Naciones Unidas A/61/161

Asamblea General

Distr. general
18 de julio de 2006
Español
Original: árabe/chino/español/
inglés

Sexagésimo primer período de sesiones
Tema 82 del programa provisional*
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

Página

I. Introducción 2
II. Respuestas recibidas de los Gobiernos 2
Bolivia 2
China 4
Emiratos Árabes Unidos 5
Jordania 7
Líbano 8
Qatar 9

* A/61/150.

06-43428 (S) 090806 100806

I. Introducción

1. En el párrafo 3 de su resolución 60/45 sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, la Asamblea General invitó a todos los Estados Miembros a que siguieran comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) la evaluación general de los problemas de la seguridad de la información; b) las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito; c) el contenido de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones; y d) las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad informática a escala mundial.

2. El 23 de febrero de 2006 se envió a los Estados Miembros una nota verbal en la que se les invitaba a comunicar al Secretario General sus opiniones y observaciones al respecto. Las respuestas recibidas figuran en la sección II *infra*. Las demás respuestas que se reciban se publicarán como adiciones del presente informe.

II. Respuestas recibidas de los Gobiernos

Bolivia

[Original: español]
[13 de junio de 2006]

La resolución 60/45, aprobada por la Asamblea General de las Naciones Unidas promueve el análisis a nivel multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información, y de posibles medidas para limitar las amenazas que surjan en ese ámbito de manera compatible con la necesidad de preservar la libre circulación de información.

Evaluación general de los problemas de la seguridad de la información

Los considerables progresos alcanzados en el desarrollo y la aplicación de las tecnologías de la información y los medios de telecomunicaciones, como Internet, fax y telefonía celular satelital, brindan información en forma indiscriminada e irrestricta en el ámbito mundial, aspecto que posibilita acceder a la información clasificada.

Sin embargo, ese proceso encierra amplias posibilidades constructivas para el desarrollo de la civilización, ampliando las oportunidades de cooperación para el bien común de los Estados y el logro de nuevas metas que beneficien a la humanidad.

Desde el punto de vista de la defensa, la seguridad de la información es manejada a un bajo nivel (dependiente de la empresa que ofrece el servicio). No existen políticas de seguridad internas en este aspecto.

Medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito

De acuerdo a las amenazas reales y potenciales en el ámbito de la seguridad de la información y las telecomunicaciones, dentro de las posibles medidas de cooperación, se dispone del procedimiento mediante el cual la información obtenida oportunamente es puesta en conocimiento del Ministerio de Informaciones y regulada a través de la Superintendencia de Telecomunicaciones.

Desde el punto de vista de la defensa, las medidas de seguridad que se adoptan son insuficientes en relación a los adelantos tecnológicos de la actualidad.

Actualmente se desarrollan proyectos de telecomunicaciones en los cuales se toman en cuenta las máximas medidas de seguridad de la información, mediante estructuras codificadas de transmisión. Los mismos tienen el objetivo de reducir y/o eliminar estas deficiencias.

El contenido de los conceptos mencionados en el párrafo 2 de la resolución 60/45

Se considera que el propósito de las medidas del párrafo 2 podría promoverse examinando los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

Medidas que la comunidad internacional podría adoptar para fortalecer la seguridad informática a escala mundial

- Evaluar los problemas de seguridad de la información y las telecomunicaciones a nivel internacional.
- Determinar criterios básicos relativos a la seguridad de la información y las telecomunicaciones, al acceso no autorizado o la utilización ilícita de dichos sistemas a través de Internet.
- Elaborar principios internacionales que permitan incrementar la seguridad de los sistemas de información y telecomunicaciones a nivel mundial, coadyuvando a la lucha contra el terrorismo y el tráfico de información clasificada.
- Expresar la preocupación ante la posibilidad de que estos medios y tecnologías sean utilizados con fines contrarios a garantizar la estabilidad y la seguridad de los Estados.
- En el campo militar y de defensa, implementar sistemas de telecomunicaciones con sistemas de seguridad acordes al avance de la tecnología mundial.

Recomendaciones

La seguridad de la información se debe considerar como una política de Estado materializada en la ley de telecomunicaciones, normada y controlada por la Superintendencia de Telecomunicaciones.

Para la seguridad de la información a nivel nacional, se debería implementar proyectos de telecomunicaciones de última tecnología para poder contar con las máximas medidas de seguridad que ofrecen las mismas dentro de sus programas operativos.

China

[Original: chino]
[24 de mayo de 2006]

Hoy día, el rápido avance de la tecnología de la información constituye un importante factor en la promoción del desarrollo económico y social de los países y en el mejoramiento de la calidad de vida de las personas. Al mismo tiempo, su desarrollo y amplia aplicación plantean nuevos desafíos para la seguridad nacional e internacional. La seguridad de la información se ha convertido en un importante factor que influye no sólo en la seguridad general de los países sino también en la seguridad y estabilidad mundiales. La comunidad internacional comparte la responsabilidad de tratar de manera adecuada esta cuestión, lo que redundará en beneficio de todos los países.

