Naciones Unidas A/68/156

Asamblea General

Distr. general
16 de julio de 2013
Español
Original: español/inglés/ruso

Sexagésimo octavo período de sesiones
Tema 94 de la lista preliminar*
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/68/50.

13-39738X (S)

I. Introducción

1. El 3 de diciembre de 2012, la Asamblea General aprobó la resolución 67/27, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”. En el párrafo 3 de esa resolución, la Asamblea General invitó a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuraban en el informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (A/65/201), siguieran comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

a) La evaluación general de los temas relacionados con la seguridad de la información;

b) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera;

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. Atendiendo a esa petición, el 22 de febrero de 2013 se envió una nota verbal a los Estados Miembros invitándolos a proporcionar información sobre el tema. Las respuestas recibidas se recogen en la sección II. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los Gobiernos

Cuba

[Original: español]
[20 de mayo de 2013]

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, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales.

Cuba comparte plenamente la preocupación que se expresa en la resolución 67/27 respecto al empleo de las tecnologías y medios de información con propósitos que pueden afectar la estabilidad y la seguridad internacionales, la integridad de los Estados y en detrimento de su seguridad en las esferas civil y militar. Igualmente, esa resolución hace adecuado énfasis en la necesidad de impedir la utilización de los recursos y las tecnologías de la información con fines delictivos o terroristas.

En este contexto, Cuba reitera su condena a la escalada agresiva del Gobierno de los Estados Unidos en su guerra radial y televisiva contra Cuba, que viola las normativas internacionales vigentes en materia de regulación del espectro radioeléctrico. Esta agresión se realiza sin reparar en el daño que pudieran causar a la paz y seguridad internacionales, creando situaciones de peligro, incluso utilizando

un avión militar para transmitir señales de televisión hacia el país, sin el consentimiento de la República de Cuba.

Las transmisiones desde aeronaves violan la disposición 42.4 del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), que prohíbe efectuar servicio de radiodifusión a las estaciones de aeronaves en el mar o por encima del mar.

En el año 2012, Estados Unidos realizó 192 vuelos a través de los cuales, además de transmitir ilegalmente señales de televisión desde aeronaves hacia territorio cubano, realizaron simultáneamente, transmisiones ilegales en la banda de radiodifusión por FM. Estas acciones provocaron interferencias perjudiciales a las estaciones de televisión cubanas, inscriptas en el Registro Maestro de la Oficina de Radiocomunicaciones de la UIT.

Cada semana, emisoras radicadas en el territorio de los Estados Unidos transmiten hacia Cuba un promedio de 2.400 horas de radio y televisión de manera ilegal, a través de 30 diferentes frecuencias de onda media, corta, FM y televisión. Varias de estas emisoras pertenecen o prestan sus servicios a organizaciones vinculadas con conocidos elementos terroristas que residen y actúan contra Cuba en territorio estadounidense, quienes transmiten programas en que se incita al sabotaje, los atentados políticos, el magnicidio y otros temas propios del radio-terrorismo.

Las transmisiones ilegales de radio y televisión contra Cuba tienen la intención de fomentar la inmigración ilegal, alentar e incitar a la violencia, el desacato al orden constitucional y la perpetración de actos terroristas. Cuba reitera que el empleo de la información con un marcado interés en subvertir el orden interno de otros Estados, violar su soberanía y realizar actos de intromisión e injerencia en sus asuntos internos resulta, una acción ilegal.

Estas transmisiones provocadoras contra Cuba violan las normas internacionales que rigen el uso del espectro radioelectrónico del Convenio Internacional de Radiocomunicaciones, del cual el Gobierno de los Estados Unidos es uno de sus países signatarios.

Cuba apoyó la resolución 67/27 y continuará contribuyendo al desarrollo global pacífico de las tecnologías de la información y las telecomunicaciones y su empleo en bien de toda la humanidad.

España

[Original: español]
[29 de mayo de 2013]

1. Introducción

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.

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 trasnacionales.

En los últimos años 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.

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.

2. Uso indebido de Internet con fines terroristas

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 colapsadas por un ataque de este tipo. Directamente relacionadas con este tipo de amenaza se encuentra el aumento considerable de nuevo software malicioso que ha aparecido en los últimos 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 de forma segura y anónima 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 la Web 2.0 y las redes sociales. 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, creándose un vacío legal si no hay acuerdos bilaterales con dichos países.

- **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. Resulta particularmente atractiva la posibilidad de que organizaciones terroristas participen en la comisión de fraudes, extorsión y blanqueo de dinero 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, ya sean personas, organizaciones o infraestructuras.

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

3.1. Medidas legislativas

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 los 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:

- La Ley Orgánica 5/1992, de 29 de octubre de 1992, 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 1999, 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 de su honor e intimidad personal y familiar, y disposiciones que la desarrollan.

