varias iniciativas multilaterales en curso relativas a la cuestión de la cooperación internacional. El Consejo de Europa está examinando un proyecto de convención sobre la delincuencia en la esfera de la cibernética; el grupo de trabajo del Grupo de los Ocho encargado de estudiar el problema de la delincuencia relacionada con la tecnología avanzada está analizando medidas relativas a la asistencia jurídica mutua y otros aspectos conexos; la Organización de los Estados Americanos también ha establecido un grupo para estudiar esas cuestiones; y el Instituto de las Naciones Unidas de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente está examinando cuestiones conexas en el contexto de las Naciones Unidas.

14. Todas esas iniciativas en curso son valiosas y debe dejarse que continúen desarrollándose y den fruto. Sería muy poco prudente que la Asamblea General formulara estrategias o emprendiera actividades que pudieran interferir con la labor que ya está realizando la comunidad internacional.

Federación de Rusia

[Original: ruso]
[9 de junio de 1999]

Observaciones generales

1. Uno de los rasgos característicos de la etapa actual de los avances científicos y tecnológicos en el mundo es la revolución mundial de la información, a saber, el rápido desarrollo y la aplicación universal de las tecnologías más recientes de la información y los medios mundiales de telecomunicaciones. La revolución de la información, que repercute en todas las esferas de las actividades vitales de los Estados, está abriendo nuevas oportunidades para el desarrollo de la cooperación internacional y está creando un ámbito global de información en el que ésta constituye una parte extremadamente valiosa de la riqueza de un país y de sus recursos estratégicos.

2. Al mismo tiempo, resulta evidente que, junto con los aspectos positivos de ese proceso, también existe un peligro real de que los avances en la esfera de la información se utilicen con fines incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales y de respetar los principios de la igualdad soberana de los Estados, la solución pacífica de las controversias y conflictos, la abstención del uso de la fuerza, la no injerencia en los asuntos internos y el respeto de las libertades y los derechos humanos.

3. La utilización de las tecnologías de la información más recientes para desarrollar el potencial militar de los países altera el equilibrio mundial y regional de fuerzas y da lugar a tensiones entre los centros de poder e influencia tradicionales e incipientes.

4. Se está generando una esfera fundamentalmente nueva de enfrentamiento en el ámbito internacional y existe el peligro de que el desarrollo científico y tecnológico en el terreno de la información y las comunicaciones pueda conducir a una escalada en la carrera de armamentos. En esa situación, se ven afectadas tanto la seguridad nacional de los Estados como el sistema general de seguridad colectiva internacional en los planos regional y mundial.

5. Nos estamos refiriendo a la creación de un “arma informática”, cuya utilización, en función del nivel de la tecnología de la información de la sociedad y de la vulnerabilidad de sus recursos vitales, puede tener consecuencias devastadoras comparables a los efectos de las armas de destrucción en masa. Es evidente que un arma de esa índole puede ser utilizada por grupos de terroristas, extremistas o delincuentes, así como por delincuentes aislados.

6. Por tanto, el carácter universal, secreto o impersonal del arma informática, la posibilidad de su amplia utilización a través de las fronteras nacionales, lo económica que resulta y su eficiencia general la convierten en un medio extremadamente peligroso de ejercer influencia, y el derecho internacional contemporáneo prácticamente no tiene medios para regular el desarrollo ni el uso de un arma de esa índole.

7. En ese contexto, es evidente la necesidad de contar con una regulación jurídica internacional del desarrollo mundial de la tecnología de la información civil y militar, y formular una política internacional coordinada sobre seguridad de la información que responda a las necesidades de la seguridad internacional.

Medidas propuestas

8. La resolución 53/70 de la Asamblea General, titulada “Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional”, que la Asamblea aprobó por consenso el 4 de diciembre de 1998, puede

servir de base para las iniciativas adicionales de la comunidad internacional en esa esfera. El proyecto de resolución sobre el tema fue presentado por la Federación de Rusia.

9. La Asamblea General debe aprobar resoluciones sobre la cuestión de la seguridad de la información con miras a reducir el peligro de la utilización de la información con fines terroristas, delictivos o militares.

10. Es esencial que continúe el examen conjunto de la situación en la esfera de la seguridad de la información a fin de conocer todas las posiciones y criterios existentes y tomarlos en cuenta en los esfuerzos comunes encaminados a promover el concepto de seguridad de la información.

