Naciones Unidas A/64/129

Asamblea General

Distr. general
8 de julio de 2009
Español
Original: español/inglés/ruso

Sexagésimo cuarto período de sesiones
Tema 90 de la lista preliminar*
Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Los avances en la esfera de 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
Brasil 2
Kazajstán 4
Líbano 8
Lituania 8
México 10
Serbia 11
Tailandia 12
Tayikistán 14
Ucrania 15

* A/64/50.

09-39636 (S) 300709 310709

Se ruega reciclar

I. Introducción

1. En el párrafo 3 de su resolución 63/37, 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 colaboración internacional en ese ámbito;

c) El contenido de los conceptos mencionados en el párrafo 2 de la resolución;

d) Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

2. En cumplimiento de dicha solicitud, el 27 de febrero de 2009 se envió una nota verbal a los Estados Miembros en que se les invitaba a ofrecer información sobre el particular. Las respuestas recibidas se reproducen en la sección II *supra*. Las demás respuestas que se reciban se publicarán en adiciones del presente informe.

II. Respuestas recibidas de los Gobiernos

Brasil

[Original: inglés]
[11 de junio de 2009]

1. La información y las telecomunicaciones son parte esencial de las sociedades modernas, que dependen en gran medida de ellas. Las actividades de la vida contemporánea no pueden concebirse sin la disponibilidad constante de esos servicios, que pasan a ser valiosos recursos cuya importancia es vital para la riqueza y la prosperidad de las naciones.

2. Los avances tecnológicos que hicieron posible esta realidad también han suscitado diversas preocupaciones en el contexto de la seguridad internacional. Habida cuenta de que las sociedades dependen cada vez más de la disponibilidad de información y la infraestructura de las telecomunicaciones, han surgido nuevas vulnerabilidades que podrían explotarse en situaciones de conflicto militar y en la realización de actividades delictivas y terroristas.

3. El aprovechamiento de esas vulnerabilidades podría entorpecer el normal funcionamiento de empresas privadas, bancos, mercados de valores y entidades gubernamentales. La interconexión cada vez más estrecha, sin dudas beneficiosa, entre las redes de comunicación de las que dependen dichas entidades plantea, a su vez, una serie de preocupaciones nuevas que requieren la atención de los Estados a nivel nacional e internacional.

4. Al tiempo que los avances en la esfera de la información y las telecomunicaciones pueden crear vulnerabilidades, también constituyen un activo que puede utilizarse como arma cibernética. Existen ya fuerzas armadas nacionales que cuentan con unidades militares especializadas que han sido entrenadas y equipadas para desactivar o incluso destruir infraestructura vital mediante operaciones de invasión y sabotaje de las redes de información. En función del objetivo y de los medios empleados, los efectos de esos ataques van desde la "neutralización" del arma del enemigo o los sistemas sensores a la perturbación cataclísmica de las redes de suministro de electricidad de todo un país.

5. La eficiencia de esta forma de actividad bélica se ve incrementada por el hecho de que muchas de esas capacidades pueden crearse con inversiones relativamente modestas. En vista de esos factores, en el futuro inmediato, la guerra cibernética podría muy bien convertirse en la piedra angular de los conflictos militares entre los Estados. Las mismas tácticas podrían ser empleadas por individuos con fines terroristas o por organizaciones terroristas.

6. Consciente de la importancia de esta cuestión para el mantenimiento de la paz y la seguridad internacionales, el Brasil sugiere que la misma se aborde de dos formas diferentes. En primer lugar, la comunidad internacional debería tratar de crear los instrumentos apropiados para hacer frente a las actividades delictivas y terroristas relacionadas con la tecnología de la información. Desde una perspectiva diferente pero complementaria, debería examinar asimismo los efectos de la aparición de actividades bélicas en el ámbito cibernético y la posible necesidad de establecer regímenes de desarme y no proliferación, así como normas internacionales sobre ese tipo de actividades, que tengan en cuenta sus múltiples efectos.

7. Las actividades delictivas y terroristas deberían examinarse apropiadamente en los foros pertinentes, y las Naciones Unidas deben desempeñar una función importante en la prestación de asistencia, en caso necesario, para que los Estados Miembros puedan lograr, entre otros, los siguientes objetivos:

- Establecer redes alternativas y de emergencia para proteger la infraestructura vital;
- Examinar la estructura de las redes analizando las interdependencias y determinar métodos eficaces de protección;
- Establecer una estrecha cooperación entre los gobiernos y el sector privado, a fin de lograr el grado deseado de seguridad de la información que intercambian entre sí las organizaciones;
- Establecer sistemas de protección para evitar o reducir al mínimo los efectos de los ataques cibernéticos;
- Aplicar instrumentos y medidas que permitan a las autoridades detectar el origen de los ataques cibernéticos;
- Examinar la pertinencia y conveniencia de adoptar instrumentos internacionales jurídicamente vinculantes respecto de los delitos cibernéticos;
- Capacitar a las instituciones nacionales para que realicen pruebas y evaluaciones del nivel de seguridad de los sistemas de información;

- Establecer procedimientos para la notificación mutua de las amenazas cibernéticas entre las autoridades nacionales competentes;
- Evitar la creación de mecanismos discriminatorios que impidan el acceso de los países a la alta tecnología en el campo de las telecomunicaciones y los sistemas de información;
- Realizar actividades de educación y concienciación acerca de la importancia de la seguridad cibernética.

8. Las Naciones Unidas deberían asimismo asumir un papel protagónico en el debate sobre el uso de la información y las telecomunicaciones como armas cibernéticas en situaciones de conflicto entre los Estados y prestar especial atención a los aspectos siguientes:

- Identificación, descripción y clasificación de las actividades bélicas en la esfera de la información;
- Identificación y clasificación de las armas informáticas y los medios que pueden utilizarse como tales;
- Establecimiento de un código de conducta para la utilización de las armas informáticas;
- Instauración de garantías que permitan a todos los países disfrutar en pie de igualdad del derecho a proteger su territorio contra ataques cibernéticos;
- Preparación de un glosario de las Naciones Unidas que contenga definiciones de los principales términos relacionados con la información y las comunicaciones en el contexto de la seguridad internacional.

