Naciones Unidas A/65/154

Asamblea General

Distr. general
20 de julio de 2010
Español
Original: español/inglés/ruso

Sexagésimo quinto período de sesiones
Tema 94 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/65/150.

10-45845 (S) 160810 160810

I. Introducción

1. En el párrafo 3 de su resolución 64/25, 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 adoptaban 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 *supra*;

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

2. En atención a esa solicitud, el 26 de febrero de 2010, se envió una nota verbal a todos los Estados Miembros invitándolos a proporcionar información sobre el tema. Las respuestas recibidas figuran en la sección II *infra*. Las respuestas que se reciban con posterioridad se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los Gobiernos

Cuba

[Original: español]
[27 de mayo de 2010]

1. Cuba comparte plenamente la preocupación que se expresa en el texto de la resolución 64/25 con respecto al empleo de las tecnologías y medios de información con propósitos incompatibles con la estabilidad y la seguridad internacionales, que afecten negativamente la integridad de los Estados, en detrimento de su seguridad en las esferas civil y militar. Igualmente, esta resolución enfatiza de manera adecuada en la necesidad de impedir la utilización de los recursos y las tecnologías de la información con fines delictivos o terroristas.

2. Cuba reitera que el uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia y una manifestación negativa e irresponsable del empleo de esos medios, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales, y socavar así los principios y propósitos consagrados en la Carta de las Naciones Unidas.

3. Cuba llama la atención, con preocupación, sobre el hecho de que los sistemas de información y telecomunicaciones pueden convertirse en armas cuando se diseñan y/o emplean para causar daños a la infraestructura de un Estado y, como consecuencia, pueden poner en riesgo la seguridad y la paz internacionales.

4. En este contexto, procede reiterar la condena ya presentada por parte de la República de Cuba, en diferentes foros internacionales, a la escalada agresiva de las

sucesivas administraciones estadounidenses en su guerra radial y televisiva contra Cuba, en franca violación de las normativas internacionales vigentes en materia de regulación del espectro radioeléctrico.

5. El Gobierno de los Estados Unidos no ha reparado en el daño que pudieran causar a la paz y seguridad internacionales creando situaciones de peligro, como el uso de un avión militar para transmitir señales de televisión hacia Cuba, sin su consentimiento.

6. La agresión radioeléctrica contra Cuba desde territorio norteamericano infringe los principios del derecho internacional que rigen las relaciones entre los Estados y las normas y reglamentos de la Unión Internacional de Telecomunicaciones (UIT), que establecen la conducta a seguir por los países miembros de dicha agencia especializada del sistema de las Naciones Unidas.

7. Cada semana, emisoras radicadas en el territorio de los Estados Unidos transmiten hacia Cuba miles de horas de radio y televisión por 34 diferentes frecuencias de onda media, corta, FM y TV. En el mes de marzo de 2010, se alcanzaron 2.156 horas de transmisiones ilegales semanalmente. Varias de estas emisoras pertenecen o prestan sus servicios a organizaciones vinculadas con conocidos elementos terroristas que residen y actúan contra Cuba en territorio norteamericano, con pleno consentimiento de las autoridades de los Estados Unidos de América.

8. Las transmisiones ilegales de radio y televisión contra Cuba no emiten información; por el contrario, la falsifican y tergiversan con fines subversivos. Para este tipo de acciones, el Congreso de los Estados Unidos de América aprueba anualmente un presupuesto de más de 30 millones de dólares de fondos federales. Desde que se crearon ambas emisoras, el Gobierno estadounidense ha gastado 659,8 millones de dólares con este propósito.

9. Estas transmisiones provocadoras contra Cuba constituyen violaciones de los siguientes preceptos internacionales:

– Principios fundamentales de la Unión Internacional de Telecomunicaciones, expresados en el Preámbulo de su Constitución, sobre la importancia creciente de las telecomunicaciones para la salvaguardia de la paz y el desarrollo económico y social de todos los Estados, con el fin de facilitar las relaciones pacíficas, la cooperación internacional entre los pueblos y el desarrollo económico y social por medio del buen funcionamiento de las telecomunicaciones. El contenido de la programación televisiva que se transmite por el Gobierno de los Estados Unidos de América contra Cuba tiene un carácter subversivo, desestabilizador y engañoso, que entra en contradicción con estos principios.

