Naciones Unidas A/64/129/Add.1

Asamblea General

Distr. general
9 de septiembre de 2009
Español
Original: español/francés

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

Adición **

Índice

* A/64/50 y Corr.1.
** La información que figura en este documento se recibió después de la presentación del informe principal.

09-50578 (S) 180909 240909

II. Respuestas recibidas de los Gobiernos

Cuba

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

Respuesta a la resolución 63/37 “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”

1. Cuba comparte plenamente la preocupación que se expresa en el texto de la resolución 63/37 respecto al empleo de las tecnologías y medios de información con propósitos incompatibles con al 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 adecuadamente 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 norteamericanas en su guerra radial y televisiva contra Cuba, en franca violación de las normativas internacionales vigentes en materia de regulación del espectro radio-eléctrico.

5. Los Gobiernos norteamericanos no han 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. Es una actitud impropia de un miembro permanente del Consejo de Seguridad de las Naciones Unidas.

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, que establecen la conducta a seguir por los países miembros de dicha agencia especializada del sistema de las Naciones Unidas.

7. A fines del mes de mayo de 2009, se contabilizó un total de 1.924 horas de transmisiones ilegales semanales desde Estados Unidos contra Cuba, emitidas por 30 frecuencias. Varias de estas emisoras de radio pertenecen o prestan sus servicios

a organizaciones vinculadas con conocidos elementos terroristas que residen y actúan contra Cuba en territorio norteamericano, los que transmiten programas en los que se incita al sabotaje, los atentados políticos, el magnicidio y otros temas propios del radio-terrorismo.

8. 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 contra Cuba tiene un carácter subversivo, desestabilizador y engañoso, que contradice 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 borde 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 de la Unión Internacional de Telecomunicaciones, 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 Unión Internacional de Telecomunicaciones, que prohíbe a las estaciones de aeronaves en el mar o por encima del mar efectuar servicio alguno de radiodifusión.

- Dictamen de la Junta de 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 concluyó la 50ª Reunión de la Junta y en su Resumen de Decisiones (documento RRB09-1/5) se reitera, una vez más, la ilegalidad de las transmisiones y solicita a la Administración de Estados

Unidos de América, que adopte todas las medidas necesarias con miras a eliminar estos dos casos de interferencia a los servicios de televisión de Cuba.

- Artículo 23, numeral 23.3 del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones, que limita las transmisiones televisivas fuera de las fronteras nacionales. Un informe emitido en enero de 2009, por la Oficina de Auditoría del Gobierno de los Estados Unidos (GAO, instancia oficial estadounidense) reconoce 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.

9. 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". Estas conclusiones fueron acordadas a nivel del plenario de la CMR-07 y tienen valor legal para el trabajo de la Unión Internacional de Telecomunicaciones. 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.

10. La hostilidad del Gobierno de Estados Unidos de América contra Cuba se ha puesto de manifiesto a través del bloqueo económico, comercial y financiero impuesto por casi 50 años, que afecta también la esfera de la información y las telecomunicaciones, lo que se evidencia en algunos de los siguientes ejemplos, entre muchos otros:

- Cuba no tiene derecho a acceder a los servicios que ofrece 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 .c*u*.

- Sin previa notificación se han bloqueado dominios .*com* relacionados con Cuba, lo cual la Oficina de Control de Bienes Extranjeros (OFAC) ha ejecutado en fecha reciente.

- Ilustrativo resulta el anuncio público realizado en mayo de 2009, por el consorcio tecnológico Microsoft de suspender su servicio de conversación "Windows Live Messenger IM" para Cuba y otros países "por su obligación de someterse a la legislación estadounidense". Al momento de conectarse a esta herramienta se lee: "Microsoft ha cortado el Windows Live Messenger IM para los usuarios de países embargados por Estados Unidos, por ello Microsoft no ofrecerá más servicio de Windows Live en su país".

- Otras páginas web han negado el acceso desde el dominio .*cu*: Cisco Systems (http://tools.cisco.com/RPF/register.do), tecnologías para conexión, ruteadores para servidores de acceso a Internet, incluso equipamiento en el campo del vídeo digital: SolidWorks (http://www.solidworks.com/sw/termsofuse.html),

sistemas automatizados de diseño, y Symantec (http://symantec.com/about/profile/policies/legal) softwares de protección contra virus.

