



Asamblea General

Distr. general
2 de julio de 2007
Español
Original: árabe/chino/español/
francés/inglés

Sexagésimo segundo período de sesiones

Tema 95 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
Burkina Faso	2
Brunei Darussalam	4
Chile	8
China	8
Cuba	9
Líbano	11
México	15

* A/62/50.



I. Introducción

1. En el párrafo 3 de su resolución 61/54, relativa a 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 seguir 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 que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación 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; d) las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad informática a escala mundial.

2. El 23 de febrero de 2007, se envió a los Estados Miembros una nota verbal en la que se les invitó a informar al Secretario General de sus opiniones y observaciones sobre este tema. Las respuestas recibidas figuran en la sección II de este documento. Las que se reciban de ahora en adelante se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los Gobiernos

Burkina Faso

[Original: francés]
[20 de junio de 2007]

1. Burkina Faso afirmó desde muy temprano su voluntad política de desarrollar las nuevas tecnologías de la información y la comunicación, a las que considera un instrumento estratégico para el fortalecimiento de la buena gobernanza y el desarrollo económico y social.

2. Así, desde 1996 ha emprendido una reflexión general sobre el desarrollo de las nuevas tecnologías de la información y la comunicación. Su objetivo era poner a dichas tecnologías al servicio de la modernización de los servicios públicos y mejorar la eficacia de la acción de la administración.

3. En 1999, adoptó un plan de infraestructura nacional de información y comunicación para el período 2001-2005 con miras a propiciar la convergencia de las políticas nacionales en la esfera de las telecomunicaciones, la informática y los medios de comunicación.

4. En 2004, el Gobierno de Burkina Faso adoptó la estrategia de operacionalización del plan de desarrollo de la infraestructura nacional de información y comunicación. Mediante ese plan, el gobierno se compromete a lograr que las tecnologías de la información y la comunicación se difundan en toda la sociedad, que todas las capas sociales tengan acceso a ellas y puedan hacerlas suyas y que su potencial se movilice en beneficio de las estrategias nacionales de desarrollo.

5. No obstante, habida cuenta de los riesgos derivados del uso de los sistemas de información, el Gobierno está elaborando un marco jurídico encaminado a la protección de la información, el establecimiento de seguridad para los sistemas de información, la protección de los derechos fundamentales de las personas y el fomento de la confianza de las empresas y la administración.

6. En el curso de ese proceso, se aprobó la ley No. 010-2004/AN, de 20 de abril de 2004, de protección de los datos personales. Dicha ley protege los derechos y libertades fundamentales de las personas, su intimidad en el marco de los tratamientos informáticos y de otro tipo de las informaciones que contengan datos de carácter personal. En virtud de dicha ley, se estableció por decreto 2007-283/PRES/PM/MPDH, de 18 de mayo de 2007, una comisión sobre informática y libertades. Dicha comisión es una autoridad administrativa independiente encargada de velar por que el tratamiento automatizado público y privado de información nominativa se realice de acuerdo con la ley. Dispone de competencias reglamentarias y sancionadoras, interviene con anterioridad y con posterioridad al tratamiento de los datos mediante la emisión de dictámenes y declaraciones previas y mediante el control y la imposición de sanciones.

7. Por último, se han establecido órganos de regulación con miras a contemplar a las necesidades de seguridad de la sociedad de la información. Así, se ha establecido el Consejo Superior de Información, la Dirección general que se encarga de la coordinación de los programas de desarrollo de las tecnologías de la información y la comunicación, dependiente del Ministerio de Correos y Tecnologías de la Información y las Telecomunicaciones.

8. No obstante, ante la sociedad de la información, que no admite fronteras, Burkina Faso considera que la cooperación internacional es fundamental en la problemática del establecimiento de la seguridad de los sistemas de información. Más allá de las diferencias cuantitativas, en materia de seguridad los países del Sur se encuentran tan expuestos como los del Norte. Por consiguiente, la colaboración entre los países resulta fundamental si se desea garantizar la seguridad tanto de los Estados, las instituciones, las empresas y las personas como de las redes y los sistemas de información. La única manera de luchar eficazmente contra el delito cibernético consiste en el fortalecimiento de la cooperación internacional.

9. Burkina Faso se felicita por el interés de las Naciones Unidas en la cuestión de la seguridad de la información, y considera que ha llegado el momento de trabajar en pro de la elaboración de un instrumento internacional sobre la seguridad informática, por un lado, y de la protección de los datos de carácter personal, por otro. En cualquier caso, los progresos de la informática, la telemática y las cuestiones relativas a la seguridad internacional deben ser abordadas desde el punto de vista de los derechos humanos para que no se llegue a una sociedad mundial de vigilancia dominada por el reflejo deshumanizante de procurar la seguridad a cualquier precio.