Kazajstán

[Original: ruso]
[2 de julio de 2009]

1. El desarrollo activo de las tecnologías de la información y las comunicaciones a nivel mundial trae consigo cambios globales en todas las esferas de la vida de cualquier país. Como se observa en la Carta de Okinawa sobre la sociedad mundial de la información, “las tecnologías de la información y las comunicaciones figuran entre los factores más importantes que influyen en la formación de la sociedad del siglo XXI. Su influencia transformadora se extiende al modo de vida de las personas, su educación y vida laboral, así como a la interacción entre los gobiernos y la sociedad civil”.

2. En el contexto de la aceleración del progreso científico y técnico contemporáneo se observa claramente una tendencia a la informatización, así como a la creación de amplios sistemas de procesamiento de datos. La Internet afecta prácticamente todos los aspectos de la vida política y social y es cada vez mayor el número de personas que la usan. En ese caso, los servicios de información, los sistemas de procesamiento de datos y las redes digitales se convierten en el eslabón más débil de la infraestructura nacional de los Estados.

3. Habida cuenta de que la Internet sigue siendo un espacio virtualmente libre y que en la práctica nadie controla, asociaciones delictivas tratan activamente de aprovecharse de las posibilidades que ofrecen las tecnologías de la información. Según expertos de la Cámara de Comercio Internacional, el número de delitos asociados con el uso de la Internet aumenta en la misma proporción que el número de usuarios de la Red. Según datos proporcionados por la INTERPOL, la Internet es un ámbito en que "el delito aumenta al mismo ritmo en todo el planeta".

4. Los delitos en cuestión podrían agruparse en tres categorías:

a) Delitos universales contra el Estado y la sociedad que representan una amenaza para la seguridad nacional y social por medio de la incitación al derrocamiento del orden establecido, el menoscabo de la soberanía y la independencia y el socavamiento de los intereses nacionales, así como por medio de la propaganda en favor del terrorismo, el chovinismo, la xenofobia y todas las formas de extremismo y de discriminación por motivo de origen étnico, raza, religión, género u otro motivo;

b) Delitos civiles universales que representan una amenaza contra los derechos y las libertades individuales (atentado contra los derechos y las libertades individuales, chantaje, presiones, difamación, divulgación de información confidencial, uso de la Internet con cargo a una cuenta ajena, falsificación de documentos, violación del derecho de autor, etc.);

c) Delitos tradicionales que representan una amenaza contra la moral y las buenas costumbres (pornografía, pedofilia, otros tipos de perversiones sexuales, drogadicción, alcoholismo, etc.).

5. La circulación de este tipo de información es prueba de que subsisten lagunas en las leyes nacionales respecto de la regulación de las relaciones jurídicas que se establecen en la Internet y plantea la necesidad de aplicar un nuevo enfoque supranacional. A nivel internacional sigue sin aplicarse un enfoque normativo único en relación con la definición y evaluación de las amenazas en el ámbito de la seguridad de la información y no se han creado mecanismos de cooperación internacional para prevenir dichas amenazas. Ninguno de los conceptos propuestos hasta la fecha por uno u otro país acerca de la seguridad internacional en la esfera de las tecnologías de la información tiene un alcance universal.

6. Entre las causas de todo ello figuran, entre otros factores, la brecha tecnológica que separa a los países desarrollados de los menos adelantados, la existencia de diferencias políticas latentes y la aplicación de enfoques divergentes a la hora de examinar fenómenos y acontecimientos en el espacio cibernético.

7. En documentos elaborados por las Naciones Unidas y la Organización para la Seguridad y la Cooperación en Europa (OSCE), una de las cuestiones prioritarias es la amenaza de la delincuencia y el terrorismo en la esfera de las tecnologías de la información, dejándose de lado la posibilidad del uso ilícito de los avances logrados en el campo de las tecnologías de la información como armas cibernéticas en conflictos armados con las que ejercer una posición dominante en el espacio cibernético y amenazar la soberanía y la identidad nacionales y soslayándose además las amenazas naturales y tecnológicas contra la infraestructura cibernética de los Estados.

8. Un aspecto importante de la protección contra esas amenazas sería no sólo la concertación de acuerdos con aliados militares y políticos en la esfera de la seguridad de la información a nivel internacional, sino además de acuerdos políticos y jurídicos sobre la renuncia mutua a usar el arma cibernética, la creación de mecanismos conjuntos de mitigación de los efectos de actividades perniciosas y la renovación de la infraestructura cibernética de los países.

9. Cabe destacar que ya están en marcha esfuerzos similares con la participación de representantes de la República de Kazajstán en el marco de la Organización del Tratado de Seguridad Colectiva (OTSC) y la Organización de Cooperación de Shangai, en las que se examina a nivel de expertos la posibilidad de concluir los acuerdos intergubernamentales pertinentes. En particular, en cumplimiento del Plan de Acción de los Estados miembros de la Organización de Cooperación de Shangai en relación con la seguridad de la información a nivel internacional, aprobado por decisión del Consejo de Jefes de Estado de los Estados miembros de la Organización, reunido en Bishkek el 16 de agosto de 2007, el grupo de expertos de esos Estados en cuestiones de protección de la información a nivel internacional elaboró un proyecto de acuerdo intergubernamental para la cooperación en materia de seguridad de la información a nivel internacional. El acuerdo se firmó en Ekaterinburg, el 15 de junio de 2009, durante la reunión del Consejo de Jefes de Estado de los Estados miembros de esa organización.

10. Hay que señalar que este acuerdo no tiene antecedentes en la práctica mundial y, dada la posibilidad de que se adhieran a él otros Estados, su entrada en vigor reviste una gran importancia a nivel internacional.

11. Además, en el marco de la OTSC funciona un grupo provisional de trabajo adscrito al Comité de secretarios de consejos de seguridad de la Organización para las cuestiones de política y seguridad en el ámbito cibernético. El grupo elaboró el Programa de actividades conjuntas para establecer un sistema de seguridad de la información de los Estados miembros de la OTSC.

12. Los Estados miembros de la OTSC han puesto en práctica medidas preventivas en el marco de la operación “PROXY”, sobre la base de una concepción común de los objetivos de la cooperación entre los órganos de seguridad y orden interior (policía).