- Con total cinismo e hipocresía Estados Unidos acusa a Cuba con la mentira de impedir el acceso de sus ciudadanos a la red global, cuando la realidad bien diferente es que Cuba no puede, por las leyes del bloqueo que le aplica Estados Unidos, conectarse a los cables de fibra óptica que rodean el archipiélago cubano, obligándola a pagar los costosos servicios de satélites.
- La Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) ha tenido pérdidas en el orden de los 53.769,8 dólares EE.UU. hasta diciembre de 2008, debido fundamentalmente a la falta de acceso al mercado estadounidense para comprar equipamiento especializado. Ello obliga a buscar intermediarios que encarecen en extremo los productos necesarios para garantizar sus servicios.

11. Esa actitud de Estados Unidos 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 sobre la Sociedad de la Información (CMSI). La CMSI instó enérgicamente a los Estados a que, en la construcción de la Sociedad de la Información, adoptaran 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.

12. El 12° período de sesiones de la Comisión de Ciencia y Tecnología para el Desarrollo, celebrada en Ginebra, del 25 al 29 de mayo de 2009, al analizar los progresos alcanzados en la implementación y seguimiento de los resultados de la CMSI, constituyó un importante marco para reiterar la denuncia de Cuba a la aplicación de la política de bloqueo por parte del Gobierno de Estados Unidos y en particular de la aplicación de medidas coercitivas unilaterales sobre el desarrollo de las tecnologías de las comunicaciones y el acceso a la información, así como la implementación de una política de agresión al espectro radio electrónico de Cuba, que contravienen las disposiciones adoptadas en las dos fases de la referida Cumbre.

13. 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 Estados Unidos de América contra Cuba, confirman la necesidad de ese debate, y la urgencia de adoptar medidas para poner fin a tales manifestaciones de terrorismo de Estado.

14. Cuba apoya resueltamente ese ejercicio en la Asamblea General de las Naciones Unidas y por eso se unió a los 178 Estados Miembros que votaron a favor de la resolución 63/37, en contraste con la reiterada actitud asumida por Estados Unidos de América, único país que votó en contra.

15. Cuba 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, y está dispuesta a colaborar con el resto de los países, incluido Estados Unidos de América, para encontrar soluciones que superen los obstáculos que impiden alcanzar esos objetivos.

España

[Original: Español]
[8 de julio de 2009]

Posición de España sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Introducción

1. La seguridad de la información es un aspecto clave de la sociedad de la información. Los avances tecnológicos han propiciado un incremento continuo y acelerado de las capacidades de tratamiento y almacenamiento de la información, en múltiples formatos; por otra parte, en el ámbito de las comunicaciones se ha producido un incremento muy significativo de los anchos de banda disponibles, lo que conlleva la posibilidad de transmitir y recibir enormes cantidades de información, prácticamente en tiempo real y sin necesidad de disponer de infraestructuras particularmente complejas.

2. Estos avances tecnológicos al tiempo que mejoran el acceso a la información de todo tipo, facilitan además el uso o acceso a la misma con fines ilícitos, destacando el empleo de los sistemas de telecomunicaciones e informáticos con fines hostiles, delictivos e, incluso, para cometer actos terroristas o agresiones, entre Estados o actores transnacionales.

3. En el último año se ha confirmado la tendencia creciente en el uso de Internet por las organizaciones criminales y en particular por los grupos terroristas, que se aprovechan fundamentalmente de dos de sus características: su carácter global y las grandes garantías de anonimato que puede proporcionar.

4. Es necesario, por consiguiente, adoptar un equilibrio entre la evolución de la sociedad y las tecnologías de la información y la evolución simultánea de una normativa, nacional e internacional, actualizada, moderna, adaptada al nuevo entorno tecnológico, que sea capaz de responder a los retos que presenta la necesidad de proteger la información para prevenir su uso ilícito sin limitar los derechos y libertades de las personas.