China cree firmemente que la seguridad de la información no sólo se refiere a los riesgos asociados a la vulnerabilidad de la infraestructura de la información, sino que está relacionada también con las consecuencias políticas, económicas, militares, sociales y culturales derivadas del uso indebido de esa tecnología. En el examen de la seguridad de la información se debe prestar igual atención a ambos aspectos.

China considera que el uso de la tecnología de la información debe respetar la Carta de las Naciones Unidas y las normas básicas que rigen las relaciones internacionales. Es necesario garantizar la libre circulación de la información sobre la base de la protección de la soberanía y la seguridad nacionales, el cumplimiento de la legislación nacional y el respeto de las diferencias históricas, culturales y políticas de cada país. Todo Estado tiene el derecho de regular su propio ciberespacio conforme a su legislación interna. Debido al grado desigual de desarrollo de los países en el ámbito de las telecomunicaciones, la comunidad internacional debe fortalecer la cooperación en el ámbito de la investigación y el empleo de la tecnología de la información, a fin de garantizar debidamente la libertad de los países para obtenerla.

Las Naciones Unidas son el foro adecuado para tratar y examinar la cuestión de la seguridad de la información. Si bien el grupo de expertos gubernamentales en materia de seguridad de la información de 2005 no logró obtener resultados sustantivos, los expertos de los distintos países intercambiaron ampliamente opiniones sobre los diversos aspectos de esa cuestión y presentaron valiosas propuestas, lo que sentó una sólida base para que la comunidad internacional siguiera tratando y examinando el tema. China apoya la creación por las Naciones Unidas de un nuevo grupo de expertos gubernamentales en 2009 a fin de examinar de manera amplia y en profundidad las amenazas y los desafíos en materia de seguridad de la información y estudiar medidas para solucionarlos. China apoyará, como siempre ha hecho, las iniciativas internacionales para tratar la cuestión de la seguridad de la información, y participará en ellas.

Emiratos Árabes Unidos

[Original: inglés]
[17 de junio de 2006]

Los Emiratos Árabes Unidos son conscientes del peligro creciente que plantea la delincuencia cibernética y reconocen que los delitos cometidos en el ciberespacio no se ven limitados por las fronteras estatales convencionales. Los sistemas modernos de información y telecomunicaciones permiten llevar a cabo actividades ilegales desde cualquier lugar y contra cualquier persona independientemente de donde se encuentre.

Para combatir con éxito la delincuencia cibernética deben adoptarse medidas eficaces en los planos nacional e internacional.

Los Emiratos Árabes Unidos han adoptado importantes medidas para fortalecer la seguridad de la información a nivel nacional, entre ellas las siguientes:

- **La ley de los Emiratos Árabes Unidos sobre la delincuencia cibernética**

La ley sobre la delincuencia cibernética se promulgó y publicó a principios de 2006 y se aplica a los delitos siguientes:

– Delitos de acceso (acceso no autorizado, propagación de virus, piratería informática, robo de identidad)

– Delitos relacionados con los datos (interceptación, modificación, robo, privacidad)

– Delitos relacionados con las redes (interferencia, modificación, destrucción)

– Otros delitos conexos (actos que facilitan la comisión de delitos, tráfico de drogas, trata de personas, blanqueo de dinero, actividades terroristas).

La ley también contiene disposiciones sobre censura y material censurable. La violación de la ley sobre la delincuencia cibernética traerá aparejada la imposición de penas de prisión o sanciones económicas o ambas cosas.

- **Iniciativa nacional del equipo de respuesta a emergencias cibernéticas**

La autoridad reguladora de las telecomunicaciones de los Emiratos Árabes Unidos está tratando de establecer un equipo nacional de respuesta a emergencias cibernéticas para reforzar la seguridad, responder a los ataques cibernéticos, emitir alertas tempranas y proporcionar información sobre amenazas cibernéticas, coordinar todas las actividades de respuesta a incidentes y fomentar la toma de conciencia a través de la capacitación y la educación en el país.

- **Código de conducta de los proveedores de servicios de Internet**

Los Emiratos Árabes Unidos están a punto de elaborar un código de conducta obligatorio para los proveedores de servicios de Internet que los llevará a ser eficientes a adoptar medidas más enérgicas para reducir la cantidad de mensajes masivos que puedan contener virus. Estos proveedores deberán explorar diligentemente el tráfico en la red para detectar servidores de correo abiertos, redes de robots o redes de computadoras usadas para fines indebidos como el envío de basura informática. También se exigirá a los proveedores de servicios de Internet

que incluyan en sus contratos cláusulas que los autoricen a desconectar el servicio a cualquier usuario que, voluntaria o involuntariamente, reenvíe basura informática. El incumplimiento de cualesquiera de las disposiciones del código traerá aparejada la imposición de penas o sanciones.