13. Habida cuenta del carácter masivo y transnacional de la Internet, proponemos que los Estados Miembros de las Naciones Unidas elaboren y aprueben una Convención Internacional sobre la Seguridad de la Información, entre cuyos pilares figure la lucha contra la delincuencia cibernética.

14. Dicho instrumento debería tener como finalidad fomentar la cooperación internacional mutuamente beneficiosa en la esfera de la seguridad de la información y la prevención de consecuencias geopolíticas negativas en el espacio cibernético mundial.

15. En dicha Convención, además, debería preverse la creación de mecanismos institucionales, técnicos, programáticos y sociales en materia de obtención de información y su utilización con el objetivo de proteger el orden constitucional, la soberanía y la integridad territorial de todos los Estados Miembros de las Naciones Unidas, la estabilidad política, económica y social, el respeto de la ley y el orden público, así como de mecanismos que faciliten el ejercicio de los derechos y las libertades constitucionales de las personas y los ciudadanos.

16. En el plano nacional, en Kazajstán se elaboró un proyecto de ley sobre la introducción de enmiendas y adiciones en algunos instrumentos legislativos del país relativos a las redes de información y telecomunicaciones, que actualmente examina el Senado del Parlamento.

17. En el referido proyecto de ley se prevé el fortalecimiento legislativo de las normas que regulan la difusión de información en el territorio de la República de Kazajstán por medio de las redes de información y telecomunicaciones.

18. Con el fin de fortalecer la seguridad cibernética y la cooperación internacional en ese ámbito, los órganos de seguridad nacional de Kazajstán realizan importantes esfuerzos. Se realizan en forma permanente actividades encaminadas a detectar y reprimir delitos cibernéticos a nivel internacional.

19. Así, en 2008, el Comité de Seguridad Nacional, conjuntamente con el Servicio Federal de Seguridad de la Federación de Rusia, desmanteló una asociación delictiva transnacional de piratas cibernéticos que habían extorsionado grandes sumas, poniendo fin a repetidos ataques del tipo “denegación de servicio” contra los sitios web de empresas que realizaban sus actividades comerciales en línea.

20. Los resultados de las pesquisas llevadas a cabo en ese ámbito revelan la aparición de nuevas formas de delitos cibernéticos, que van de la extorsión, el chantaje, la trata de personas, el proxenetismo y la distribución de materiales pornográficos al culto de la crueldad y la violencia y la propaganda en favor del terrorismo y el extremismo.

21. Por ejemplo, en 2008 se detectaron 45 casos de distribución de materiales pornográficos, a propósito de lo cual es necesario señalar que ha aumentado el acceso a la pornografía infantil en la Internet. Si en 2005-2006 se registró un solo caso de distribución de pornografía infantil, el número de casos similares aumentó a 7 en 2007, y a 14 en 2008, entre ellos 2 en sitios web de Kazajstán.

22. Hay que señalar, además, que la represión del delito en el ámbito de la seguridad de la información y las tecnologías de punta no responde a las necesidades actuales, debido a la carencia de una base legislativa en la que se regulen de manera estricta las cuestiones relativas a la seguridad de la información.

23. Deberán perfeccionarse los instrumentos jurídicos y normativos vigentes en ese ámbito, teniendo en cuenta la realidad contemporánea.

24. A nuestro juicio, sería conveniente modernizar, a partir de la experiencia de los países más avanzados, la legislación penal vigente con miras a reforzar la penalización de los delitos cibernéticos.

25. Por otro lado, si se tiene en cuenta la naturaleza transnacional de los delitos cibernéticos, se comprenderá la necesidad de que los órganos encargados de hacer cumplir la ley amplíen permanentemente los ámbitos de cooperación operacional, a fin de responder con celeridad a los ataques contra la Internet. Los resultados de la cooperación entre los órganos encargados de hacer cumplir la ley de Kazajstán y órganos homólogos y servicios especiales de otros Estados apuntan a la intensificación de los ataques cibernéticos provenientes de sitios web de Kazajstán. Como consecuencia de esos ataques, las partes afectadas tropiezan constantemente con dificultades operativas a la hora de transmitir información sobre los ataques sufridos, por cuanto no existe en Kazajstán ningún servicio oficial encargado de recibir y

enviar informes sobre incidentes cibernéticos a los órganos competentes del Estado, a diferencia de otros países en los que existen centros de seguridad cibernética.

26. A tal fin, creemos que es necesario crear en los órganos encargados de hacer cumplir la ley dependencias especializadas que se ocupen de detectar, reprimir y esclarecer los delitos contra la seguridad de la información y dotarlas de los medios necesarios para combatir esos delitos.

27. Por último, Kazajstán presentó a sus candidatos a miembro del grupo de expertos gubernamentales que se establecerá de conformidad con lo dispuesto en el párrafo 4 de la resolución 63/37 de la Asamblea General, titulada “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.

Líbano

[Original: inglés]
[22 de mayo de 2009]

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 su fase final de aprobación por la Cámara de Diputados; dicha ley abarcará todas las cuestiones conexas, incluidas la seguridad y las demás cuestiones relativas a los delitos en el ámbito de la información.

2. Una vez que la ley entre en vigor, el Ministerio de Telecomunicaciones abordará las cuestiones que figuran en los apartados b), c) y d) del párrafo 3 de la resolución 63/37 conjuntamente con otros ministerios y todas las administraciones competentes.

Lituania

[Original: inglés]
[26 de mayo de 2009]

1. Lituania atribuye una gran importancia a la seguridad de la información tanto en su política nacional como internacional. La cuestión de la seguridad cibernética es un elemento importante de la seguridad nacional.

2. La cooperación a nivel internacional es sumamente importante para poder intensificar la protección de los sistemas de comunicación e información, así como para promover una mayor conciencia en ese ámbito. Lituania acoge con beneplácito el hecho de que la cuestión relativa a la seguridad de la información reciba una atención cada vez mayor en los programas de organizaciones internacionales como las Naciones Unidas, la Unión Europea, la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Seguridad y la Cooperación en Europa, a la vez que participa activamente en la labor de esas organizaciones en lo que atañe a seguridad de la información. Las instituciones lituanas cooperan estrechamente con sus asociados. Desde el 1º de julio de 2004, Lituania es parte en la Convención del Consejo de Europa sobre la ciberdelincuencia.