11. Una vez definidos los criterios y tendencias comunes, debe comenzarse a trabajar en la elaboración de principios internacionales (por ejemplo, un régimen y un código de conducta para los Estados) con miras a reforzar la seguridad internacional de la información. Inicialmente, esos principios podrían presentarse en forma de declaración multilateral; más tarde podrían incorporarse en un instrumento jurídico multilateral internacional. La labor en esa esfera debería realizarse, además, en el marco de la Conferencia de Desarme de Ginebra.

12. Por otra parte, la comunidad internacional debería considerar y aprobar los principios mencionados en conjunto, es decir, teniendo presentes los peligros de carácter militar, terrorista o delictivo y con miras a aplicar dichos principios tanto en la esfera militar como en la civil.

Principales peligros para la seguridad internacional de la información

13. Los principales peligros para la seguridad internacional de la información son los siguientes:

a) La creación y utilización de medios para modificar o dañar los recursos y sistemas de información de otro Estado;

b) La utilización deliberada de la información para ejercer influencia en las estructuras vitales de otro Estado;

c) La utilización de la información con el objeto de socavar el sistema político y social de un Estado; la manipulación psicológica de una población con el objetivo de desestabilizar la sociedad;

d) La adopción de medidas por los Estados para dominar y controlar la esfera de la información, impedir el acceso a las tecnologías más recientes de la información y crear una situación en que otros Estados sean tecnológicamente dependientes en la esfera de la información;

e) La adopción de medidas por asociaciones, organizaciones o grupos internacionales de terroristas, extremistas o delincuentes o por delincuentes aislados que pongan en peligro las estructuras vitales y los recursos de información de un Estado;

f) La formulación y adopción por los Estados de planes o doctrinas que incluyan la posibilidad de hacer la guerra en el campo de la información y puedan provocar una carrera de armamentos y generar tensiones en las relaciones entre los Estados, y conducir a guerras de información per se;

g) La utilización de los medios y tecnologías de la información en detrimento de las libertades y los derechos humanos en la esfera de la información;

h) La divulgación transfronteriza no controlada de la información, en contravención de los principios y normas del derecho internacional y de las leyes nacionales de países concretos;

i) La manipulación de las corrientes de información, la desinformación y el ocultamiento de información con el objeto de debilitar el marco espiritual y psicológico de una sociedad y socavar sus valores culturales, morales, éticos y estéticos tradicionales;

j) La expansión de las actividades de información y la monopolización de las infraestructuras nacionales de información y telecomunicaciones de otro Estado, incluidas las condiciones para su funcionamiento en el ámbito internacional de la información.

Principales tareas y objetivos para el desarrollo de un régimen de seguridad internacional de la información

14. Es necesario crear una base jurídica internacional para:

a) Determinar y clasificar los rasgos característicos de las guerras en la esfera de la información;

b) Determinar y clasificar los rasgos característicos de las armas informáticas, así como de los métodos y medios que pudieran considerarse como armas informáticas;

c) Restringir el tráfico de armas informáticas;

d) Prohibir el desarrollo, la divulgación y el empleo de tipos especialmente peligrosos de armas informáticas;

e) Prevenir el peligro de que se desencadenen guerras en la esfera de la información;

f) Prohibir la utilización de las tecnologías y los medios de información con fines hostiles y, en particular, contra categorías convenidas de servicios;

g) Reconocer que la utilización de armas informáticas contra estructuras vitales es comparable a las consecuencias del empleo de las armas de destrucción en masa;

h) Crear las condiciones para el intercambio internacional equitativo y seguro de información, sobre la base de un equilibrio de los intereses de los individuos, la sociedad y el Estado;

i) Prevenir el peligro de la utilización de las tecnologías y los medios de información con fines terroristas o con otros fines de carácter delictivo;

j) Prevenir el peligro de la utilización de las tecnologías y los medios de información para influir en la conciencia social con miras a desestabilizar una sociedad o Estado;

k) Desarrollar un procedimiento para la notificación mutua y la prevención del empleo no autorizado de la información para influir en otros Estados;

l) Crear un mecanismo para solucionar las situaciones de conflicto en la esfera de la seguridad de la información;

m) Crear un sistema internacional para certificar las tecnologías y los medios de información (incluidos programas y equipos) con miras a garantizar su seguridad;

n) Desarrollar un sistema de cooperación internacional entre los organismos encargados de hacer cumplir la ley, con miras a prevenir el delito en la esfera de la información;

o) Crear un mecanismo para vigilar el cumplimiento de las condiciones del régimen internacional de seguridad de la información;

p) Armonizar la legislación nacional a fin de garantizar la seguridad de la información.