Brunei Darussalam

[Original: inglés]
[25 de junio de 2007]

Brunei Darussalam presentó el siguiente informe de la Real Fuerza de Policía de Brunei.

I. Introducción

(Evaluación general de los problemas de la seguridad de la información.)

1. La tecnología de la información, que abarca todos los avances logrados en la esfera de la información y las telecomunicaciones, ha llegado a desempeñar un papel fundamental en todos los sectores de la sociedad. Las tecnologías de la información están transformando la manera en que creamos, reunimos, procesamos, gestionamos y compartimos la información. Las transacciones electrónicas y el almacenamiento electrónico de datos ocupan un lugar dominante y central en todas las esferas, desde el comercio hasta la atención de la salud. La fuerza que mueve esos cambios es el establecimiento de redes informáticas. El crecimiento exponencial cada año tanto de Internet como del número de usuarios refleja esa transición hacia una sociedad conectada por redes informáticas.

2. Por consiguiente, la seguridad de la información ha pasado a ser un elemento fundamental de la tecnología de la información, en particular en el contexto de la sociedad de la información. No obstante, se trata de un asunto complejo, y la determinación de cuáles sean las medidas más adecuadas en esta esfera dependerá con frecuencia y en gran medida del tipo de equipo de tecnología de la información que se trate, de la infraestructura en la que opere y de su ubicación.

3. Las redes informáticas están impulsando muchos de esos cambios. Esas transformaciones también plantean nuevas preocupaciones para la seguridad y la privacidad de la información incorporada a las redes informáticas. Si no se contemplan adecuadamente esas preocupaciones, se corre el riesgo de limitar el pleno potencial de esas redes tanto en lo relativo a la participación en ellas como respecto de su utilidad. Por ese motivo, es preciso adoptar medidas institucionales y tecnológicas que protejan adecuadamente una gran variedad de información que tenga carácter personal, delicado o confidencial, o esté protegida por derechos de propiedad intelectual.

4. Será preciso evaluar minuciosamente las amenazas y riesgos potenciales en cada situación, y resulta absolutamente vital lograr que todos los interesados tomen conciencia de las amenazas y riesgos que les afectan y sobre las que tienen algún control. Sólo entonces comprenderán plenamente y aplicarán los procedimientos de seguridad pertinentes.

5. La atención se centrará en proteger la información presente en las redes que no sea clasificada, garantizar la seguridad o la capacidad de supervivencia de las redes y lograr la fiabilidad de los servicios de las redes informáticas para garantizar el acceso a la información.

6. Se debe examinar tres esferas principales: a) la política en materia de criptografía, en particular las normas y controles gubernamentales de procesamiento de la información; b) las directrices para proteger la información de los organismos

gubernamentales que no sea clasificada; y c) las cuestiones jurídicas y de seguridad de la información, en particular las relativas al comercio electrónico, la privacidad y los derechos de propiedad intelectual.

7. Las salvaguardias en materia de información, en particular las criptográficas, están adquiriendo una importancia creciente. Las salvaguardias adecuadas (contramedidas) deben tener en cuenta y prever los desafíos técnicos, institucionales y sociales que cada vez en mayor medida trasladan a los usuarios finales la responsabilidad de salvaguardar la información. Si no se solucionan las cuestiones que plantean las políticas en materia de criptografía, se malograrán las iniciativas de mayor alcance para salvaguardar la información incorporada a las redes. La medida más importante que cabe adoptar con miras a establecer salvaguardias adecuadas para la información incorporada a las redes en un organismo gubernamental o en una organización de otra índole consiste en que la dirección superior defina los objetivos generales de la organización, formule una política de seguridad de la organización que refleje esos objetivos y que ponga en práctica dicha política. Sólo la dirección superior puede consolidar el consenso y aplicar los recursos necesarios para proteger de un modo eficaz la información incorporada a las redes.

8. Ese punto de vista intenta evaluar las amenazas y los riesgos que plantean las actividades delictivas en el contexto de la tecnología de la información y señalar las recomendaciones que la policía puede ofrecer sobre procedimientos de seguridad y métodos para prevenir los delitos informáticos. Las amenazas a los sistemas de información pueden surgir de actos intencionales y no intencionales y pueden provenir de fuentes externas o internas.

II. Preocupaciones

9. A la Real Fuerza de Policía de Brunei le preocupa que no se preste atención a la preparación de la seguridad en el contexto de las iniciativas nacionales de desarrollo del gobierno electrónico.