3. Lituania es uno de los siete países miembros de la OTAN que patrocinó el establecimiento del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN en Tallin (Estonia), reconocido como centro de excelencia de la OTAN el 14 de mayo de 2008.

4. El 11 de marzo de 2005, por decisión del Parlamento Europeo y del Consejo de Europa, se aprobó el programa comunitario multianual “Safer Internet Plus”, cuyo objetivo es promover el uso de la Internet y las nuevas tecnologías en línea en condiciones de mayor seguridad. Entre las tareas principales del programa figura la educación de la sociedad sobre el aumento de la seguridad en el uso de la Internet y los servicios telefónicos de emergencia.

5. Durante la Asamblea General de la International Association of Internet Hotlines (INHOPE), celebrada en Dublín del 28 al 29 de mayo de 2008, el servicio telefónico de emergencia de Lituania pasó a formar parte de dicha asociación.

6. A nivel nacional, en 2000 se realizó la primera evaluación del estado de la infraestructura de la información, con lo que se puso en marcha un proceso de participación amplia en la solución de los problemas propios en esa esfera. Entre los principales ámbitos de evaluación figuraron el nivel de comprensión de la cuestión de la seguridad de la información, las políticas en vigor y el nivel de protección cibernética de las instituciones del Estado.

7. De conformidad con la resolución núm. 291 del Gobierno de la República de Lituania, de 14 de marzo de 2001, se asignó al Ministerio del Interior la tarea de coordinar las actividades relacionadas con las tecnologías de la información en las instituciones del Estado.

8. Se han elaborado y puesto en práctica una serie de medidas con el objetivo de salvaguardar la seguridad de la información, como quedó plasmado en la estrategia nacional de protección de las tecnologías de la información hasta 2004 y la estrategia nacional sobre la seguridad de la información electrónica de los organismos del Estado hasta 2008.

9. El 17 de junio de 2008, por decreto del Primer Ministro de Lituania, se estableció el grupo de trabajo interinstitucional sobre la seguridad cibernética. El 21 de noviembre de 2008, el grupo de trabajo presentó un informe al Gobierno, en que se formulaban propuestas y recomendaciones para aumentar la seguridad cibernética en Lituania.

10. El Gobierno de Lituania tiene previsto elaborar próximamente un proyecto de ley sobre las redes electrónicas de comunicación y la seguridad de la información y una nueva estrategia nacional sobre la seguridad de la información electrónica, con el objetivo de fortalecer la capacidad del Estado en el ámbito de la seguridad de la información y, en particular, la defensa cibernética. Entre los objetivos de dicha estrategia figuran aumentar la eficiencia de la estructura institucional como marco para protegerse contra ataques cibernéticos; aumentar la seguridad y la resistencia de la infraestructura de la transmisión de datos; proteger de manera eficaz la infraestructura vital de la información contra ataques cibernéticos y asegurar un alto grado de cumplimiento de las políticas y los requisitos mediante la realización de auditorías externas por segundas y terceras partes.

11. Desde 2005, la Dirección de Comunicaciones de Lituania ha realizado estudios sobre las redes electrónicas de comunicación y la seguridad de la información con el objetivo de eliminar deficiencias pendientes. La Dirección de Comunicaciones ejerce las funciones de equipo nacional de respuesta ante emergencias informáticas.

12. El Equipo nacional de respuesta ante emergencias informáticas de Lituania tiene a su cargo promover la seguridad de la información por medio de la prevención, la vigilancia y la solución de problemas que representen una amenaza para la seguridad de la información, así como por medio de la difusión de información sobre esas amenazas. El 30 de septiembre de 2008 entró en funcionamiento el nuevo sitio web del Equipo (www.cert.lt). El 16 de enero de 2009, el Equipo nacional de respuesta ante emergencias informáticas de Lituania se convirtió en miembro acreditado de Trusted Introducer, la red fiduciaria de equipos de respuesta ante incidentes de seguridad informática y equipos de respuesta ante emergencias informáticas de Europa.

13. Lituania vela por que la comunidad internacional siga prestando gran atención a las cuestiones relacionadas con la seguridad de la información y redoblen los esfuerzos encaminados a solucionar los problemas en ese ámbito. Lituania se propone participar activamente en la labor futura de la comunidad internacional por aumentar la seguridad de la información.

México

[Original: español]
[8 de junio de 2009]

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

2. En este contexto, y preocupado por el desarrollo de la seguridad en las telecomunicaciones en el mundo, México participó en la “Asamblea Mundial de Normalización de las Telecomunicaciones” celebrada en Sudáfrica en octubre de 2008, durante la cual presentó junto con otros miembros de la Comisión Interamericana de Telecomunicaciones (CITEL) (Canadá, Paraguay y Uruguay) una resolución para invitar a las universidades a participar activamente en las sesiones de la Unión Internacional de Telecomunicaciones (UIT) con el fin de reforzar su trabajo.

3. Igualmente, en el ámbito regional, México fungió como vicepresidente de la XX Reunión del Comité Directivo Permanente de la CITEL, durante la cual ofreció a los Estados de la región un curso sobre “Interferencias perjudiciales a los sistemas satelitales” a través de la Comisión Federal de Telecomunicaciones. En tal ocasión, los Estados acordaron realizar la V Asamblea Ordinaria de la CITEL en el primer trimestre de 2010 en México.

4. Entre las actividades que México realiza para fortalecer la seguridad internacional en el ámbito de la información y las comunicaciones, puede destacarse que México cuenta con la “Unidad de Policía Cibernética” que, además de las acciones preventivas que realiza en materia de delitos cometidos a través de Internet y otros medios informáticos, cuenta con un área específica para la prevención y atención de denuncias de delitos contra menores.