- Real Decreto-Ley 14/1999, de 17 de septiembre de 1999, 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 jurídico 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 2003, 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 de 2002, reguladora del Centro Nacional de Inteligencia (CNI) y posteriormente, el Real Decreto 421/2004, de 12 de marzo de 2004, 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 2002, 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 de 2000, 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 de 1998, 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 3 de noviembre de 2003, 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 2003, de firma electrónica, ya citada.

- Ley 11/2007, de 22 de junio de 2007, 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 de 2007, 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 2007, 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 de 2007, 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 2007, 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.

3.2. 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 la Oficina Europea de Policía (Europol).
- El Centro Criptológico Nacional del Centro Nacional de Inteligencia contribuye diariamente y de forma decisiva a la lucha contra los ataques cibernéticos, destacando la actividad del CCN-equipo de respuesta a emergencias cibernéticas (CERT), que soporta la capacidad de respuesta a incidentes de seguridad de la información. Creado a principios de 2007 como CERT gubernamental español, está presente en los principales foros internacionales en los que se comparte objetivos, ideas e información sobre la ciberseguridad.
- Creación del Centro Nacional de Protección de Infraestructuras Críticas.
- El Ministerio de Defensa viene desarrollando diversas actuaciones en el campo de la ciberdefensa. Destaca la participación, a través del Estado Mayor de la Defensa, en el Centro de Excelencia de Ciberdefensa de la Organización del Tratado del Atlántico Norte (OTAN) en Tallín, Estonia, que España cofinancia desde su creación, y al que aportando dos expertos. La relevancia internacional de dicho Centro en la lucha contra el ciberterrorismo es creciente, como rubrica la reciente visita de Su Majestad el Rey, en la que resaltó el compromiso de España con las iniciativas internacionales sobre ciberseguridad.
- Por otro lado, la OTAN está siendo muy activa en el desarrollo de actividades de ciberdefensa, habiendo desarrollado un concepto, establecido una política y nombrado una autoridad de gestión de la ciberdefensa en la alianza.
- La Organización para la Seguridad y la Cooperación en Europa (OSCE) ha establecido un grupo de trabajo informal para la elaboración de medidas de fomento de la confianza para reducir los riesgos de conflictos dimanantes del uso de tecnologías de la información y las comunicaciones. Este grupo de

trabajo tiene como objetivo el reducir las posibilidades de ciberataques al mismo tiempo que se apuntala la seguridad mutua a través de la cooperación internacional, promoviendo claridad y transparencia y reduciendo los riesgos de una percepción errónea que puede llevar a una escalada de los conflictos, todo ello a través del desarrollo de medidas de fomento de la confianza en la dimensión político-militar para el uso de las tecnologías de la información y la comunicación.

- Esquema Nacional de Seguridad. Tiene por objeto establecer la política se seguridad nacional en la utilización de los medios electrónicos. Se fundamenta en principios básicos y requisitos mínimos que permitan una protección adecuada de la información, y en él participan todas las administraciones. Su respaldo legal se encuentra próximo a publicar como Real Decreto, para dar cumplimiento al artículo 42 de la Ley 11/2007. De hecho, la Estrategia Española de Seguridad, al identificar las amenazas y riesgos más importantes para la seguridad de nuestro país y señalar cómo responder a ellas, especifica el ciberespacio como uno de los diferentes ámbitos donde hay que actuar. Este análisis constituye la base sobre la que formular líneas estratégicas de respuesta y desarrollar capacidades y acometer reformas organizativas.

La Directiva de Defensa Nacional 2012, al enumerar las amenazas globales a las que debemos hacer frente, establece en primer lugar los ataques cibernéticos como uno de los principales riesgos, que solo podrán ser enfrentados desde una coalición de fuerzas que en nuestro caso tendrá como base la OTAN y la Unión Europea pero que, además, debe contar con el apoyo de otros países y grupos de países directa e igualmente interesados en el control de estos fenómenos.

Del mismo modo, esta Directiva marca como directriz a seguir, la participación “en el impulso de una gestión integral de la ciber-seguridad, en el marco de los principios que se establezcan al efecto en la estrategia de ciber-seguridad nacional.

La Directiva de Política de Defensa, aprobada durante el año 2012, también hace referencia a la aparición del ciberespacio como un nuevo ámbito para las relaciones internacionales, identificando como una necesidad de la defensa “el reforzamiento de los sistemas de obtención de información y de elaboración de inteligencia para apoyar a las operaciones, así como de los sistemas de mando y control para reducir el riesgo de ataques cibernéticos”.

El Jefe del Estado Mayor de la Defensa emitió, en enero de 2011, su visión de la ciberdefensa militar, que persigue orientar la definición, desarrollo y empleo de las capacidades militares necesarias que permitan garantizar la eficacia en el uso del ciberespacio en las operaciones militares.

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

El aumento de la dependencia de los sistemas de información y el incremento de la interconexión de las infraestructuras críticas han hecho que la seguridad del ciberespacio sea fundamental en el funcionamiento de un estado moderno. Por ello,

la ciberseguridad debe formar parte intrínseca del planeamiento de la seguridad nacional.