Conceptos básicos relacionados con la seguridad internacional de la información

15. Entre los conceptos básicos relacionados con la seguridad internacional de la información cabe citar los siguientes:

a) *Esfera de la información*. Esfera de actividad que comprende la creación, transformación y utilización de la información, incluidas la conciencia individual y social, la infraestructura de información y telecomunicaciones y la información propiamente dicha;

b) *Recursos de información*. La infraestructura de información (equipo y sistemas para crear, procesar, almacenar y transmitir información), incluidos archivos y bases de datos, la información y las corrientes de información);

c) *Guerra en la esfera de la información*. Enfrentamiento entre los Estados en la esfera de la información con el objetivo de dañar los sistemas, procesos, recursos y estructuras vitales de la información y socavar los sistemas político y social de otro Estado, así como la manipulación sicológica de la población de un Estado y la desestabilización de la sociedad;

d) *Arma informática*. Medios y métodos empleados con el objetivo de dañar los recursos, procesos y sistemas de información de otro Estado; la utilización de la información en detrimento de los sistemas vitales de defensa, administrativos, políticos, sociales, económicos o de otra índole de un Estado y la manipulación de la población de un Estado con el objetivo de desestabilizar la sociedad y el Estado;

e) *Seguridad de la información*. Protección de los intereses básicos del individuo, la sociedad y el Estado en la esfera de la información, incluidas las infraestructuras de la información y las telecomunicaciones, así como la información per sé en lo que se refiere a sus características, como son la integridad, la objetividad, la accesibilidad y la confidencialidad;

f) *Peligros para la seguridad de la información*. Factores que ponen en peligro los intereses básicos del individuo, la sociedad y el Estado en la esfera de la información;

g) *Seguridad internacional de la información*. La condición de las relaciones internacionales que excluye la violación de la estabilidad internacional y la creación de peligros para la seguridad de los Estados y de la comunidad internacional en la esfera de la información;

h) *Uso ilícito de los sistemas de información y telecomunicaciones y de los recursos de información*. Uso de los recursos y sistemas de telecomunicaciones e información sin la autorización pertinente o en contravención de las reglas, leyes o normas del derecho internacional aplicables;

i) *Injerencia no autorizada en los sistemas de información y telecomunicaciones y en los recursos de información*. La injerencia en la reunión, el procesamiento, la acumulación, el almacenamiento, la búsqueda, la divulgación o el uso de la información con miras a interrumpir el funcionamiento normal de los sistemas de información, o la violación de la integridad, la confidencialidad o la accesibilidad de los recursos de información;

j) *Estructuras vitales*. Servicios, sistemas e instituciones de un Estado que cuentan con recursos de información cuya modificación deliberada puede tener consecuencias que afecten directamente la seguridad nacional (transporte, suministro de energía, crédito y finanzas, comunicaciones, órganos administrativos del Estado, sistema de defensa, organismos encargados de hacer cumplir la ley, recursos

estratégicos de información, instituciones científicas y desarrollo científico y tecnológico, instalaciones que entrañan alto riesgo tecnológico y ambiental, y órganos para combatir las consecuencias de los desastres naturales u otras situaciones de emergencia);

k) *Terrorismo internacional en la esfera de la información*. La utilización de los sistemas y recursos de telecomunicaciones o de información, o la modificación de esos sistemas o recursos, en el ámbito internacional de la información con fines terroristas;

l) *Delito internacional en la esfera de la información*. La utilización de los sistemas y recursos de telecomunicaciones o de información, o la modificación de esos sistemas o recursos, en el ámbito internacional de la información con fines ilícitos.

Omán

[Original: árabe]
[22 de junio de 1999]

1. No es competencia de la Administración de Telecomunicaciones de la Sultanía proporcionar información a los suscriptores, sino sólo proveer las redes y tecnologías que faciliten el acceso a los sistemas de información.

2. En su calidad de proveedor de redes y tecnologías, la Administración tiene una visión general de los problemas relativos a la seguridad de la información. Cabe decir que las tecnologías proporcionadas por la Administración son susceptibles de ser utilizadas por partes no autorizadas para tener acceso a la información, lo cual puede tener consecuencias negativas.

3. Como proveedor de servicios de telecomunicaciones, la Administración normalmente no se ocupa de la seguridad de la información de los suscriptores, quienes deben establecer por sí mismos las salvaguardias necesarias para proteger su información. Sin embargo, la Administración puede limitar el acceso a la información puesta al alcance del público mediante algunos servicios, como la Internet.