10. Hasta el momento, la Real Fuerza de Policía de Brunei no ha sido llamada a participar ni ha participado en los preparativos nacionales del avance hacia la era de la información. Durante los últimos tres años, se ha aprobado una gran cantidad de normas con miras a preparar al país para la era de la información. Asimismo, se han establecido o están en vías de establecerse numerosos órganos gubernamentales y reguladores encargados de impulsar las iniciativas relativas al gobierno electrónico.

11. No se ha promovido activamente la seguridad en lo que respecta a la preparación de los organismos encargados de hacer cumplir la ley, ni se le ha dado la misma prioridad que a otros puntos del temario nacional. En opinión de la Real Fuerza de Policía de Brunei, la seguridad desempeña un papel muy importante en las aspiraciones nacionales de entrar en la sociedad de la información.

12. La seguridad es fundamental para la era de la información. No se puede insistir lo suficiente en la importancia de establecer una infraestructura segura y fiable.

III. Iniciativas de la Real Fuerza de Policía de Brunei

(Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación en ese ámbito)

13. Habida cuenta de que la Real Fuerza de Policía de Brunei es la principal institución encargada de hacer cumplir la ley en el país, desea prestar asistencia en la promoción de los aspectos de seguridad necesarios para entrar plenamente en la era de la información

14. Con esa finalidad, se ha enviado a numerosos agentes a otros países para capacitarse en lo tocante a los delitos relacionados con la Internet, en particular delitos cibernéticos y transnacionales. En un principio, dada la falta de financiación, no se lograron nuevos avances en la compra de los equipos de tecnología de la información y los programas necesarios para investigar los ataques a los sistemas informáticos. En la actualidad, la Real Fuerza de Policía de Brunei tiene capacidad para iniciar investigaciones relativas a delitos cibernéticos.

15. La Real Fuerza de Policía de Brunei ha tomado medidas encaminadas a mejorar la colaboración internacional en este contexto al participar en varios foros dedicados a mejorar las capacidad para hacer cumplir la ley. La Real Fuerza de Policía de Brunei mantiene contactos con redes informáticas regionales e internacionales de organismos encargados de hacer cumplir la ley, lo que mejora su capacidad de perseguir a los fugitivos.

IV. Propuestas y recomendaciones de la Real Fuerza de Policía de Brunei

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

16. La Real Fuerza de Policía de Brunei presenta los siguientes como puntos de partida para facilitar y mejorar la seguridad en el contexto de la seguridad de la información.

A) Comunicación y seguimiento de las amenazas y los puntos débiles:

1) Desde que se estableció el Equipo de Respuesta ante Emergencias Informáticas de Brunei Darussalam en 2004, ha habido cierta forma de control. No obstante, dicho control no es completo, habida cuenta de que el Equipo de Respuesta no tiene vinculación alguna con la Real Fuerza de Policía de Brunei y no existen mecanismos para poner en marcha una respuesta rápida: por ejemplo, el seguimiento o la intercepción de un ataque informático mientras se está produciendo.

B) Mecanismos educativos y de seguridad para un uso seguro de las computadoras:

1) Prestación de apoyo para la elaboración de materiales y programas educativos sobre el ciberespacio para todo tipo de usuarios. Con ello se proporcionaría formación temprana sobre prácticas y conductas seguras y medidas de seguridad en Internet;

2) Inversión en campañas de concienciación en las que se haga hincapié en la necesidad de que los administradores de sistemas, gestores de redes y

oficiales principales de sistemas de información reciban formación sobre seguridad;

3) Facilitación del desarrollo y despliegue de mecanismos de seguridad relativos a la información en el ciberespacio que permitan a las partes en una transacción decidir por sí mismas qué precauciones y limitaciones desean establecer.

C) Investigación y desarrollo:

1) Asignación de fondos para la investigación y el desarrollo en las esferas de la seguridad y la capacidad de supervivencia de las arquitecturas informáticas de los sistemas no administrados con control distribuido;

2) Elaboración de conjuntos de instrumentos de amplio alcance que presten apoyo a los esfuerzos de los administradores de redes por lograr que sus sistemas sean seguros;

3) Elaboración de técnicas de amplio alcance y programas integrales y continuos de identificación y mitigación de los riesgos.

D) Uso de normas:

1) Establecer y alentar la aceptación de las normas de seguridad de los programas informáticos como método de corto plazo para hacer arrancar el proceso de mejoramiento de la seguridad de los productos de Internet;

2) Establecer una política gubernamental por la que todo equipo y programa informático adquirido por el Gobierno deba cumplir normas de seguridad específicas, en particular la exigencia de un servicio de alerta, que informe al cliente de las vulnerabilidades y las formas de repararlas.