Uso indebido de Internet con fines terroristas

5. En la actualidad las principales amenazas que se derivan del uso de Internet por parte de organizaciones terroristas son las siguientes:

a) Uso de Internet como un arma, es decir, la utilización de Internet como un medio para lanzar ataques contra sistemas informáticos de infraestructuras críticas o contra la propia infraestructura de Internet. Ataques de este tipo son relativamente frecuentes en el ámbito de la delincuencia común, pero el ataque sufrido por Estonia en el año 2007 puso de manifiesto que las infraestructuras de la información de un Estado también pueden verse afectadas por un ataque de este tipo. Directamente relacionadas con este tipo de amenaza se encuentra el aumento considerable de nuevo software dañino que ha aparecido en los últimos dos años y las “botnets” o redes de ordenadores “zombies”, que se utilizan para desarrollar ataques contra sistemas informáticos.

b) Uso de Internet como un medio para desarrollar otras actividades, fundamentalmente las siguientes:

- Actividades de comunicación. El uso de la Red está desplazando a las comunicaciones realizadas por las organizaciones criminales a través de otros medios como la telefonía fija o la telefonía móvil. Los instrumentos más utilizados para desarrollar comunicaciones a través de Internet son el correo electrónico, los programas de mensajería instantánea y los foros.
- Difusión de propaganda y material relacionado con actividades terroristas. En la actualidad existen miles de sitios web relacionados con actividades terroristas o que incitan a la violencia, tendencia que se ha visto amplificada con el surgimiento del fenómeno de los "blogs". En cuanto a la forma de impedir este uso de la Red por parte de las organizaciones terroristas se trata de un asunto bastante complicado puesto que estos sitios migran con mucha facilidad. Se trata de un fenómeno transnacional, ya que los países en los que se encuentra el servidor en el que se aloja la página y desde donde se administra la misma pueden ser diferentes y además distintos del país en el que actúa la organización terrorista en cuestión.
- Actividades de reclutamiento. En ocasiones Internet se utiliza como medio para desarrollar actividades de captación, sobre todo a través de los foros y los programas de mensajería instantánea.
- Financiación. Internet también ofrece oportunidades para que las organizaciones terroristas realicen actividades orientadas a la obtención de financiación. Es particularmente interesante la posibilidad de que organizaciones terroristas participen en la comisión de fraudes a través de Internet como medio para obtener financiación.
- Difusión de manuales de entrenamiento. A través de Internet las organizaciones terroristas difunden manuales sobre técnicas terroristas, fabricación de explosivos o manejo de armas.
- Recogida de información para la comisión de atentados. Internet constituye una fuente de información muy importante que en muchas ocasiones es utilizada por las organizaciones terroristas para obtener datos sobre objetivos de sus actividades.

Medidas adoptadas en el ámbito nacional para luchar contra el uso de Internet por organizaciones terroristas

Medidas legislativas

6. Entre las medidas que adoptan los diversos Estados, España ha realizado un gran esfuerzo en los últimos años y en especial en 2007, incluyendo en su sistema jurídico una serie de leyes que inciden en la seguridad de la información y en el libre ejercicio de los derechos y libertades reconocidos en la Declaración Universal de Derechos Humanos y en la Constitución Española. Se ha desarrollado una amplia legislación y normativa, incluyendo tanto aspectos puramente nacionales como directivas procedentes de la Unión Europea, encaminada a cumplir con estos objetivos, aplicando unos nuevos criterios de seguridad de la información, en donde se considera que para alcanzar un grado razonable de protección, además de preservar la confidencialidad de la información, se convierte en primordial, en la

mayoría de los casos, preservar la integridad y la disponibilidad de ésta. Destacan (orden cronológico):

- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, animada por la idea de implantar mecanismos cautelares que previniesen las violaciones de la privacidad resultantes del tratamiento de la información, y disposiciones que la desarrollan.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, cuyo objeto es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar, y disposiciones que la desarrollan.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas, que incorporaba al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. La Ley 59/2003, de 19 de diciembre, de firma electrónica, actualiza este marco mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y, posteriormente, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, mediante los cuales se encomienda al CNI, entre otras cosas, coordinar la acción de los diferentes organismos de la Administración que utilicen medios y procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito y velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Tiene por objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.
- Ley 32/2003, de 13 de noviembre, general de telecomunicaciones, que regula la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.
- Ley 59/2003, de 19 de diciembre, de firma electrónica, ya citada.

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que regula la comunicación mediante el empleo y la aplicación de las técnicas y medios electrónicos, informáticos y telemáticos existentes entre los ciudadanos y las Administraciones Públicas.
- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ácido desoxirribonucleico (ADN), que crea una base de datos en la que, de manera única, se integran los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado en los que se almacenan los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal, o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que incide positivamente en las investigaciones desarrolladas en este ámbito.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.
- Tipificación penal de los siguientes delitos cibernéticos relacionados con la actividad de organizaciones terroristas en Internet:
  - Sabotajes informáticos, artículo 264 del Código Penal.
  - Amenazas, artículo 169 y siguientes del Código Penal.
  - Apología y enaltecimiento del terrorismo, artículo 578 del Código Penal.