4. Respecto de los criterios básicos relacionados con la seguridad de la información, en las disposiciones vigentes en la Sultanía, y en las relativas a los derechos de autor en particular, se considera que la información tiene valor material y moral y, por consiguiente, merece protección jurídica. Sobre la base de este principio es posible definir los criterios básicos relacionados con la seguridad de la información. Los más importantes son los siguientes:

a) Interceptación ilícita de información y datos;

b) Entrada ilícita en los sistemas informáticos;

c) Espionaje electrónico;

d) Violación de la privacidad de otros o de su derecho a la confidencialidad;

e) Utilización no autorizada de todo tipo de datos o documentos almacenados electrónicamente;

f) Destrucción, alteración y desvío de datos;

g) Reunión y desvío de información;

h) Revelación no autorizada de información y datos;

i) Intrusión en los programas informáticos mediante modificación o falsificación de datos;

j) Copia ilícita de programas en violación de los derechos de propiedad intelectual;

k) Robo y uso de direcciones de redes;

l) Alteración, adición o supresión de información en un mensaje original durante su transmisión antes de que llegue a su destinatario;

m) Introducción de virus y alteración fraudulenta del contenido de las redes;

n) Destrucción real (física) de equipo y edificios.

5. Entre las posibles soluciones para aumentar la seguridad de los sistemas de información figuran las siguientes:

a) Educación del personal en materia de seguridad, en particular en relación con los peligros existentes y su prevención;

b) Control del acceso; es decir, emisión de permisos de diversos tipos para las personas con acceso autorizado a determinadas categorías de información;

c) Uso de identificadores numéricos (firmas y certificaciones numéricas) para la comunicación entre usuarios autorizados;

d) Cifrado de equipo y programas de computadoras;

e) Uso de barreras de seguridad para evitar la entrada de información alterada;

f) Uso de programas antivirus.

6. La Sultanía tiene la esperanza de que se establezcan principios internacionales para aumentar la seguridad de los sistemas mundiales de información, en particular habida cuenta de que el país ha introducido un servicio de Internet y, por consiguiente, ha quedado expuesto a los peligros relacionados con la seguridad de la información.

Qatar

[Original: inglés]
[10 de junio de 1999]

Las autoridades competentes del Estado de Qatar han comunicado la información siguiente sobre sus opiniones y apreciaciones respecto de los párrafos 2 y 3 de la resolución 53/70 de la Asamblea General, de 4 de diciembre de 1998:

a) *Evaluación general de los problemas de la seguridad de la información.* El intercambio de conocimientos especializados y la comprensión del riesgo de injerencia no autorizada, así como sus efectos en aspectos financieros y de seguridad, permitirían hacer una evaluación general de los problemas de la seguridad de la información;

b) *Determinación de criterios básicos relacionados con la seguridad de la información*. Los criterios básicos para promover la seguridad son las medidas que han de adoptarse para garantizar los medios para la comunicación de la información, así como los problemas imprevistos, como se ilustra en los cuadros 1 y 2 *infra*. En ellos se enumeran las medidas necesarias en cada etapa para garantizar la seguridad de la información, además de las nuevas dificultades que surgen en ese sentido;

c) *Principios que aumenten la seguridad de las comunicaciones*. La seguridad de la información podría promoverse perfeccionando los medios de transmisión de la información. A continuación se exponen los aspectos más importantes para promover la seguridad de las comunicaciones, habida cuenta de su elevado costo financiero:

i) La utilización de protocolos de comunicación no ordinarios que podrían estar concebidos concretamente para el intercambio de determinada información;

ii) El uso de un sistema de codificación destinado a un propósito concreto y que no utilice programas que se fabrican en cantidades comerciales; y

iii) La introducción de cambios en distintos momentos y con códigos diferentes.

Cuadro 1
Soluciones para la seguridad de las redes

Medidas de seguridad

Peligro	*Solución*	*Función*
Interceptación, lectura o modificación ilícitas de datos	Cifrado (DES, algoritmo RSA)	Codificación de datos para evitar su alteración no autorizada
Acceso de un usuario autorizado a datos que no está autorizado a consultar	Programa de computadora para el control del acceso	Asignación y control de los privilegios de los usuarios
Falsificación de la identidad de un usuario para cometer fraude	Autenticación	Técnica que incluye programas de computadora para el cifrado y tarjetas para verificar la identidad del remitente y del destinatario
Acceso de una red a otra por un usuario no autorizado	Barrera de seguridad	Filtrado y prevención de la entrada de cierta información en la red o servidor
Aprovechamiento por un pirata informático de lagunas en el sistema operativo del servidor para lograr acceder a los datos y alterarlos ilícitamente	Herramientas de sistemas operativos	Eliminación de las lagunas conocidas en el sistema operativo

DES: Data Encryption Standard (norma de cifrado de datos).