Serbia

[Original: inglés]
[9 de junio de 2009]

1. Es necesario que los Estados consoliden sus normas jurídicas relativas al espacio cibernético, ya que éste no se limita al territorio de ningún país y a menudo las personas o grupos involucrados en la desestabilización o el uso no autorizado de los sistemas de información y telecomunicaciones no se encuentran en el país en que ocurre un accidente. La resolución 63/37 de la Asamblea General es un primer paso hacia el establecimiento de un enfoque equilibrado, basado en recomendaciones, de la consolidación de las legislaciones a nivel internacional con el objetivo de fortalecer la seguridad internacional, por un lado, y asegurar la libre circulación de la información, por el otro, a la vez que proporciona una base sólida para la aplicación de dicho enfoque.

2. Se necesitan leyes más estrictas, en primer lugar a nivel nacional, que se ajusten a los conocimientos técnicos y el nivel de educación de los usuarios y estén respaldadas por la educación permanente de los usuarios y el establecimiento de organismos especializados encargados de planificar, organizar y supervisar las cuestiones técnicas en este ámbito.

3. Al examinar la aplicación del principio de la seguridad de la información en el marco de los sistemas de información y telecomunicaciones, se ha establecido lo siguiente:

Problemas

- A diario aparecen nuevos tipos de programas malignos que amenazan la seguridad de los sistemas de información y telecomunicaciones
- Son numerosos los intentos de atacar los sitios web oficiales del Ministerio de Defensa y las Fuerzas Armadas de la República de Serbia
- Se utiliza la Internet para hacer propaganda en favor del terrorismo

Procedimientos de seguridad y cooperación

- Aplicación de programas antivirus adecuados a todos los niveles de los sistemas de información y telecomunicaciones del Ministerio de Defensa y las Fuerzas Armadas de la República de Serbia
- Protección permanente de los sitios web oficiales del Ministerio de Defensa y las Fuerzas Armadas de la República de Serbia contra ataques piratas cibernéticos
- Participación en conferencias y seminarios dirigidos a aumentar la conciencia sobre el peligro de la delincuencia y el terrorismo cibernéticos

Recomendaciones

Establecer un organismo internacional encargado de:

– Examinar los problemas existentes en materia de protección de los sistemas de transmisión de datos y telecomunicaciones

– Vigilar los factores de “amenaza” en materia de delincuencia y terrorismo cibernéticos

– Examinar los problemas relativos a la seguridad internacional en el ámbito de los sistemas de información y telecomunicaciones y recomendar soluciones

– Diseñar programas de educación dirigidos a aumentar la conciencia sobre el peligro de la delincuencia y el terrorismo cibernéticos

– Organizar intercambios de conocimientos y experiencias a nivel intergubernamental

Tailandia

[Original: inglés]
[3 de junio de 2009]

Examen general de las cuestiones relacionadas con la seguridad de la información

1. La humanidad ha entrado en la era de la sociedad de la información, en la que la tecnología de la información se utiliza para facilitar la vida diaria; por ejemplo, en las transacciones financieras y el intercambio de noticias e información. No obstante, la tecnología de la información no sólo proporciona beneficios, sino que también crea oportunidades para su uso ilícito e inmoral por parte de determinados grupos, lo que da lugar a problemas como el robo de información mediante el uso del propio sistema de información, los ataques cibernéticos, la falsificación de documentos electrónicos, la infiltración en las bases de datos de los gobiernos con el propósito de robar datos personales y la violación de la privacidad. Pese a ello, la tecnología de la información y las comunicaciones es necesaria para el desarrollo económico de cada país. La complejidad cada vez mayor de la tecnología, la escasez de personal con una buena formación en la seguridad de la información y la falta de recursos suficientes pueden hacer que disminuya la seguridad de la información de los sistemas y redes digitales, lo que a su vez menoscabaría la confianza de los usuarios, especialmente en esferas como la banca, el comercio electrónico y la administración. Por tanto, es necesario detectar y pronosticar los problemas concomitantes para establecer salvaguardias y adoptar medidas de seguridad contra esos riesgos. A tal fin, los países deberían cooperar entre sí para adoptar medidas de seguridad de la información y establecer normas internacionales a las que se atengan todos los países.

Medidas adoptadas a nivel nacional con el fin de fortalecer la seguridad de la información y promover la cooperación internacional en esa esfera

2. La política de seguridad nacional del Gobierno Real de Tailandia es uno de los ámbitos normativos prioritarios de su plan estratégico para los años 2009-2011 (2552-2554, según el calendario tailandés). Actualmente, el Gobierno adopta medidas para promover la seguridad de la información y, por ese medio, prevenir el uso de las redes digitales con fines inmorales e impedir que se ponga en peligro la seguridad nacional. Entre esas medidas figura la promulgación de leyes sobre delitos cibernéticos, transacciones electrónicas, firmas electrónicas y transferencias electrónicas de dinero.

3. El Ministerio de Tecnología de la Información y las Comunicaciones atribuye una gran importancia a la necesidad de velar por la seguridad de la información en las redes digitales y solventar las cuestiones relativas a los sitios web inapropiados e ilegales, para lo que se ha creado un centro de operaciones para la seguridad de la Internet, con el propósito de mantener bajo vigilancia las amenazas contra la tecnología de la información, así como coordinar con otros organismos la adopción de medidas sobre el uso de las redes de información contra la seguridad nacional. El centro persigue, además, el objetivo de poner fin al uso ilícito de las redes de información y establecer un sistema de vigilancia contra virus y el envío masivo de mensajes electrónicos no solicitados.

4. En lo que respecta a la cooperación internacional, debería establecerse un órgano que sirva de centro de coordinación. Dicho órgano debería formular políticas dirigidas a prevenir y combatir la difusión de información inapropiada, así como adoptar medidas para hacer frente a las amenazas contra la seguridad de la información y medidas preventivas que sirvan de directrices para la realización de actividades conjuntas.

Examen de los criterios internacionales pertinentes sobre el fortalecimiento de la seguridad de los sistemas de información y telecomunicaciones a nivel mundial

5. Habida cuenta de que el universo cibernético contemporáneo es un espacio cuyos elementos están interconectados y que no conoce fronteras, se necesitan criterios y principios internacionales comunes para promover la seguridad de la información a nivel mundial. Consiguientemente, los problemas que surjan en cualquier país en materia de seguridad de la información pueden propagarse y afectar a otros países.