– Disposiciones CS 197 y CS 198 de la Constitución de la Unión Internacional de Telecomunicaciones, que establecen que todas las estaciones, cualquiera que sea su objeto, deberán ser instaladas y explotadas de tal manera que no puedan causar interferencias perjudiciales a las comunicaciones o servicios radioeléctricos de otros Estados miembros.

– Acuerdo de la novena sesión plenaria de la Conferencia Mundial de Radiocomunicaciones (CMR), celebrada en noviembre de 2007, que estableció en el párrafo 6.1, inciso g) “que toda estación de radiodifusión que funcione a

bordo de una aeronave y transmita exclusivamente en el territorio de otra administración sin su consentimiento, no puede considerarse que funcione de conformidad con el Reglamento de Radiocomunicaciones".

– Artículo 8, numeral 8.3 del Reglamento de Radiocomunicaciones, que establece que las frecuencias asignadas e inscritas, con reconocimiento internacional, deberán ser tenidas en cuenta por las otras administraciones cuando efectúen sus propias asignaciones a fin de evitar una interferencia perjudicial.

– Artículo 42, numeral 42.4 del Reglamento de Radiocomunicaciones de la UIT, que prohíbe a las estaciones de aeronaves en el mar o por encima del mar efectuar servicio alguno de radiodifusión.

– Dictamen de la Junta del Reglamento de Radiocomunicaciones, que en su 35ª reunión en diciembre de 2004, estableció la interferencia perjudicial a los servicios cubanos que esas transmisiones causaban en los 213 MHz y reclamó a la administración de los Estados Unidos de América tomar las medidas pertinentes para su eliminación. Además, desde septiembre de 2006, la Junta del Reglamento de Radiocomunicaciones ha estado reclamando a la Administración de los Estados Unidos de América las medidas adoptadas para eliminar la interferencia en los 509 MHz, sin que haya dado respuesta hasta el momento. El 20 de marzo de 2009 la 50ª Reunión de la Junta en su Resumen de Decisiones (documento RRB09-1/5) reiteró, una vez más, le ilegalidad de las transmisiones y solicitó a la Administración de Estados Unidos de América que adoptara todas las medidas necesarias con miras a eliminar estos dos casos de interferencia a los servicios de televisión de Cuba. El 26 de marzo de 2010, la 53ª Reunión de la Junta del Reglamento de Radiocomunicaciones de la IUT reiteró su conclusión, de que las transmisiones de los Estados Unidos de América provocan interferencia perjudicial a las estaciones cubanas inscritas en el Registro Internacional de Frecuencias, e instó a la Administración de Estados Unidos a eliminar esta interferencia perjudicial, a la vez que encargó a la Oficina que supervisara la situación y actuara de conformidad a los procedimientos establecidos en el Reglamento de Radiocomunicaciones.

– Artículo 23, numeral 23.3 del Reglamento de Radiocomunicaciones de la UIT, que limita las transmisiones televisivas fuera de las fronteras nacionales.

10. Un informe emitido en enero de 2009, por la Oficina de Auditoría del Gobierno de los Estados Unidos de América (GAO) (instancia oficial estadounidense) reconoció las violaciones de las normas internacionales y la legislación interna en que incurre el programa de transmisiones radiales y televisivas del Gobierno estadounidense contra Cuba:

– Reflejó que la Unión Internacional de Telecomunicaciones determinó en 2004 y 2006 que las transmisiones televisivas en los canales 13 y 20 causan interferencia perjudicial a estaciones cubanas y el Departamento de Estado no ha emprendido acción alguna para responder a esta demanda de la UIT. El informe planteó, además, que la Conferencia Mundial de Radiocomunicaciones, celebrada en noviembre de 2007, dictaminó que las transmisiones desde un avión no estaban en conformidad con las regulaciones de la UIT.