RSA: Rivest, Shamir, Adleman (apellidos de los creadores del sistema de cifrado).

Cuadro 2
Problemas de seguridad

Cambios	*Problemas*
Red actual:	**La seguridad se ve amenazada por:**
Tiene muchas más computadoras portátiles	Las computadoras portátiles son fáciles de robar
Tiene más conexiones inalámbricas	Las conexiones inalámbricas son más fáciles de interceptar
Es más dispersa geográficamente	Las estaciones remotas son más difíciles de proteger
Conecta una gama más amplia de plataformas	El usuario olvida la contraseña de acceso o escribe contraseñas múltiples
Se conecta cada vez más con redes públicas, como la Internet	Los piratas informáticos están al acecho en las redes públicas
Utiliza con más frecuencia sistemas informáticos UNIX	El sistema operativo UNIX tiene determinados puntos débiles

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[30 de mayo de 1999]

Generalidades

1. La conexión mundial de los sistemas basados en la información ha llegado actualmente al punto en que numerosos Estados, si no todos, encaran el peligro de posibles ataques electrónicos por parte de delincuentes y terroristas contra elementos importantes de su infraestructura esencial. Si bien el peligro de ataques electrónicos es probablemente pequeño de momento, éste aumentará con el tiempo en la medida en que los sectores público y privado dependan cada vez más de los sistemas computadorizados que están cada vez más conectados entre sí. Además, por cuanto los sistemas están conectados en redes internacionales, el peligro es de carácter transfronterizo. Por tanto, los intentos delictivos y terroristas de penetrar nuestros sistemas con fines malintencionados constituyen un peligro para todos los miembros de las Naciones Unidas. Por consiguiente, el Reino Unido de Gran Bretaña e Irlanda del Norte acoge con beneplácito los pasos encaminados a estudiar la posibilidad de adoptar medidas unilaterales y multilaterales que nos permitan proteger contra esos ataques la integridad de la infraestructura esencial basada en la información.

Medidas nacionales

2. Con ese fin, en enero de 1999, el Gobierno de Su Majestad anunció medidas para reducir al mínimo el peligro de ataques electrónicos contra la infraestructura nacional esencial del Reino Unido. Entre esas medidas cabe citar:

a) Velar por que, dentro del Gobierno, se identifiquen todos los sistemas esenciales y se apliquen y comprueben efectivamente las medidas de protección de esos sistemas;

b) Colaborar con el sector privado en la elaboración de medidas que sean proporcionales a nivel de riesgo y asegurar que se apliquen normas adecuadas de protección para los sistemas clave incluidos en la infraestructura nacional esencial;

c) Mejorar de forma más general la comprensión y las normas de seguridad de la información en el sector privado mediante la aplicación de las iniciativas existentes para promover mejores prácticas.

Medidas internacionales

3. Al mismo tiempo, debido a la conexión transfronteriza, los ataques contra los sistemas de otros Estados pueden tener repercusiones en la infraestructura nacional esencial del Reino Unido, y los terroristas y delincuentes que operen desde un tercer país podrían tratar de atacar los sistemas del Reino Unido. Por tanto, el Reino Unido reconoce que la cooperación internacional es fundamental para combatir el peligro de ataques malintencionados y está tratando de promover el diálogo sobre estos temas con sus asociados internacionales. Ello incluye el trabajo en el grupo establecido por el Grupo de los Ocho para analizar la prestación de asistencia jurídica mutua para combatir los delitos relacionados con la tecnología avanzada, y en el Consejo de Europa para la elaboración de una convención sobre la delincuencia en la esfera de la cibernética.

4. El Reino Unido considera que las Naciones Unidas deberían supervisar el trabajo en esos y otros foros con miras a evaluar en el momento oportuno el tipo de medidas sustantivas que podría adaptar como contribución valiosa en ese campo. Esas medidas podrían incluir la elaboración de principios internacionales para fomentar la seguridad de los sistemas mundiales y ayudar a combatir el terrorismo y la delincuencia en la esfera de la información.