Medidas que podría adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial

6. Entre las medidas que la comunidad internacional podría adoptar figuran el intercambio de información, el intercambio de medidas preventivas y el intercambio de medidas para combatir las amenazas contra la seguridad de la información. También debería aumentar la cooperación para la creación de capacidades similares en los países en materia de tecnología de la información, especialmente en lo que atañe a la transferencia de tecnologías y conocimientos especializados de países desarrollados a países menos adelantados para ayudar a fomentar la capacidad de estos últimos. Además, deberían elaborarse programas de capacitación sobre cuestiones relacionadas con la prevención, la detección y la gestión de riesgos y amenazas contra la seguridad de la información, la respuesta a los mismos y la sensibilización respecto de esos problemas.

7. Por otro lado, es necesario crear un mecanismo de coordinación de las actividades de los diversos organismos que se ocupan de trazar las líneas directrices y formular las políticas en relación con la seguridad de la información en cada país, de modo que esas actividades se ajusten a las mismas normas y se desarrollen en la misma dirección.

8. Deberían alentarse los esfuerzos de algunos organismos internacionales para promover la cooperación internacional en favor del fortalecimiento de la seguridad de la información, en particular la Unión Internacional de Telecomunicaciones

(UIT). Ésta organizó una conferencia internacional con el fin de intercambiar experiencias y examinar medidas para dar solución a los problemas derivados del mal uso de la tecnología de la información. Se han creado, además, grupos de estudio encargados de elaborar medidas para fortalecer la seguridad de la información, cuyos resultados puedan ser aplicados y aprovechados por los gobiernos y organismos interesados.

9. Asimismo, en todos los países deberían establecerse equipos de respuesta ante emergencias informáticas con la ayuda de los países que hayan tenido éxito en el establecimiento de esos equipos.

10. Debería abordarse la protección de la infraestructura vital de cada país contra ataques cibernéticos, así como la prestación rápida de asistencia o cooperación en la comunidad internacional, y debería examinarse conjuntamente la adopción de medidas para eliminar o reducir al mínimo esos riesgos.

11. Debería alentarse la realización de actividades de concienciación sobre la seguridad de la información de las Naciones Unidas y, tal vez, examinarse la posibilidad de adoptar normas y reglamentos en materia de guerra informática, además de presentarse informes anuales sobre amenazas y vulnerabilidades en la esfera de la seguridad de la información.

Tayikistán

[Original: inglés]
[20 de mayo de 2009]

1. Actualmente se considera que las telecomunicaciones son un factor muy importante para el desarrollo de la economía, así como para la estabilidad y la seguridad de cualquier Estado.

2. En Tayikistán se han creado las condiciones necesarias para el desarrollo de las telecomunicaciones por medio de la libre competencia y la concesión de licencias a operadores y proveedores de servicios alternativos y la creación de nuevos servicios.

3. Es esencial que se atienda a la necesidad de velar por la seguridad del funcionamiento de la infraestructura de la información y las telecomunicaciones, aumentar el grado de protección de los sistemas de información de las empresas y, por esa vía, contrarrestar la propagación de la ideología del terrorismo, el extremismo y la violencia.

4. Tayikistán está listo para respaldar estas iniciativas y prestar su cooperación al desarrollo de la sociedad internacional de la información.

Ucrania

[Original: ruso]
[20 de mayo de 2009]

1. El interés que despiertan las cuestiones relativas a la seguridad de la información constituye un reflejo de la función cada vez más importante que desempeña la información en las diversas esferas de la vida social. Con la aplicación de las tecnologías de la información en las actividades diarias del Estado y la sociedad, aumenta la posibilidad de que los sistemas de información y telecomunicaciones y los servicios de información de los organismos del Estado y las entidades comerciales se vean amenazados por grupos y personas involucrados en actividades delictivas por medios digitales.

2. La mitad de los delitos cibernéticos registrados a nivel mundial guardan relación con el acceso no autorizado a la información digital. Aumenta la tendencia a la comisión de delitos informáticos con fines de lucro, que causan daños materiales cada vez mayores. Ha aumentado el número de delitos cometidos por agrupaciones transnacionales involucradas en la realización de ataques cibernéticos.

3. La delincuencia cibernética se caracteriza por su alto grado de latencia, lo que impide formarse una idea completa de las infracciones cometidas, ya que tanto las entidades estatales como las empresas privadas que son objeto de ataques cibernéticos tratan por todos los medios de ocultar tales incidentes, por temor a ver dañada su autoridad, no se muestran inclinadas a divulgar los daños sufridos y poseen un sistema inadecuado de protección de la información. Como resultado, no siempre se divulgan esos incidentes delictivos, lo que plantea la necesidad de adoptar medidas fundamentales para el sistema de protección de la información, dirigidas a prevenir e impedir la comisión de tales actos.

4. Por regla general, los delitos cibernéticos son solo el primer paso en una cadena de actos delictivos tradicionales, como el robo, el soborno, el fraude y otros. Estos delitos son cada vez más elaborados, refinados y difíciles de detectar y ocasionan daños enormes en el plano económico y político en casi todos los países del mundo. Además, la mayoría de los expertos establecen un vínculo directo entre la soberanía informática de los Estados y la seguridad nacional.

5. En la lucha contra los delitos en la esfera de las tecnologías de la información surgen numerosos problemas jurídicos derivados del carácter inmaterial y, a menudo, la fugacidad de las pruebas incriminatorias electrónicas. La complejidad de la solución de los problemas relacionados con la delincuencia cibernética exige con particular urgencia que se fomente la cooperación internacional, por lo que, en última instancia, todos los países deberían disponer de instrumentos jurídicos, procesales y normativos pertinentes y comunes.

6. La práctica de la investigación de los delitos cibernéticos plantea la necesidad de que los órganos encargados de hacer cumplir la ley de diferentes Estados cooperen entre sí.

7. A nivel mundial existen antecedentes de actividades conjuntas en materia de investigación de delitos cibernéticos. Los servicios de seguridad de Ucrania participan activamente en operaciones conjuntas con los órganos encargados de hacer cumplir la ley y los servicios especiales de otros Estados, realizadas en el

marco de la lucha contra la pornografía infantil, las actividades fraudulentas en la Internet y el terrorismo internacional.