E) Leyes y medios para hacerlas cumplir:

1) Prestar apoyo a nuestros policías cibernéticos. Asignar fondos suficientes a los organismos encargados de hacer cumplir la ley, sufragar las actividades de capacitación, los recursos físicos y el personal necesarios para hacer frente a los delitos cibernéticos que se denuncien;

2) Lograr que en las políticas nacionales se refleje la necesidad de que los organismos encargados de hacer cumplir la ley se coordinen internacionalmente para combatir los delitos en el ciberespacio y prestar apoyo a dichos organismos para que concierten acuerdos internacionales sobre persecución ininterrumpida;

3) Lograr que las políticas públicas propicien la difusión del uso del cifrado para proteger a la información y a los usuarios del ciberespacio.

Chile

[Original: español]
[13 de junio de 2007]

1. Chile otorga gran relevancia a la seguridad de la información en el marco de la seguridad internacional. Coincidimos con la preocupación mundial ante la posibilidad de que las tecnologías de la información sean utilizadas con propósitos incompatibles con el objetivo de mantener la estabilidad y seguridad internacionales y afecten a la infraestructura de los Estados. Consideramos que es necesario impedir la utilización de las tecnologías de la información con fines delictivos.
2. En el ámbito legislativo se ha avanzado en la adopción de diversas leyes y normas respecto a la seguridad y confidencialidad de los documentos electrónicos y de la eficiencia de las comunicaciones entre órganos de la administración del Estado y entre éstos y los ciudadanos.
3. Por la importancia que reviste este tema, nuestro país ha participado activamente en las dos fases de la Cumbre Mundial de la Sociedad de la Información, celebradas en Ginebra en diciembre de 2003 y en Túnez en noviembre de 2005.

China

[Original: chino]
[15 de mayo de 2007]

1. El rápido desarrollo y la amplia aplicación de la tecnología de la información contribuyen actualmente de manera activa al desarrollo económico y social y a una mayor calidad de vida en todos los países del mundo. Al mismo tiempo, la seguridad de la información se ha convertido en un importante factor que influye en la seguridad general de los distintos países y en la seguridad y estabilidad mundiales. El tratamiento adecuado de esa cuestión en beneficio colectivo de todos los países es una responsabilidad compartida por la comunidad internacional.
2. A juicio de China la cuestión de la seguridad de la información no sólo está relacionada con los riesgos derivados de la vulnerabilidad y la interconectividad de la infraestructura de la información, sino también con diversos problemas en materia política, económica, militar, social y cultural y en muchas otras esferas provocados por el uso indebido de esa tecnología. En el examen de la cuestión de la seguridad de la información se deberá prestar igual atención a esos dos factores.
3. China considera que la tecnología de la información debe aplicarse de conformidad con lo dispuesto en la Carta de las Naciones Unidas y los principios básicos de las relaciones internacionales y que debe asegurarse 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 entre los distintos países. Todos los países tienen el derecho de regular su propio ciberespacio conforme a su legislación interna. En vista del 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 la aplicación de la tecnología de la información a fin de garantizar la libertad de los países para obtenerla.

4. El Gobierno de China ha otorgado continuamente gran importancia a la cuestión de la seguridad de la información. Ha establecido y aplicado de manera gradual una estrategia nacional en materia de seguridad de la información y ha formulado varias leyes y normas en la materia. Ha dedicado grandes esfuerzos a fortalecer la supervisión de los incidentes relativos a la seguridad del ciberespacio, a perfeccionar el mecanismo de coordinación y gestión, a llevar a cabo estudios sobre tecnologías relacionadas con la seguridad del ciberespacio y a crear un sistema de gestión de crisis respecto a la seguridad del ciberespacio, lo que ha contribuido a mejorar de manera continua la seguridad de las redes de información y los sistemas de información fundamentales.

5. China participa activamente en la cooperación internacional relativa al ámbito de la seguridad de la información. En junio de 2006, los jefes de los Estados miembros de la Organización de Cooperación de Shanghai firmaron la “Declaración de los jefes de los Estados miembros de la Organización de Cooperación de Shanghai sobre la seguridad internacional de la información”, en la cual se decidió crear un grupo de expertos internacionales en materia de seguridad de la información. China ha participado de manera constructiva en la labor de ese grupo de expertos.

6. China considera que las Naciones Unidas son el foro apropiado para estudiar la cuestión de la seguridad de la información. En 2004 y 2005 el Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances de la información y las telecomunicaciones en el contexto de la seguridad internacional examinó la cuestión de la seguridad de la información en todos sus aspectos y formuló varias propuestas valiosas que han sentado una sólida base para que la comunidad internacional siga examinando esa cuestión en el futuro. China está a favor de que en 2009 las Naciones Unidas restablezcan el Grupo de Expertos Gubernamentales, a fin de examinar ampliamente y en profundidad las amenazas y los desafíos en materia de seguridad de la información y buscar soluciones eficaces. China seguirá apoyando las iniciativas internacionales en ese ámbito y participando en ellas de manera activa.