– Reconoció que, a pesar de que las leyes estadounidenses prohíben la difusión interna de este tipo de transmisiones, tanto la radio como la televisión pueden

ser captadas en territorio de los Estados Unidos de América, principalmente en Miami, y que se ha detectado en las estaciones contratadas el uso de anuncios políticos pagados y publicidad de carácter sexual. Adicionalmente, señaló que las transmisiones contra Cuba no cumplen los estándares periodísticos de balance y objetividad, y se observa el uso de lenguaje incendiario y ofensivo.

11. Cuba recuerda, además, que la Conferencia Mundial de Radiocomunicaciones (CMR-07) que sesionó en Ginebra, Suiza, desde el 22 de octubre hasta el 16 de noviembre de 2007 aprobó un texto de conclusiones que califica de no conformes con el Reglamento de Radiocomunicaciones las transmisiones desde aeronaves desde los Estados Unidos hacia Cuba. Las conclusiones refrendadas por el plenario, establecieron textualmente que: "una estación de radiodifusión que funcione a bordo de una aeronave y transmita únicamente hacia el territorio de otra Administración sin su acuerdo, no puede considerarse que esté de conformidad con el Reglamento de Radiocomunicaciones".

12. Estas conclusiones fueron acordadas a nivel del plenario de la CMR-07 y tienen valor legal para el trabajo de la UIT. De esta forma, la Conferencia Mundial de Radiocomunicaciones refrendó el pronunciamiento realizado en 1990 por la entonces Junta Internacional de Registro de Frecuencia, según el cual la transmisión de televisión a bordo de un aerostato con programación dirigida hacia territorio nacional cubano contraviene la regulación del Reglamento.

13. La hostilidad del Gobierno de los Estados Unidos de América contra Cuba se ha puesto de manifiesto a través del bloqueo económico, comercial y financiero impuesto por más de 50 años, que afecta también la esfera de la información y las telecomunicaciones:

– Cuba no tiene derecho a acceder a los servicios que ofrece un gran número de sitios en la web, negación que se produce al reconocerse que el enlace se establece desde una dirección de Internet (IP) otorgada al dominio cubano .cu.

– Sin previa notificación se han bloqueado dominios .com relacionados con Cuba, lo cual se ha ejecutado por la Oficina de Control de Bienes Extranjeros.

– Cuba no puede, por las leyes del bloqueo económico, comercial y financiero que le aplica el Gobierno de los Estados Unidos de América, conectarse a los cables de fibra óptica que rodean el archipiélago cubano, obligando al país a pagar los servicios de satélites con restricciones por disponibilidad de ancho de banda, graves obstáculos para la adquisición de las tecnologías necesarias y elevados costos de conexión.

– Se utiliza Internet para aplicar campañas difamatorias contra Cuba, con fines subversivos y para desacreditar al país.

14. Esa actitud erosiona el espíritu, la voluntad y los resultados que prevalecieron entre las naciones de todo el mundo cuando se reunieron en Suiza y Túnez durante la celebración de la Cumbre Mundial de la Sociedad de la Información (CMSI), en los años 2003 y 2005.

15. Dicha Cumbre instó enérgicamente a los Estados a que, en la construcción de la Sociedad de la Información, tomasen las disposiciones necesarias para evitar, y abstenerse de adoptar, medidas unilaterales no conformes con el derecho internacional y con la Carta de las Naciones Unidas, que impidan la plena

consecución del desarrollo económico y social de la población de los países afectados, y que menoscaben el bienestar de sus ciudadanos.

16. La discusión en la Asamblea General de las Naciones Unidas sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional es muy pertinente, y cada día incrementa su actualidad e importancia. Actuaciones como las detalladas anteriormente de los Estados Unidos de América contra Cuba confirman la necesidad de ese debate, y la urgencia de adoptar medidas para poner fin a tales manifestaciones.

17. Cuba apoya resueltamente ese ejercicio en la Asamblea General de las Naciones Unidas y continuará aportando sus mayores esfuerzos para contribuir al desarrollo global pacífico de las tecnologías de la información y las telecomunicaciones y su empleo en bien de toda la humanidad. Está dispuesta, asimismo, a colaborar con el resto de los países, incluido los Estados Unidos de América, para encontrar soluciones que superen los obstáculos que impiden alcanzar esos objetivos.