8. Es necesario, además, aunar esfuerzos para fomentar la cooperación en favor del fortalecimiento de la seguridad cibernética, la creación de intereses comunes y la adopción de medidas para protegerlos, principalmente mediante acuerdos bilaterales y multilaterales. A nuestro juicio, los problemas relativos a la seguridad informática podrán solucionarse a condición de que los órganos pertinentes de los diferentes Estados cooperen de manera eficaz, sobre todo si se tiene en cuenta que ya existe la base jurídica común necesaria.

9. Ante la necesidad de contrarrestar las amenazas de la delincuencia cibernética y el terrorismo cibernético, el Servicio de Seguridad de Ucrania mantiene contactos con los órganos encargados de hacer cumplir la ley y los servicios especiales de otros Estados.

10. Cabe señalar que con frecuencia los ataques orquestados por delincuentes cibernéticos van dirigidos contra las redes de los organismos del Estado y que, en las circunstancias actuales, el éxito de las operaciones de captura y enjuiciamiento de los delincuentes depende tanto del establecimiento de vínculos internacionales eficaces como de la optimización de las leyes nacionales.

11. A finales de 2008, en colaboración con la Policía Nacional del Reino de los Países Bajos y el Servicio Federal de Seguridad de la Federación de Rusia, se llevó a cabo una operación coordinada para poner fin a las actividades ilícitas de una agrupación internacional involucrada en actos de piratería cibernética, que se dedicaba a robar fondos de clientes de instituciones financieras y de crédito mediante el acceso no autorizado a los sistemas automatizados de dichas entidades.

12. Teniendo en cuenta el constante aumento de la delincuencia cibernética a nivel mundial, la existencia de vínculos entre las agrupaciones delictivas dedicadas a la piratería cibernética de diferentes países y el carácter transnacional de las amenazas cibernéticas, es necesario fortalecer la cooperación internacional en el accionar contra esas amenazas.

13. A tal fin, de conformidad con la Convención Internacional sobre la Delincuencia Cibernética, se estableció la red de puntos nacionales de contacto “24/7”, mecanismo viable y conveniente que une a los países del Grupo de los Ocho y otros Estados partes en la Convención.

14. De conformidad con la decisión del Presidente de Ucrania sobre el establecimiento del punto nacional de contacto de la red “24/7”, subordinado al Servicio de Seguridad de Ucrania, actualmente un grupo de trabajo interministerial integrado por funcionarios del Servicio de Seguridad, el Ministerio del Interior, la Fiscalía General y el Ministerio de Justicia de Ucrania está enfrascado en la elaboración de proyectos de ley sobre la introducción de enmiendas en la ley sobre la ratificación de la Convención Internacional sobre la Delincuencia Cibernética; la ley sobre la introducción de enmiendas en la ley de telecomunicaciones, y la ley sobre la estructura y el personal del Servicio de Seguridad de Ucrania, así como del proyecto de Decreto del Presidente de Ucrania sobre la organización de la labor del referido punto de contacto.

15. En cumplimiento de la decisión del Presidente de Ucrania sobre el Servicio de Seguridad de Ucrania, actualmente se trabaja en la inscripción del punto nacional de contacto en la red internacional.

16. Se prevé que, como resultado de la labor del referido punto nacional de contacto, se podrán llevar a cabo con mayor rapidez y calidad las actividades pertinentes de intercambio de información y lucha contra las amenazas cibernéticas a nivel internacional.

17. En cumplimiento de las decisiones de la Cumbre Mundial de la Sociedad de la Información, celebrada en Ginebra, del 10 al 12 de diciembre de 2003 (primera etapa) y Túnez, del 16 al 18 de noviembre de 2005 (segunda etapa), se aprobó la Ley sobre los principios fundamentales del desarrollo de la sociedad de la información en Ucrania para 2007-2015, entre cuyas prioridades figura la integración de Ucrania en el espacio cibernético mundial y el desarrollo de la sociedad de la información en ese país. En dicha Ley se prevé el aumento de la seguridad de la información en el marco de las tecnologías más avanzadas de la información y las comunicaciones.

18. Asimismo, se elaboró y aprobó un documento conceptual sobre el desarrollo de las telecomunicaciones en Ucrania, en que se prevé adoptar, entre otras, las siguientes medidas organizativas y técnicas para garantizar el funcionamiento seguro de todos los elementos de la infraestructura nacional de telecomunicaciones:

– Elaborar y aplicar de manera gradual una base jurídico-normativa que garantice la protección técnica y criptográfica de la información y que esté armonizada con las normas europeas e internacionales;

– Elaborar métodos modernos de protección de la información con la ayuda de medios técnicos para la solución integral de los problemas relativos a la protección de la información en las redes de telecomunicaciones;

– Crear un sistema para la interceptación legal de información en las redes de telecomunicaciones en los casos previstos por la ley;

– Crear un centro nacional de coordinación de las actividades relacionadas con la seguridad de las redes públicas de información y telecomunicaciones y fomentar el establecimiento de centros estatales y no gubernamentales de atribución de jurisdicción y respuesta en relación con incidentes en las redes de telecomunicaciones.

19. Conforman igualmente la base jurídico-normativa de la protección de la información en Ucrania, entre otros instrumentos legislativos, la ley sobre los principios de la seguridad nacional de Ucrania; la ley sobre la información; la ley sobre la protección de la información en los sistemas de información y telecomunicaciones; los actos legislativos del Presidente y el Consejo de Ministros de Ucrania sobre la protección técnica de la información en Ucrania; el reglamento para la protección de la información en los sistemas de información, telecomunicaciones e información y telecomunicaciones; el procedimiento para conectarse con las redes mundiales de transmisión de datos, así como un número considerable de instrumentos normativos depositados en el Ministerio de Justicia que reglamentan la conexión de los sistemas nacionales de información con las redes mundiales, la concesión de licencias para la realización de diversos tipos de actividades y la evaluación de los productos en la esfera de la protección de la información, entre otras cuestiones.

20. En dichos instrumentos jurídicos y normativos se estipula que en el procesamiento de la información sujeta a protección deberán utilizarse solamente sistemas protegidos de información y telecomunicaciones, es decir, sistemas que comprendan un subsistema integral de protección de la información constituido por un conjunto de actividades jurídicas y organizativas, así como por medios técnicos e informáticos capaces de contrarrestar cualquier amenaza. Para ello, deberá verificarse que el subsistema integral de protección de la información y los medios de protección a su alcance cumplan con los requisitos fijados en los documentos normativos vigentes en materia de protección de la información.