Cuba

[Original: español]
[16 de mayo de 2007]

1. Los resultados que Cuba puede exhibir en materia de tecnologías de la informática y las comunicaciones, en estos momentos, se basan en un alto carácter social, ajeno a cualquier manifestación de consumismo y formando especialistas de nuevo tipo, con total comprometimiento y valores éticos ajenos a los patrones que promueve el mundo globalizado y neoliberal.

2. El sustancial mejoramiento de la infraestructura tecnológica o la masiva y profunda preparación del capital humano desde edades tempranas, son ejemplos de los ingentes esfuerzos del Estado cubano por transitar aceleradamente hacia la informatización de la sociedad, como vía para aumentar la calidad de vida, la eficiencia y la competitividad del país.

3. Sobre la base de esa política, Cuba ha organizado el uso racional y eficiente de los recursos informáticos, tanto de equipamiento como de conectividad, de forma social masiva. Así se priorizan sectores claves como la salud, la educación, los centros científicos, instituciones culturales y empresas, que garantizan el desarrollo económico y social de la nación.

4. Sin embargo, este desarrollo se ha enfrentado a un cruel y prolongado bloqueo económico, comercial y financiero desde los Estados Unidos de América, cuyas acciones se han acrecentado con la administración actual.

5. La conexión de Cuba a Internet data de 1996, cuando el gobierno norteamericano otorgó a Cuba la licencia para el acceso. Sin embargo, en la actualidad, a pesar de que muy cerca de las costas cubanas pasan cables internacionales de fibra óptica, las leyes del bloqueo han impedido la conexión a ellos, con lo que la nación se ve obligada a emplear una canal satelital con escasos 65 Mbps de ancho de banda para la salida y 124 Mbps para la entrada. La conexión a través de fibra óptica no sólo permitiría mayor velocidad de conexión, sino costos significativamente menores. Las propias Leyes establecen que cualquier nueva adición o modificación del canal requiere la obtención de Licencia del Departamento del Tesoro de los Estados Unidos.

6. En cuanto a infraestructura tecnológica, el bloqueo norteamericano contra Cuba no sólo nos impide la adquisición de equipamiento y programas informáticos desde compañías norteamericanas; por su carácter extraterritorial persigue nuestras operaciones comerciales con empresas de otras nacionalidades y se bloquea la descarga de software e informaciones, incluso las gratuitas, si el número IP se identifica con Cuba.

7. Internet, como área común global, tiene ciertamente retos por superar; no sólo aquellos referidos a su gobernabilidad por toda la humanidad, y la consecuente inclusión de todos los países en su administración, sino también a la erradicación de flagelos universalmente condenados, como la difusión de pornografía, la incitación al terrorismo, el racismo, el fraude, la divulgación de ideologías fascistas y cualquier manifestación de crimen cibernético.

8. Pero otro gran reto, acallado por los países ricos, es la eliminación de su carácter selectivo y elitista, que hoy traslada las desigualdades y barreras del mundo real al espacio cibernético, generando lo que se ha dado en llamar “brecha digital”.

9. Millones de personas en el mundo están muy distantes de convertirse en “internautas”, cuando aún no saben leer y escribir y su gran preocupación diaria es sobrevivir al hambre, la sed y las enfermedades. Con la voluntad política de los gobiernos, la cooperación internacional y un mínimo de recursos de los que hoy el llamado mundo desarrollado despilfarra en publicidad, sobre consumo o carrera armamentista, Internet podría convertirse en vehículo para la realización de una revolución cultural y educativa que promueva el conocimiento, que promulgue educación, cultura, cooperación, solidaridad junto a valores éticos y morales que requiere este nuevo siglo, propugnando los sentimientos humanos más nobles y desechando las conductas inhumanas, egoístas e individualistas.

10. Por otra parte, las agencias de seguridad han prestado especial atención al tema y su mayoría las utilizan como asesores del Gobierno. Con la asignación de gigantescos fondos, han desarrollado diversos medios y programas para fortalecer tecnologías existentes o crear nuevas posibilidades de interceptación de las

comunicaciones, acceso a sistemas y bases de datos, sistemas de identificación y seguimiento de vehículos y personas. Estos complejos entramados incluyen sistemas de antenas, estaciones de escucha, radares y satélites, apoyados por submarinos y aviones espías, todos unidos a supercomputadoras y aplicaciones especializadas.