Grecia

[Original: inglés]
[28 de junio de 2010]

1. Las cuestiones relativas a la seguridad de la información se abordan con mayor profundidad que antes. Se examinan las medidas para hacer frente a las amenazas modernas que son inherentes al advenimiento de la globalización de las redes y los sistemas. Se estudian medidas para preservar la libre circulación de información y se aplican en el contexto nacional y transfronterizo.

2. Se hace un seguimiento de los actuales conceptos internacionales y multinacionales. Se requiere orientación internacional en materia de evaluación de los riesgos. También debe abordarse la cuestión de la defensa cibernética. Deben mantenerse los derechos de soberanía nacional en relación con la seguridad informática en el contexto del intercambio mundial de información.

3. Se entiende que todos los Estados Miembros deben continuar transmitiendo al Secretario General sobre sus opiniones y evaluaciones en relación con las cuestiones pertinentes. A este respecto, se señalan las siguientes cuestiones:

a) Se atribuye suma importancia a todas las cuestiones relativas a la seguridad de la información en general.

b) Se estudian y aplican los medios para mantener la corriente de información y garantizar el grado necesario de confidencialidad, integridad y accesibilidad a nivel nacional y a través de las fronteras.

c) Se debe elaborar y acordar una base conceptual para la interconexión de redes que garantice que las capacidades se utilicen e intercambien a nivel nacional e internacional. Se debe velar por que se evalúen los riesgos para la interconexión de redes y asegurar el acceso a asesoramiento internacional pertinente. Además, dado que la necesidad de tomar medidas de defensa cibernética es motivo de gran preocupación para todos los países, se requiere una orientación internacional coherente a efectos de cooperación, eficiencia y economía. Por último, no se debe

pasar por alto la necesidad de que los países preserven su soberanía y mantengan su propia base de información, y esto debe tenerse en cuenta en todos los conceptos que se elaboren.

d) A continuación se enumeran las posibles medidas que debería adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial:

1) Elaborar en detalle los conceptos internacionales pertinentes y convenir en ellos;

2) Proponer un plan de orientación para crear una infraestructura general armonizada que abarque las cuestiones básicas en materia de legislación a fin de garantizar a un determinado número de usuarios certificados la seguridad de la información necesaria para la manipulación electrónica de toda la correspondencia y los mensajes, facilitando los diversos modos de comunicación;

3) Armonizar y ampliar conceptos que sirvan de guía a las alianzas multinacionales y pequeñas constelaciones de países a fin de que sean aplicables a nivel mundial. Llegar a un acuerdo en lo que respecta a determinar la amenaza y sus efectos negativos podría ser más importante que elaborar medidas complejas, ya que éstas últimas también podrían ser utilizadas por los adversarios;

4) Al mismo tiempo, la soberanía nacional debe servir de referencia básica en todo intento de globalización. Se debe elaborar un concepto internacional a fin de definir los portales nacionales para el intercambio de información con marcos hipotéticos que reflejen el nivel deseado de integración para todas las actividades a nivel nacional, internacional y multinacional.

México

[Original: español]
[18 de mayo de 2010]

Evaluación general de los problemas de la seguridad de la información

1. Las instituciones bancarias y financieras, así como las dependencias del gobierno federal que atienden temas de seguridad pública y seguridad nacional son las organizaciones en el país que realizan mayores esfuerzos en materia de seguridad informática. Se tiene una Unidad de Delitos Cibernéticos y una Policía Cibernética dentro de la Secretaría de Seguridad Pública Federal para entender ciberdelitos de seguridad pública.

2. Por otro lado, aunque existen esfuerzos aislados para el combate de los delitos cibernéticos en los tres órdenes de gobierno, no existe una política de seguridad cibernética del gobierno federal que guíe las estrategias del combate al cibercrimen en el país, la legislación en la materia requiere ser fortalecida, los jueces requieren contar con más instrumentos que les permitan atender y sancionar los ciberdelitos, la regulación para proveedores de servicios de Internet también requiere complementarse para que éstos mantengan el registro de actividad en su plataforma

y aporten información ante un posible incidente. Por otra parte, se requiere establecer acuerdos internos y crear convenios de cooperación con otros países para la atención del cibercrimen y el ciberterrorismo que atentan contra la seguridad nacional.