21. Con el objetivo de reglamentar los requisitos con los que deben cumplir los sistemas integrales de protección de la información y los diversos medios de protección de la información en Ucrania, se han elaborado y promulgado cerca de 50 instrumentos normativos de carácter técnico en los que se definen los criterios de protección de la información, se clasifican los sistemas de información y telecomunicaciones, se establecen los procedimientos para la realización de las actividades de protección y se fijan los requisitos con que deben cumplir los diferentes medios de protección de la información y los sistemas integrales de protección de la información, atendiendo al tipo de sistema de información y telecomunicaciones y la función, la esfera de aplicación y el tipo de información procesada.

22. Ucrania posee, además, un sistema nacional propio de criterios de evaluación de la protección de las tecnologías de la información. Este sistema se basa en un conjunto de documentos normativos sobre la protección contra el acceso no autorizado a la información de los sistemas de información y telecomunicaciones, que han sido armonizados con documentos análogos de los países de la Unión Europea y las normas internacionales vigentes, en particular la norma ISO 15408 de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

23. Por otro lado, se está creando en Ucrania un sistema nacional de medidas organizativas y técnicas que tienen por objetivo prevenir la realización de actividades ilícitas en relación con los sistemas de información y telecomunicaciones de los órganos del poder del Estado; los órganos encargados de hacer cumplir la ley, los organismos aduaneros y tributarios y las instituciones financieras y de crédito, entre otros, en particular la interferencia en su labor valiéndose de las posibilidades que ofrece la red mundial de la Internet.

24. En respuesta a esas actividades ilícitas, la comunidad internacional ha establecido equipos de respuesta ante emergencias informáticas, que constituyen un sistema complejo y amplio de mecanismos de respuesta rápida ante incidentes que pongan en peligro la seguridad de los servicios de información. El Foro de equipos de respuesta de emergencia y seguridad (FIRST) es la organización internacional encargada de coordinar las actividades de esos equipos a nivel internacional.

25. A fin de sentar las bases jurídico-normativas de esas actividades, la Dirección del Servicio Estatal de Sistemas Especializados de Comunicación emitió la Orden No. 94, de 10 de junio de 2008, sobre la aprobación de las modalidades de coordinación de las actividades de los órganos del poder del Estado, los órganos locales de gobierno, las fuerzas armadas y las empresas, instituciones y organizaciones públicas o privadas en materia de prevención, identificación y eliminación de las consecuencias de actividades no autorizadas en relación con los servicios de información del Estado en uso en los sistemas de información, telecomunicaciones e información y telecomunicaciones.

26. En cumplimiento de dicho decreto, se creó el sitio web correspondiente (www.cert.gov.ua).

27. Sobre la base de la experiencia acumulada a nivel internacional en materia de protección de los servicios de información, se están adoptando en Ucrania medidas dirigidas a establecer un centro nacional subordinado al Servicio Estatal de Sistemas Especializados de Comunicación que se ocupe de coordinar las actividades para prevenir la realización de actos violatorios de la seguridad de la información en los sistemas de información y telecomunicaciones del Equipo de respuesta ante emergencias informáticas de Ucrania CERT-Ucrania (CERT-UA) y acreditar dicho centro ante el Foro de equipos de respuesta de emergencia y seguridad. A tal fin, el 17 de marzo de 2009 se organizó y celebró una reunión entre representantes de la Dirección del Servicio Estatal de Sistemas Especializados de Comunicación y el asesor superior para asuntos de seguridad informática de la Dirección de Comunicaciones de Finlandia.

28. Pese a que el Equipo de respuesta ante emergencias informáticas de Ucrania no ha sido todavía acreditado ante el Foro de equipos de respuesta de emergencia y seguridad, entre 2006 y 2008 el equipo ucraniano recibió más de 200 comunicaciones de los equipos de Finlandia, Australia, Austria, Eslovenia y otros Estados sobre actividades no autorizadas en la red mundial de la Internet por parte de usuarios ucranianos. Como resultado de las medidas adoptadas, se enviaron más de 250 mensajes electrónicos a los correspondientes proveedores de servicios de Internet con el objetivo de localizar las fuentes de programas malignos y virus. Por otro lado, en mayo de 2007 se adoptaron medidas para poner fin a la realización de ataques DDoS contra servidores de Estonia, cuya fuente se localizó en Ucrania, mientras que en octubre de 2007 se neutralizó un ataque DDoS contra el sitio web del Presidente de Ucrania.

29. Se debe añadir que en Ucrania se han sentado las bases jurídico-normativas y adoptado las medidas organizativas necesarias para fomentar la cooperación entre la Dirección del Servicio Estatal de Sistemas Especializados de Comunicación y los órganos encargados de hacer cumplir la ley, a fin de velar por la seguridad de los servicios de información del Estado en los sistemas de información y telecomunicaciones y aumentar la eficacia del sistema de respuesta ante incidentes de uso no autorizado de dichos servicios de información.

30. Así pues, existen en Ucrania las condiciones necesarias para garantizar la protección de la información en todas las fases del establecimiento de los sistemas de información y telecomunicaciones y sus respectivos sistemas integrales de protección de la información, independientemente del tipo y la importancia de la información de que se trate o del tipo y la complejidad del sistema de información y telecomunicaciones correspondiente. Por lo tanto, los criterios fundamentales que se aplican para establecer requisitos, proyectar, elaborar, evaluar el grado de protección y asegurar la protección de los servicios de información en los sistemas de información y telecomunicaciones se ajustan en general a los criterios que aplican los órganos competentes de los Estados Miembros de las Naciones Unidas y la Unión Europea encargados de velar por la seguridad de la información.

31. Con el objetivo de realizar las actividades correspondientes de formación de especialistas en la esfera de la seguridad de la información y la ingeniería informática, se creó el Instituto de Protección de la Información, dependencia docente y científica de la Universidad Estatal de Tecnologías de la Información y las Comunicaciones.