11. Sería muy ingenuo pensar que las compañías proveedoras de servicios y tecnologías, en su colaboración con las mencionadas agencias, no facilitan información que posibilite la labor de inteligencia y espionaje por parte de aquellas. Téngase en cuenta que, de conformidad con las disposiciones de la denominada “Ley Patriótica” de los Estados Unidos de América, se le otorga autoridad al gobierno para exigir a cualquier empresa información, secreta o no, si considera que esta resulta de interés para la seguridad nacional.

12. Con la premisa de que el conocimiento es patrimonio de toda la humanidad, se impone democratizar la presencia y distribución del capital de información que debe ser puesto en función de la paz y el desarrollo, pues son imprescindibles para seguir avanzando en el nuevo milenio.

Líbano

Las cartas que se transcriben a continuación, que fueron recibidas por la Misión Permanente del Líbano ante las Naciones Unidas, constituyen comunicaciones entre la Misión y los Ministerios de Telecomunicaciones, del Interior y de Defensa del Líbano.

Ministerio de Telecomunicaciones

[Original: inglés]
[4 de junio de 2007]

1. Estamos en vías de dictar una nueva ley relativa al sector de las tecnologías de la información y las comunicaciones en el Líbano, que se encuentra en la fase final de aprobación por la Cámara de Diputados. Dicha ley abarcará la seguridad y todas las demás cuestiones atinentes a los delitos relativos a la información.

2. Cuando dicha ley entre en vigor, el Ministerio de Telecomunicaciones abordará las secciones b), c) y d) conjuntamente con otros ministerios y todas las administraciones interesadas.

Ministerio del Interior

[Original: árabe]
[23 de mayo de 2007]

I. En el plano nacional

1. El intercambio de información entre las distintas secciones de las Fuerzas de Seguridad Interna se lleva a cabo a través de medios de comunicación fijos (teléfono y fax) e inalámbricos (como los centros de operaciones en todas las regiones). Esta manera de intercambiar información está expuesta a ser violada o interceptada, o a ser objeto de escuchas, pese a que la Dirección General ha comenzado a adoptar la red de comunicación TETRA para las Fuerzas de Seguridad Interna en algunas zonas como paso previo a su generalización en todas las regiones, además de haber

proporcionado recientemente a las Fuerzas de Seguridad Interna una red cerrada de líneas de telefonía móvil en aplicación del decreto del Consejo de Ministros No. 47, de 15 de septiembre de 2006.

II. En el plano internacional

2. El intercambio de información, especialmente la de seguridad, entre las Fuerzas de Seguridad Interna y otros organismos internacionales se lleva a cabo por medio del Departamento de Comunicación Internacional de la Dirección General de las Fuerzas de Seguridad Interna, que cuenta con una estación de transmisión y recepción de información de seguridad por conducto de la oficina de la Interpol en Beirut, que depende de la mencionada Dirección General. En la actualidad se utiliza un sistema normal de comunicación basado en tecnología de Internet, que se caracteriza por la rapidez en el intercambio de información y su capacidad para proteger la confidencialidad mediante redes especializadas que garantizan su mantenimiento de acuerdo con la Organización Internacional de Policía Criminal (Interpol), que supervisa la gestión y mejora de esa red.

III.

3. En lo que se refiere al párrafo a), relativo a la evaluación general de los problemas de la seguridad de la información, las Fuerzas de Seguridad Interna hacen todo lo posible por utilizar medios técnicos eficaces en materia de seguridad de la información y las comunicaciones fijas e inalámbricas. En este ámbito se afrontan numerosos retos entre los que cabe destacar la unificación de criterios sobre la estructura de la seguridad de la información y un entorno de protección con criterios apropiados y aceptables que satisfagan la creación, aplicación y refuerzo de los sistemas de información de seguridad y las medidas de control de estos sistemas.

4. En lo que respecta a los párrafos b) y c), relativos a las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito, hemos tenido experiencias concretas y realistas sobre cómo valorar los peligros de intrusión en función del estado de la red informática de la que disponemos y en este campo hemos hecho todo lo posible para mejorar las condiciones de seguridad de nuestra red de información sirviéndonos de técnicas y soluciones modernas y de medidas de aplicación adoptadas para la protección y recuperación de los sistemas y la evaluación de la inmunidad frente a intrusiones y virus, así como adoptando planes que permitan seguir trabajando en caso de ataque a los sistemas, y asimismo formando personal capacitado que pueda intervenir en caso de que surja una urgencia.