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

3. Existen esfuerzos en México para dar certidumbre en el marco de la seguridad de la información como los siguientes:

a) Regulación de algunos ciberdelitos en las siguientes leyes: Código Penal Federal, Código Penal del Distrito Federal, Código Federal de Procedimientos Penales, Ley de Protección de Datos de Colima, y Códigos Penales de los Estados de Aguascalientes, Sinaloa, Tabasco y Tamaulipas;

b) El 30 de abril de 2009 se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona la fracción XXIX-O del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, la cual establece la facultad del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares;

c) El 1 de junio de 2009 se publicó el decreto por el que se adiciona al artículo 16 de la Constitución un segundo párrafo, reconociendo que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros;

d) Se cuenta con el Equipo de Respuesta a Incidentes de Seguridad en cómputo de la Universidad Nacional Autónoma de México que atiende problemas de seguridad en el ámbito académico y brinda apoyo y asesoría técnica a las autoridades de gobierno en México para la atención de delitos cibernéticos;

e) Se tiene una Policía Cibernética dentro de la Policía Federal para dar seguimiento a las investigaciones sobre delitos de seguridad pública;

f) Se está generando dentro del Gobierno Federal un informe ejecutivo en materia de vulnerabilidad cibernética para informar a las altas autoridades del gobierno federal sobre los incidentes cibernéticos a nivel mundial con el fin de prever y apoyar iniciativas que contribuyan a fortalecer la ciberseguridad en México;

g) Se está planeando dentro del Gobierno Federal la creación de un CSIRT[1] nacional con el fin de coordinar los esfuerzos de atención de los ciberdelitos a nivel interno y externo;

h) La vulnerabilidad cibernética es un tema de la Agenda Nacional de Riesgos.

i) Se realizan programas de concientización del público en general, coordinadas por entidades públicas y privadas para prevenir los delitos cibernéticos.

[1] CSIRT Computer Security Incident Response Team.

j) Se asiste a diferentes foros y se establecen acuerdos de buena voluntad con otros países para la atención de ciberdelitos.

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

4. A continuación se enumeran las medidas para fortalecer la seguridad de la información a escala mundial:

a) Crear legislaciones adecuadas o actualizar las existentes en caso necesario para la protección de la información en el ciberespacio;

b) Capacitación a los jueces en temas de ciberseguridad con el fin de que puedan entender la naturaleza de los ciberdelitos y dar sentencias acordes a los mismos;

c) Creación de CSIRT nacionales para coordinar los esfuerzos de atención ante incidentes de seguridad mayores y para que sean los puntos de contacto con otros países;

d) Mantener una comunicación permanente entre CSIRT nacionales con el fin de coordinarse en caso de un incidente regional o mundial;

e) Realización de foros de intercambio de experiencias y de capacitación para los equipos de seguridad miembros de la comunidad internacional;

f) Realización de convenios internacionales de colaboración en contra de los ciberdelitos con el fin de agilizar las investigaciones y formar un frente común.

Panamá

[Original: español]
[21 de junio de 2010]

1. En la República de Panamá existen instituciones que combaten el uso indebido de Internet con fines delictivos, incluidos los actos terroristas. Para ello se cuenta con el Consejo de Seguridad Nacional y el Instituto de Medicina Legal y Ciencias Forenses-Departamento de Criminalística.

2. El Consejo de Seguridad Nacional realiza la labor de inteligencia en contra de actividades del crimen organizado, terrorismo entre otras, en caso de un posible ataque a los bienes e integridad del territorio nacional.

3. Por su parte, el Instituto de Medicina Legal y Ciencias Forenses cuenta con el Departamento de Criminalística que fue creado mediante la Ley 69 de 27 de diciembre de 2007, que realiza la labor investigativa sobre delitos cibernéticos.

4. Nuestro Código Penal tipifica, reprime y sanciona el uso de Internet para fines terroristas, cuando en su artículo 289 señala “Quien utilice Internet para enseñar a construir o reclutar personas para realizar actos con fines terroristas será sancionado con prisión de cinco a diez años”.