El propósito de este código de conducta es exigir a los proveedores de servicios de Internet que se atengan a normas elevadas de conducta y prácticas empresariales intachables dentro de su sector.

- **Acuerdos bilaterales**

Las empresas que prestan servicios de Internet en los Emiratos Árabes Unidos han participado activamente en acuerdos bilaterales entre países vecinos para combatir la difusión de basura informática y han conseguido reducir la cantidad de información de este tipo que se retransmite al exterior del país. Los Emiratos Árabes Unidos fomentan y alientan la cooperación internacional en la lucha contra la delincuencia cibernética y están a favor de examinar posibles memorandos de entendimiento sobre el intercambio de información y el apoyo transfronterizo en materia de cumplimiento forzoso.

- **Campañas de concienciación y educación**

La autoridad estatal reguladora de las telecomunicaciones y la industria del sector están trabajando en estrecha cooperación para fomentar la concienciación y educar a la población acerca de los beneficios que ofrece la tecnología y de los peligros asociados a la delincuencia cibernética.

Por ejemplo, la autoridad reguladora de las telecomunicaciones publicó recientemente en *Wireless Security Guidelines* (directrices sobre la seguridad de las redes inalámbricas) y la *Web Hosting policy* (política de hospedaje de sitios web). En la primera publicación se explica en detalle cómo configurar una red inalámbrica y los pasos que deben seguirse para archivarla con éxito y con las medidas de seguridad necesarias. En la segunda se describen los usos permitidos del servicio y, en particular, las políticas en materia de uso, basura informática, delitos contra la propiedad intelectual y contenidos ilegales.

- **Importancia de las medidas técnicas en el contexto de la seguridad internacional**

Existen una serie de medidas técnicas que contribuyen a garantizar la seguridad en el ciberespacio, entre ellas:

– La puesta en funcionamiento de infraestructuras de clave pública (ICP) y la creación de protocolos seguros;

– El diseño de programas informáticos de calidad, cortafuegos, programas antivirus, sistemas de gestión de los derechos electrónicos, encriptación, etc.;

– El empleo de tarjetas inteligentes, sistemas de identificación biométrica, firmas electrónicas, tecnologías adaptadas a las funciones de cada usuario, etc.

No obstante, a medida que aumenta la complejidad del ciberespacio y de sus componentes, van surgiendo amenazas nuevas e impredecibles. De ahí la necesidad de redoblar esfuerzos por desarrollar tecnologías de seguridad y de tener siempre en cuenta las cuestiones de seguridad al iniciar los procesos de diseño de cualquier tecnología que se cree en el futuro.

- **Medidas que podrían adoptarse para reforzar la seguridad informática a escala mundial**

  – La colaboración internacional es indispensable porque la delincuencia cibernética no tiene fronteras y no puede controlarse por los métodos convencionales;

  – El establecimiento de un marco jurídico común que facilite el intercambio de información y la colaboración entre los países. Además, se debe apuntar a una definición universal de la delincuencia cibernética, teniendo en cuenta que las definiciones específicas variarán de un país a otro;

  – Las autoridades encargadas de hacer cumplir la ley deben estar familiarizadas con los delitos cometidos en el ciberespacio y ser capaces de buscar y confiscar los datos almacenados en las computadoras para evitar que se destruyan las pruebas del delito.

Jordania

[Original: árabe]
[5 de junio de 2006]

1. La seguridad de los datos se relaciona con el concepto de seguridad nacional y, a su vez, el sistema de seguridad de la información se vincula directamente con la seguridad de las comunicaciones, dado que por medio de ellas se llevan a cabo las transferencias e intercambios de datos a través de las redes fijas o inalámbricas. Con el fin de proteger y reforzar la seguridad de los datos y las comunicaciones se requiere lo siguiente:

a) Aprobar instrumentos jurídicos, leyes y reglamentos que regulen la protección de la confidencialidad, la seguridad y la disponibilidad de los datos y combatan las acciones destinadas a atacarlos y a aprovechar los sistemas de información para la comisión de delitos;

b) Establecer un plan nacional en el que se reconozca la importancia de la seguridad de la información, las comunicaciones y las redes, con la participación de todas las partes interesadas del sector de la información y las redes. El plan se sustentaría en los principios siguientes:

i) Secreto y confidencialidad: garantizar que los datos no se harán públicos y que las personas sin la debida autorización no tendrán acceso a ellos;