5. En lo que se refiere al párrafo d), relativo a las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad informática a escala mundial, para empezar proponemos adoptar una política preventiva para poner fin a los intentos individuales de intrusión, colaborar a nivel internacional en este ámbito y elaborar una ley específica para combatir el sabotaje y el intrusismo contra las redes de información que tipifique a esas acciones como delitos, además de beneficiarse del intercambio de experiencias entre los Estados miembros, lo que supondría un salto cualitativo en este ámbito.

6. Hay que mencionar que en este ámbito la Dirección General ha adoptado las siguientes medidas:

a) Creación de una oficina especial contra la delincuencia informática en las Fuerzas de Seguridad Interna, entre cuyas funciones principales está la de advertir sobre los delitos informáticos y sobre los peligros que amenazan la seguridad de la información digital, además de investigar y perseguir judicialmente a quienes cometan delitos informáticos;

b) Participación de oficiales especializados de las Fuerzas de Seguridad en los trabajos de preparación del proyecto de ley para combatir la delincuencia informática, que ha preparado la comisión parlamentaria de tecnología, y que se encuentra listo para su ratificación por parte del parlamento;

c) Participación activa de las Fuerzas de Seguridad Interna en las actividades de la Interpol y en los trabajos de la Comisión regional de Oriente Medio y Norte de África contra la delincuencia informática de Interpol, puesto que el vicepresidente de esta Comisión y uno de sus miembros son oficiales de las Fuerzas de Seguridad Interna especializados en el campo de la informática. Asimismo, el presidente de la Oficina de lucha contra la delincuencia informática es el oficial de enlace con la Interpol en asuntos relativos a la seguridad de la información y la lucha contra los delitos informáticos, especialmente aquellos que afectan a la seguridad de la información.

7. En vista de que las amenazas existentes, a nivel nacional e internacional, para la seguridad en general, y en especial para los sistemas de información y las comunicaciones, es imperativo establecer una estrategia de futuro que contemple el desarrollo técnico y aspire a garantizar la protección y hallar los medios para hacer frente a cualquier intento de infracción; a este respecto señalamos lo que se expone a continuación.

a) Dinamismo de la información y criterios de seguridad

8. Hay un gran dinamismo en los medios de transferencia y conservación de la información debido al desarrollo tecnológico, pese a la dificultad que supone controlar los “sistemas/medios/contenidos”, lo que exige medidas de protección a todos los niveles y la elaboración de criterios internacionales para la norma sobre la seguridad de la información (ISO 17799).

b) El Líbano y la seguridad de la información

9. El Líbano carece de instrumentos jurídicos y legislativos para crear un entorno seguro para la información. No existe ninguna ley o procedimiento administrativo que obligue a las administraciones e instituciones oficiales a aplicar los criterios de la norma sobre la seguridad de la información (ISO 17799). Hay que mencionar que en la actualidad se aplica un compendio de directrices similares a los criterios internacionales, adoptadas por el Banco del Líbano y algunas bancos privados. Tampoco existe legislación que regule las bases de la codificación en las redes de comunicación privadas.

c) A nivel de la aplicación

10. No se cumple la directriz del Ministerio de Telecomunicación No. 4/2 de 19 de diciembre de 2005, sobre el mantenimiento de los expedientes de circulación de la

información, ni existe legislación que regule el funcionamiento de los cibercafés, así como tampoco hay un control eficaz de las comunicaciones por satélite en el espacio libanés.

11. Hay que señalar que en los Estados Unidos de América, a raíz de los ataques terroristas del 11 de septiembre, se ha creado un Ministerio de Seguridad Interior y se ha adoptado un sistema de control de todos los sistemas de comunicación nacionales que asegura el análisis y el control, y asimismo se han dispuesto estrictos instrumentos jurídicos en el ámbito de la codificación de datos y de la entrada y salida a las redes.

d) Medios de lucha y de protección

12. Ha quedado demostrado que el ciberespacio, en tanto que red de Internet que se rige por el protocolo de comunicación TCP/IP es un entorno frágil e inseguro al que las organizaciones delictivas podrían agredir e incluso destruir, debido a que otorga prioridad a los fines comerciales y a las ventas. Asimismo, la delincuencia informática se caracteriza por la rapidez y la ausencia de límites y controles, mientras que las medidas para combatirla son lentas, la coordinación inexistente y los instrumentos jurídicos insuficientes.

13. Se han realizado numerosas mejoras en los protocolos de Internet, en lo tocante a los usuarios y a la codificación, como el protocolo IPv6, y se están llevando a cabo investigaciones serias para lograr tecnologías de seguridad para redes informáticas susceptibles de combatir los delitos de intrusión o destrucción.