5. Igualmente, existen otras disposiciones legales que penalizan el uso de Internet para fines delictivos, y se sanciona penal, civil y administrativamente tales delitos según la ley 14 de 18 de mayo de 2007, capítulo VIII y Capítulo I “Delitos contra la

seguridad informática", la ley 51 de 22 de julio de 2008 que regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios y adoptan otras disposiciones para el desarrollo del comercio electrónico y la ley 38 de 8 de febrero de 1996 por la cual se dictan normas para la regulación de las telecomunicaciones en la República de Panamá.

Qatar

[Original: inglés]
[25 de mayo de 2010]

1. El Estado de Qatar está convencido de que la tecnología de la información y las comunicaciones deben utilizarse de conformidad con las disposiciones de la Carta de las Naciones Unidas y los principios básicos de las relaciones internacionales. Además, se debe garantizar la libre circulación de información sin perjuicio de la soberanía nacional y velando al mismo tiempo por la seguridad y el respeto de las diferencias culturales, políticas y morales que existen entre las naciones.

2. Las actividades que se llevan a cabo a nivel nacional están basadas en el interés en la seguridad de las comunicaciones y tienen por objeto mejorarla a fin de mantenerse al día con los últimos adelantos en esta esfera a nivel nacional e internacional.

3. A continuación se resumen las tareas que se plantean a nivel nacional:

- Elaborar estrategias y políticas de seguridad y promulgar leyes para limitar el uso de esas tecnologías para fines que no sean compatibles con los objetivos de la protección de la estabilidad de la seguridad
- Establecer un mecanismo para reforzar la seguridad de la información a fin de garantizar la protección de la infraestructura de la información confidencial en Qatar
- La Oficina de Seguridad de la Internet e Inteligencia se ocupa de vigilar las redes gubernamentales y la red nacional a fin de hacer frente a las amenazas que se plantean al Estado a través de la Internet
- Gestionar los incidentes de Internet y coordinar las medidas para hacerles frente a fin de garantizar la solución de los problemas relativos a la Internet después de notificarlos, con un tiempo mínimo de inactividad. En el Estado de Qatar, el Equipo de respuesta a emergencias informáticas de Qatar se encarga de estas tareas
- Cumplir una función más eficaz en materia de información y concienciación para elevar el nivel de conocimientos técnicos y cualificaciones del personal de las instituciones pertinentes de Qatar
- Prestar apoyo a los ciudadanos de Qatar en la solución de problemas relacionados con la Internet
- Mantenerse al día con los últimos adelantos en la esfera de las tecnologías modernas relacionadas con la seguridad y la protección de la Internet y velar por la evaluación de los productos técnicos, su seguridad y servicios conexos

– Promover las relaciones internacionales para hacer frente a los problemas relacionados con la Internet

4. A continuación se enumeran las medidas más importantes que la comunidad internacional puede tomar para promover la seguridad de la información a nivel nacional:

– Las Naciones Unidas deben continuar dirigiendo el debate y aclarar las cuestiones en relación con el uso de la información y la tecnología de la comunicación alámbrica e inalámbrica en la guerra electrónica y determinar si los principios de derecho internacional existentes son suficientes para asegurar un marco adecuado para definir el comportamiento apropiado en línea ante actos de agresión

– Establecer un comité especial internacional para la seguridad de la información transmitida por vía alámbrica e inalámbrica y llevar a cabo estudios amplios sobre este tema

– El Estado de Qatar alienta a todos los Estados Miembros a establecer equipos para hacer frente a emergencias informáticas a nivel nacional

– Concertar acuerdos con instituciones especializadas en materia de seguridad en la esfera de la comunicación

– Crear conciencia respecto de las cuestiones de seguridad mediante simposios y reuniones a nivel local e internacional

– Alentar a los Estados a cooperar a fin de combatir el espionaje y la piratería electrónica

– Utilizar equipos seguros y cifrados para transferir información y documentos de manera segura y garantizar su confidencialidad durante su transmisión

– Actualizar los sistemas de protección y organizar talleres periódicos para tomar conocimiento de los últimos adelantos científicos en la esfera de la seguridad de la información

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[2 de junio de 2010]

1. El Reino Unido de Gran Bretaña e Irlanda del Norte tiene el honor de responder a la resolución 64/25 de la Asamblea General, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.