ii) Integridad y seguridad del contenido: el contenido de los datos informáticos deberá ser auténtico y no se modificará ni alterará; en especial, no se destruirá el contenido ni se modificará o alterará en ninguna de las fases de procesamiento o de intercambio, ya sea durante el procesamiento interno de los datos o a causa de una intrusión ilícita;

iii) Disponibilidad permanente de la información o del servicio: garantizar el funcionamiento continuo de los sistemas de información, la capacidad constante para interactuar con la información y la prestación de servicios a los centros informáticos; garantizar que el usuario de la información no deberá enfrentarse a una prohibición de uso o de acceso a la información;

iv) Obligación de no rechazar una acción vinculada a un dato determinado por parte de quien la realizó (principio de “no rechazo”): la persona que lleva a cabo una acción relacionada con determinados datos o con los lugares en los que se almacenan esos datos no podrá negar la autoría de tal acción; de esta forma es posible establecer que una acción determinada fue realizada por cierta persona en un momento en particular.

c) Establecer una estrategia para la seguridad de la información, compuesta por un compendio de las normas que aplican las personas que trabajan en el sector de la tecnología y los datos a nivel institucional y que guardan relación con el acceso a los datos, la gestión y la administración de sus sistemas informáticos. Los objetivos de esta estrategia son:

i) Que los usuarios y administradores conozcan los compromisos y obligaciones que deben cumplir para proteger los sistemas de datos y las redes informáticas, así como para salvaguardar la información en todas sus formas durante las etapas de introducción, tratamiento, almacenamiento, transporte y recuperación de datos.

Líbano

[Original: árabe]
[21 de junio de 2006]

En respuesta a su amable nota relativa a la evolución de las tecnologías de la información y las comunicaciones fijas e inalámbricas en materia de seguridad internacional, el Ministerio de Defensa Nacional quisiera señalar lo siguiente:

A efectos de evaluar los aspectos relativos a la seguridad de la información, vale la pena señalar que las redes informáticas del Ejército son redes privadas a las que se aplican medidas pasivas de seguridad, dada la escasa disponibilidad de tecnologías avanzadas, que se protegen debido al costo creciente que conlleva su obtención. Las redes fijas e inalámbricas, por otra parte, constituyen una infraestructura de telecomunicaciones civiles que se extiende por todo el Líbano y en las que son de aplicación las leyes generales; por lo tanto, no se les aplican medidas de seguridad.

Entre las medidas que se adoptan en el ámbito nacional para reforzar la seguridad de la información, existe una diferencia palpable entre los procesos jurídicos relativos a la tecnología informática y aquellos referentes a la tecnología de las comunicaciones, puesto que en esta última las transgresiones son constantes. En el Líbano está vigente la ley 140, de fecha 27 de octubre de 1999, relativa a la protección del derecho a la confidencialidad de las comunicaciones y a las condiciones en las que se puede revocar este principio mediante orden judicial o administrativa, conforme a los requisitos especificados en los artículos 2 al 13 de esta ley. Conviene señalar aquí que la legislación presenta deficiencias en lo relativo a la coordinación entre los órganos de seguridad nacional y las empresas privadas (proveedores de acceso a Internet, compañías de telefonía móvil), coordinación que sería deseable para aunar esfuerzos en la persecución, la detección y la detención de las potenciales amenazas en este ámbito. Por lo tanto, se reafirma la necesidad de cooperación internacional y experiencia técnica en este aspecto con el fin de reducir la brecha entre la ley y la tecnología en el Líbano.

Qatar

[Original: árabe]
[12 de junio de 2006]

En lo que respecta a la evolución del sector de las tecnologías de la información y las comunicaciones fijas e inalámbricas en el ámbito de la seguridad internacional, el Gobierno del Estado de Qatar trabaja con empeño para controlar por completo la seguridad de la información y las comunicaciones con el fin de evitar los riesgos existentes y potenciales en esta esfera de las tecnologías de la información. Para conseguirlo, el Estado ha aprobado las leyes pertinentes.

En fecha reciente el Estado creó el Consejo Superior de las Comunicaciones y la Tecnología de la Información, a cuya Dirección Jurídica se ha asignado la tarea de ultimar el proyecto de ley electrónica y presentarlo ante las instancias pertinentes para su aprobación y entrada en vigor el año próximo.

El proyecto de ley tiene como objetivo evitar el uso de los recursos o las tecnologías de la información para fines delictivos o terroristas. Las autoridades competentes tendrán la obligación de notificar las actividades realizadas con propósitos delictivos y terroristas con el fin de que los Estados Miembros tengan un conocimiento cabal de los mismos. De este modo podrán cumplir sus compromisos plenamente y tratar de elaborar definiciones unificadas de los conceptos sobre los que no hay consenso internacional, definiciones que se debatirían en los foros internacionales.