14. Los acuerdos internacionales para la lucha contra la delincuencia cibernética, especialmente el Convenio sobre delincuencia cibernética de Budapest, contemplan la cooperación rápida entre Estados y han dado lugar a:

- La creación de una red de comunicaciones 7/24 paralela a la red de la Interpol y especializada en delincuencia informática;
- La constitución de un comité permanente y de grupos de trabajo regionales para estimular la cooperación técnica y mejorar la competencia de las oficinas de lucha contra la delincuencia cibernética.

15. Sin embargo, parece que ese Convenio no es capaz de garantizar una lucha rápida e inmediata contra los virus que pueden lanzarse a la red.

e) Propuestas:

16. Se formulan las propuestas siguientes:

- Aplicar y desarrollar instrumentos jurídicos en el ámbito de la seguridad de la información y normas de protección de la seguridad informática;
- Activar y mejorar las medidas de seguridad de todos los organismos pertinentes con vistas a proteger los medios y los sistemas de información;
- Activar y desarrollar sistemas especializados en el Ministerio de Telecomunicaciones y garantizar que interactúen con los organismos e instituciones públicos y privados de seguridad con vistas a encontrar un entorno seguro para los sistemas de información;

- Seguimiento de las novedades mundiales, sobre todo en la aplicación de protocolos de Internet como el IPv6, y adopción de los medios técnicos necesarios para conocer la identidad de toda persona que entra en la red de Internet y de un sistema de identificación digital (certificado digital);
- Activar la coordinación entre los sistemas de protección del derecho en el ámbito de la seguridad de la información y establecer unos criterios internacionales a nivel técnico que garanticen un fácil seguimiento, control y coordinación; y unificar al máximo los sistemas legislativos, preservando la seguridad nacional a la par que las exigencias de la seguridad internacional.

17. La Dirección General de Seguridad Pública informa que sus comunicaciones de seguridad se efectúan dentro del territorio libanés y que no lleva a cabo comunicaciones exteriores. En lo que se refiere a las comunicaciones interiores, los sistemas de protección están siendo mejorados con la ayuda de la experiencia de algunos organismos de seguridad amigos, aunque los equipos necesarios no se encuentran todavía disponibles por no disponer de los medios materiales y técnicos.

Ministerio de Defensa

[Original: árabe]
[1° de mayo de 2007]

El Ministerio de Defensa Nacional transmite la siguiente comunicación del Líbano:

- Su determinación de no utilizar la tecnología de la información y las telecomunicaciones con fines no acordes con los conceptos de la estabilidad y la seguridad internacionales;
- La adopción de las medidas necesarias a nivel nacional (mejora y modernización de los reglamentos y leyes conexas) para reforzar la seguridad de la información y alentar el intercambio de la información disponible entre las partes interesadas;
- El respeto a las resoluciones de las Naciones Unidas sobre la protección de la seguridad de la información y la confidencialidad, evitando por todos los medios su uso indebido y prohibiendo el uso de recursos o tecnologías informáticos con fines delictivos o terroristas.

México

[Original: español]
[22 de mayo de 2007]

1. México ha dado su apoyo a la resolución sobre “Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”, presentada por la Federación de Rusia en la Asamblea General de la ONU y considera de gran importancia la promoción de un mayor intercambio de puntos de vista sobre el tema y los conceptos conexas. Estima que podrían ser aprovechados los trabajos de la Primera Comisión, o de otros foros de desarme para realizar paralelamente presentaciones por expertos o discusiones sobre el tema.

2. La mayor parte de los mecanismos de verificación internacional derivados de instrumentos jurídicos internacionales o bien de acuerdos políticos de control de las exportaciones se valen de medios de información y telecomunicaciones para su efectivo funcionamiento, y en estos campos resulta de primer orden examinar el estado que guardan los avances al respecto. Por otro lado, el desarrollo de los sistemas de misiles balísticos, y de modernización de arsenales nucleares supone un desarrollo en información y telecomunicaciones que necesariamente está presente. Además, los desarrollos en materia de tecnologías en el espacio ultraterrestre y satelitales sin duda están vinculados con aspectos de seguridad internacional.

3. México ha señalado constantemente, en el marco de la Conferencia de Desarme, la urgencia de adoptar un programa de trabajo que incluya como uno de sus temas centrales “la prevención en la carrera de armamentos en el espacio ultraterrestre (PAROS)”, el cual se considera está vinculado con la vulnerabilidad de las Tecnologías de la Información y las Comunicaciones (TIC) que se encuentran en el espacio.

4. México estima de importancia la continuación de la labor del Grupo de Expertos Gubernamentales (GEG) sobre el tema creado de conformidad con la resolución 58/32 de la Asamblea General, y que se restablecerá en 2009. Por ello estima que una discusión amplia debería ser promovida en tanto esa fecha se cumple.