2. Consideramos que este tema es sumamente importante, vital para algunas naciones, su comercio, la protección de sus ciudadanos y en el contexto más amplio de la seguridad internacional. El Reino Unido dedica considerables esfuerzos a hacer del espacio cibernético un ámbito más seguro para todas las naciones y acogemos con beneplácito las actividades internacionales en esta esfera, ya que creemos que todas las naciones deberían cooperar para promover un entorno seguro y resistente en el espacio cibernético. .

Apreciación general de las cuestiones relativas a la seguridad de la información

3. Creemos que un espacio cibernético seguro es vital en el mundo actual. Los ciudadanos, el comercio la infraestructura nacional de importancia crítica y el Gobierno dependen cada vez más de la Internet. Cualquier incidente que afecte adversamente el servicio de Internet en una nación puede tener consecuencias para esa nación, y éstas podrían ser graves. Es lamentable el hecho de que es muy probable que haya varios agentes que suponen una amenaza tanto externa como interna para cualquier nación, que puedan intentar interrumpir o manipular el servicio de Internet por diversos motivos.

Esfuerzos adoptados a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional sobre el terreno

4. El Reino Unido sigue trabajando a nivel nacional e internacional para promover un espacio cibernético más seguro. A nivel nacional, en junio de 2009 publicamos nuestra Estrategia Nacional de Seguridad Cibernética. Este documento sirve de base para las actividades que se realizan a nivel nacional en materia de seguridad de la información. En la Estrategia se solicitaba que se establecieran dos nuevas organizaciones, la Oficina de Seguridad Cibernética y el Centro de Operaciones de Seguridad Cibernética. Estas entidades ya se han creado y continúan creciendo. Existen tres equipos de respuesta a incidentes de seguridad informática administrados por el Gobierno del Reino Unido que prestan servicios especializados a la infraestructura nacional crítica, las fuerzas armadas y otras redes gubernamentales del Reino Unido. A nivel internacional, también realizamos una activa labor en este ámbito. Nuestra participación en el marco de las Naciones Unidas incluye la participación en el Grupo de Expertos Gubernamentales. El Reino Unidos ha sido copatrocinador de la resolución de la Asamblea General de las Naciones Unidas, titulada “Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales”. Somos miembros de los órganos competentes de la Unión Internacional de Telecomunicación (UIT) y participamos en las actividades de la Organización para la Seguridad y la Cooperación en Europa. Con nuestro pleno apoyo y participación, la Unión Europea ha empezado a trabajar en una serie de iniciativas para la protección de la infraestructura nacional crítica en la Unión Europea. Participamos en el compromiso de la Unión Europea con la labor del Foro Regional de la ASEAN en materia de seguridad cibernética. Asimismo, tomamos parte en varias actividades en el marco de la OTAN para proteger las redes de esa organización. El Reino Unido es desde hace tiempo un líder en el marco de MERIDIAN (www.meridian2007.org), FIRST (Forum on Incident Response and Security Teams, www.first.org) y European Government CERTs Group, www.egc-group.org).

5. La Estrategia Nacional de Seguridad Cibernética del Reino Unido puede descargarse de la página web de la Oficina del Gabinete en www.cabinetoffice.gov.uk.

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

6. Alentamos a todas las naciones a establecer sus propios equipos de respuesta a incidentes de seguridad informática. También las alentamos a promulgar leyes nacionales eficaces contra los delitos cibernéticos. Consideramos que si bien la delincuencia electrónica no es la única actividad nociva en el espacio cibernético, es la más difundida, y la reducción de las actividades delictivas en este ámbito beneficiaría a todos. Creemos que el Consejo de la Convención Europea sobre Delitos Cibernéticos representa un instrumento adecuado para luchar contra los delitos electrónicos a nivel internacional. Además, consideramos que el conjunto de instrumentos elaborado por la UIT y promovido en el marco de las Naciones Unidas constituye una base sólida para que las naciones lleven a cabo una autoevaluación de su disposición para hacer frente a los posibles ataques contra infraestructura nacional crítica. Acogemos con agrado los esfuerzos desplegados en diversos foros para promover las mejores prácticas en materia de seguridad de la información.