Otras medidas

- Creación de grupos policiales dedicados a luchar contra el uso de Internet por parte de grupos criminales.
- Participación en el proyecto “Check the Web” desarrollado por Europol.
- Creación de un centro de respuesta rápida CERT para mejorar la seguridad de los sistemas informáticos de las Administraciones Públicas.
- Creación del Centro Nacional de Protección de Infraestructuras Críticas.

Medidas que podrían ser adoptadas por la comunidad internacional para fortalecer la seguridad informática a escala mundial

- El uso de Internet por parte de organizaciones terroristas es un fenómeno de dimensión transnacional que requiere en muchas ocasiones la investigación conjunta en diferentes países. Por tanto, la investigación y prevención de actividades terroristas en Internet depende en gran medida de la existencia de acuerdos internacionales y de otras herramientas de cooperación internacional. En este aspecto es importante que se tienda a una armonización legislativa que permita luchar de forma más eficaz contra la presencia de estos grupos criminales en la Red. La colaboración internacional en el ámbito policial es

también un aspecto clave puesto que la rapidez es crucial en este tipo de investigaciones debido a la volatilidad de las evidencias electrónicas.

- Involucrar al sector privado en la lucha contra la ciberdelincuencia. La colaboración del sector privado es esencial puesto que la mayoría de los servicios de Internet está en sus manos. El sector privado lleva mucho tiempo haciendo frente a las amenazas existentes en Internet y sus conocimientos y experiencia pueden ser muy valiosos en este terreno.

- Concienciar el usuario final para que preste atención a la seguridad de sus sistemas informáticos. Una mayor conciencia sobre este problema reduciría el número de ordenadores utilizados por los ciberdelincuentes para desarrollar sus actividades, en especial las relacionadas con las “botnets”.

- Sobre las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial, debería conseguirse la firma de un convenio entre Estados (análogo al convenio SOLAS o similar), en el que los mismos se comprometan a unificar las legislaciones para permitir la persecución de los delitos en la Red, intentando evitar en la medida de lo posible que el anonimato, la ausencia de legislación y los intereses económicos hagan de la Red el caldo de cultivo ideal para la delincuencia y el terrorismo. Todo ello equilibrándolo con la libertad de información y el libre acceso a la misma.

- Agilizar los procedimientos de cooperación judicial y policial en la escena internacional para poder perseguir ilícitos penales, con rapidez y eficacia, debido al carácter distribuido de Internet y la volatilidad de los registros de conexiones, según la legislación de cada país.

7. Como conclusión, se considera que la comunidad internacional debería adoptar las medidas de protección de la información que se estimen necesarias, partiendo de una visión estratégica unitaria y, si es posible, estableciendo una dirección única, que establezca normas y pautas comunes a todos los países, establezca un conjunto equilibrado y completo de medidas específicas de protección y permita la armonización de las políticas y acciones de las diferentes organizaciones nacionales e internacionales implicadas.

Malí

[Original: francés]
[9 de julio de 2009]

Opiniones y observaciones relativas a la aplicación de la resolución relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Evaluación general de los problemas de la seguridad de la información

1. La denegación de servicio, que tiene por objeto detener el funcionamiento de un sistema informático, y la intrusión con miras a desviar las informaciones son las principales formas de ataque de los sistemas informáticos.

2. Las amenazas que se ciernen sobre los sistemas gubernamentales o de empresas delicadas son amenazas o incidentes que afectan a la integridad, la confidencialidad o la disponibilidad de la infraestructura de información fundamental.

3. Se pueden mencionar, entre otras formas de amenazas, las siguientes:

- Las amenazas organizadas por un gobierno extranjero, un grupo terrorista o por extremistas que tienen un móvil político
- Las amenazas relacionadas con objetivos de espionaje, sabotaje, injerencia extranjera o violencia de carácter político (terrorismo)

4. El empleo de tecnologías de la información aparece como una alternativa al empleo de métodos más tradicionales, como la destrucción, la interferencia por radiación electromagnética, la intrusión física o el control de las fuentes de información internas.

5. Los ataques informáticos pueden estar dirigidos tanto contra particulares como contra empresas o instituciones políticas. En relación con los que afectan a la defensa o la seguridad nacional, los servicios estatales, los operadores de importancia vital y las empresas que intervienen en esferas estratégicas o delicadas se ven particularmente implicados. Sin embargo, esos ataques no tienen las mismas consecuencias si van dirigidos contra sitios o servicios accesibles al público que contra sistemas operacionales o más directamente contra personas que manejan información delicada.

6. La determinación del origen de un ataque informático es particularmente difícil. Los procedimientos utilizados recurren la mayoría de las veces a una sucesión de computadoras que pueden encontrarse en países diferentes. Seguir la pista de las máquinas implicadas supondría realizar investigaciones extremadamente largas, cuyos resultados dependerían de la contingencia de la cooperación judicial internacional. Los métodos de enmascaramiento son numerosos y van desde el desvío de las computadoras sin conocimiento de sus propietarios hasta la utilización de computadoras públicas y anónimas, como las que existen en los cibercafés.

7. A pesar de todo, la mayoría de los servicios gubernamentales y de los observadores perciben tras esos ataques a grupos de piratas informáticos cuyos métodos parecen cada vez más complejos.

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

a) En el plano nacional

8. Actualmente Malí no cuenta con una legislación vigente en materia de seguridad de la información.

9. La aplicación de un marco jurídico y reglamentario es uno de los ejes prioritarios del plan estratégico nacional de tecnologías de la información y las comunicaciones aprobado por el Gobierno en junio de 2005.

10. El Gobierno de Malí ha obtenido un crédito (núm. 4033 MLI) de la Asociación Internacional de Desarrollo (AID) para financiar el proyecto de apoyo al crecimiento y se propone utilizar parte de ese crédito para realizar una consulta en relación con la asistencia técnica para la preparación del marco jurídico y reglamentario para las tecnologías de la información y las comunicaciones de Malí.

11. La selección de consultores para los préstamos del Banco Mundial se tradujo en la solicitud de muestras de interés Núm. 001/2009/SPM/UCP-PAC, conforme a las instrucciones elaboradas en mayo de 2008 por el Organismo de Tecnologías de la Información y las Comunicaciones (AGETIC).

12. En ese marco jurídico y reglamentario se prevé la elaboración de textos legislativos sobre las libertades, los negocios, el comercio electrónico, la propiedad intelectual, la seguridad y confidencialidad de los datos, los delitos cibernéticos, el libre acceso a las informaciones públicas y a las que constituyen patrimonio de la humanidad.

b) Actividades de cooperación internacional para fortalecer la seguridad de la información

13. Los ataques informáticos atraviesan las fronteras y pueden dirigirse simultáneamente contra varios Estados. La vigilancia de las redes y la adopción de medidas en caso de que se produzcan incidentes justifican la cooperación y la asistencia internacionales. De manera general, la protección de los sistemas de información contra las actividades ilegales constituye en la actualidad una preocupación común de numerosos Estados.

14. Malí, por su parte, opta por un enfoque regional de la evolución de la reglamentación del sector de las telecomunicaciones, lo que lo ha llevado a ratificar las directrices de la Unión Económica y Monetaria de África Occidental (UEMAO) en 2006 y las actas adicionales de la Comunidad Económica de los Estados de África Occidental (CEDEAO) en 2007.

15. La Unión Internacional de Telecomunicaciones trabaja en el establecimiento de un marco internacional para la promoción de la seguridad cibernética (Programa Mundial de Ciberseguridad) en el que se interesa muy particularmente el Estado de Malí. Esta promoción de la ciberseguridad ha dado lugar a la creación de un grupo de expertos de alto nivel encargado de proponer una estrategia a largo plazo que

comprenda las medidas jurídicas y las medidas técnicas orientadas a remediar las deficiencias de los programas informáticos, así como la prevención y detección de los ataques informáticos y la gestión de crisis.

Conceptos internacionales encaminados a fortalecer la seguridad de los sistemas de información y telecomunicaciones

16. La seguridad de la información a nivel internacional debería basarse en el derecho internacional vigente (*jus ad bellum*), que define cómo contrarrestar las amenazas a la paz y la seguridad internacionales, y en el derecho internacional humanitario (*jus in bellum*), que se refiere a los métodos y los medios de guerra, la protección de los Estados que no son partes en un conflicto, así como a las personas y los bienes que se ven o podrían verse afectados por el conflicto.

17. La Carta de las Naciones Unidas es la piedra angular del derecho internacional en lo atinente al mantenimiento de la paz y la seguridad internacionales.