Conceptos internacionales pertinentes

7. El concepto internacional primordial es el de derecho internacional. Hay un debate importante, en particular en las conferencias sobre cuestiones cibernéticas, acerca de la aplicabilidad del derecho internacional existente al espacio cibernético. El Reino Unido ha examinado esta cuestión y nuestra opinión es que los principios de derecho internacional existentes tanto respecto del uso de la fuerza como del derecho sobre los conflictos armados, constituyen un marco adecuado para determinar y analizar el uso del espacio cibernético en el contexto de las hostilidades.

Ucrania

[Original: ruso]
[12 de mayo de 2010]

Logros en la esfera de la informatización y las telecomunicaciones en el contexto de la seguridad internacional

1. El interés en los problemas de la seguridad de la información está determinado por el papel creciente que desempeña la información en las distintas esferas de la vida de la sociedad. Con la introducción de tecnologías de la información avanzadas en las actividades cotidianas del Estado y la sociedad, aumentan las posibilidades 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 agrupaciones y personas involucradas en actividades delictivas por medios informáticos.

2. La mitad de los delitos informáticos registrados a nivel mundial están relacionados 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 secuestro, la extorsión, 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. 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.

12. 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.

13. 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 técnicas y de organización 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.

14. 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; y el procedimiento para conectarse con las redes mundiales de transmisión de datos, así como un gran número de instrumentos normativos depositados en el Ministerio de Justicia que reglamentan las cuestiones relativas a 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.

15. 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.

16. 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.

17. 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.

18. Por otro lado, se está creando en Ucrania un sistema nacional de medidas técnicas y de organización cuya finalidad es prevenir la realización de actividades ilícitas contra 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 bancarias, entre otros, en particular la interferencia en su labor valiéndose de las posibilidades que ofrece la red mundial de la Internet.

19. De conformidad con lo dispuesto en los apartados 10 y 11 del artículo 16 de la Ley sobre el Servicio Estatal de comunicaciones especiales y protección de la información de Ucrania, y con el fin de mejorar la coordinación de las actividades de los órganos del Estado dirigidas a detectar amenazas para la información en los sistemas informáticos, de información y telecomunicaciones, así como para mitigar las consecuencias de tales amenazas y establecer la cooperación en este ámbito, el Servicio Estatal de comunicaciones especiales y protección de la información de Ucrania estableció y puso en funcionamiento la dependencia CERT-UA.

20. De conformidad con las tendencias mundiales de desarrollo de redes de respuesta ante emergencias, el equipo de respuesta ante incidentes de seguridad de la información (CERT) es un grupo que se ocupa de responder a las emergencias informáticas. 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.

21. El 13 de julio de 2009 la dependencia especializada del Servicio Estatal de comunicaciones especiales y protección de la información de Ucrania CERT-UA (www.cert.gov.ua) pasó a ser miembro pleno de FIRST.

22. En el marco de sus actividades realizadas en 2009, CERT-UA elaboró 461 comunicaciones de los CERTs de 30 países del mundo (Australia, Austria, Bélgica, Hungría, Países Bajos, Dinamarca, Israel, India, España, Italia, Canadá, China, Corea, Lituana, Malasia, Alemania, Noruega, Pakistán, Polonia, Portugal, Federación de Rusia, Rumania, Arabia Saudita, Estados Unidos de América, Taiwán, Turquía, Finlandia, Francia, Estonia y Japón) sobre actividades no autorizadas en el segmento ucraniano de la red de la Internet (difusión de elementos informáticos dañinos, ataques DDoS y otros intentos de actividades no autorizadas).

23. 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.

24. 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 seguridad y asegurar la protección de los servicios de información y telecomunicaciones se ajustan en general a los criterios que aplican los órganos estatales competentes de los Estados Miembros de las Naciones Unidas y la Unión Europea encargados de velar por la seguridad de la información.

25. 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.