18. Los especialistas de derecho internacional, en conjunto, reconocen que esas reglas crean un mecanismo universal de seguridad para preservar la paz y la seguridad internacionales. Si bien las tecnologías de la información y las comunicaciones se conciben y emplean como medios de destrucción (en otras palabras, las "armas de la información") y la comunidad internacional no ha decidido aún el lugar que la seguridad de la información ocupa en el derecho internacional en vigor, la Carta de las Naciones Unidas podría interpretarse de manera tal que concediera a los agentes internacionales una libertad considerable para utilizar las tecnologías de la información y las comunicaciones para llevar a cabo actividades agresivas y arreglar conflictos y controversias internacionales.

19. Esta situación sorprendente se deriva del hecho de que las acciones hostiles en la esfera de la información no son abordadas aún explícitamente por el derecho internacional en el mismo plano que las acciones hostiles llevadas a cabo con armamento clásico, aun cuando la interrelación del mundo en la actualidad y su dependencia respecto de las tecnologías de la información y las comunicaciones signifique que un ataque sería tan devastador como un ataque clásico, incluso podría serlo más. Las dificultades se ven exacerbadas por la ausencia de interpretaciones comúnmente admitidas de nociones tales como el "acto de agresión" (Art. 1), la "fuerza" (párrafo 4 Art. 2) y la "agresión armada" (Art. 51) en relación con la seguridad de la información.

20. En la resolución 3314 (XXIX) de la Asamblea General, de 14 de diciembre de 1974, se define el acto de agresión.

21. Aun cuando esta resolución no se haya aprobado por consenso, sus disposiciones indicativas proporcionan al Consejo de Seguridad y a todos los miembros de la comunidad internacional criterios para determinar un acto de agresión.

22. La utilización de un arma de información puede interpretarse como un acto de agresión si el Estado víctima tiene motivos para pensar que el ataque se llevó a cabo por las fuerzas armadas de otro Estado y tenía por objetivo perturbar el funcionamiento de instalaciones militares, destruir la capacidad de defensa y la economía, o violar la soberanía del Estado en un territorio particular.

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

23. A fin de reforzar la seguridad de la información a escala mundial y de hacer frente a la amenaza de utilización de las tecnologías de la información y las comunicaciones con fines hostiles, la comunidad internacional tiene el deber de intensificar su intervención en determinadas esferas, entre las que cabe señalar:

a) El apoyo de los Estados en la sensibilización y la rendición de cuentas de los diferentes actores (administración, empresas y usuarios) respecto de la seguridad de los sistemas de información;

En ese contexto, debe concederse gran importancia a la coordinación de políticas entre los Estados en relación con el apoyo a la base industrial y tecnológica en materia de productos asegurados. También se debe prestar atención especial a la colaboración entre los Estados y el sector privado.

b) El fortalecimiento de la capacidad de los Estados poniendo a su disposición los recursos humanos y la experiencia técnica necesarios para la vigilancia y, por ende, la detección de las corrientes anormales por las que transitan los ataques informáticos;

c) La reorganización de las políticas de las diferentes instituciones internacionales que operan en la esfera de la seguridad de los sistemas de información atribuyendo a cada una de ellas competencias específicas;

d) El establecimiento de indicadores en la esfera de la seguridad informática para ayudar a las naciones a administrar mejor las infraestructuras de las tecnologías de la información y las comunicaciones. Esos indicadores pueden referirse a los aspectos siguientes, entre otros:

- Recuperación de los datos en caso de desastre
- Utilización de los estándares (normas)
- Control del funcionamiento (benchmarking)
- Transferencia electrónica
- Colaboración con Interpol
- Plataforma de acceso

Conclusión

24. De nuestras observaciones se desprende que las cuestiones relativas a la seguridad informática y la utilización de las tecnologías de la información y las comunicaciones con intenciones dolosas causan cada vez mayor preocupación. Es cierto que esas tecnologías ofrecen numerosas ventajas, pero pueden dar lugar a desastres de consecuencias extraordinarias, habida cuenta de su desarrollo desenfrenado.

25. Las cuestiones jurídicas derivadas de su desarrollo no han encontrado hasta ahora respuestas satisfactorias debido a la diversidad de las reglamentaciones, a menudo mal adaptadas.

26. Corresponde a los Estados velar por la construcción armoniosa de esos instrumentos para garantizar un mejor progreso hacia una sociedad de la información dotada de una mejor seguridad.