En la actualidad, no existe la garantía de un marco legal internacional que responda ante las amenazas a la seguridad en este campo, por lo que, sin ceder soberanía nacional en aspectos de ciberseguridad, se deberían alcanzar acuerdos multilaterales de colaboración en esta materia, análogo al Convenio internacional para la seguridad de la vida humana en el mar (SOLAS), o similar, en el que los estados 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.

Se debe involucrar al sector privado, especialmente a los proveedores de servicios de Internet, 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.

Los CERTs son piezas clave en la ciberseguridad. El establecimiento de CERTs especializados y la formación continua de sus componentes sobre las últimas tendencias son los primeros pasos que deben adoptar los gobiernos para garantizar la ciberseguridad. Resulta igualmente importante la creación dentro de las fuerzas de orden público de unidades especializadas en la investigación de los delitos cometidos a través de Internet.

La ciberseguridad es un desafío global, por ello, la cooperación internacional orientada a su mejora es fundamental y debería ser alentada tanto a nivel político como operacional. Las comunicaciones entre CERTs de diferentes países deben ser muy fluidas para facilitar compartir información sobre ataques con un breve tiempo de respuesta. También las lecciones aprendidas y las mejores prácticas nacionales e internacionales deben ser compartidas.

Otras medidas incluyen:

- Formar y concienciar al ciudadano, desde edades tempranas, para que preste atención a la seguridad de los sistemas informáticos que utilice. Muchas formas del cibercrimen se aprovechan (o incluso dependen) del hecho de que muchos usuarios de Internet no toman las debidas precauciones para hacer sus ordenadores y cuentas tan seguras e impenetrables como sea posible. Por ello la educación del usuario es esencial. Una mayor concienciación sobre este problema reduciría el número de ordenadores utilizados por los ciberdelincuentes para desarrollar sus actividades, en especial las relacionadas con las “botnets”.
- 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 de la volatilidad de los registros de conexiones, según la legislación de cada país.
- Organizar foros, seminarios y conferencias multinacionales. Tendrían por objetivo elevar los conocimientos de los expertos y compartir el conocimientos de las diferentes formas de ataque, las nuevas tendencias de ciberataques, el análisis de las vulnerabilidades y el impacto de potenciales ataques, así como

compartir las lecciones aprendidas y mejores prácticas, y promover una formación homogénea de las fuerzas de orden público sobre investigación de cibercrímenes.

- Coordinar los esfuerzos de otras organizaciones especializadas en áreas específicas de ciberseguridad, como el Consejo de Europa y la OTAN. Esto evitaría una innecesaria duplicación de esfuerzos.
- Generar guías o relación de buenas prácticas para mejorar la ciberseguridad, en cooperación con el sector privado y la sociedad civil.

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 internacionales implicadas.

Ucrania

[Original: ruso]
[31 de mayo de 2013]

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

Las esferas de la seguridad de la información, la seguridad de las telecomunicaciones y la respuesta a la ciberdelincuencia son básicas para la seguridad nacional en Ucrania. A su vez, velar por la seguridad nacional de Ucrania fomenta el fortalecimiento de la seguridad internacional en un mundo globalizado.

La globalización, la creación de una sociedad de la información y la adopción de nuevas tecnologías de la información, todos ellos fenómenos que se están produciendo en todo el mundo, contribuyen al aumento de la importancia atribuible a la seguridad de la información como componente de la seguridad nacional. La seguridad de la información se define como el grado en el cual los intereses nacionales en la esfera de la información están protegidos de amenazas externas y nacionales.

Por consiguiente, el concepto genérico de amenazas internacionales a la seguridad de la información incluye todos los elementos siguientes:

- Uso ilegal de los recursos de la información;
- Actividades no autorizadas y destructivas relacionadas con sistemas automatizados, incluidos los empleados para la gestión de instalaciones cruciales de la infraestructura nacional;
- Uso del ciberespacio, de actividades conexas, o de tecnologías y recursos de la información de manera que menoscabe los derechos humanos y las libertades fundamentales o con fines de llevar a cabo actos de terrorismo, extremistas o delictivos de otro tipo, incluidas agresiones;

- Uso de la infraestructura de la información para difundir mensajes que inciten a la animosidad y el odio, en general o en un país específico;
- Difusión de información contraria a la legislación nacional vigente y a las normas y los principios morales;
- Uso del ciberespacio para desestabilizar la sociedad y socavar el sistema económico, político y social de otro Estado o para difundir información falsa destinada a distorsionar los valores culturales, éticos y estéticos;
- Obstáculos al acceso a tecnologías de vanguardia que fomentan la dependencia en la esfera de la tecnología de la información a fin de lograr ventajas y control sobre el ciberespacio de otros países.

Cabe destacar los siguientes ámbitos problemáticos relacionados con la globalización: manipulación psicológica y de la información de manera masiva o dirigida a personas concretas, limitaciones al acceso de los consumidores a servicios basados en las tecnologías de la información y las telecomunicaciones, y ciberdelincuencia.

Según especialistas de Ucrania, los factores siguientes pueden aumentar las probabilidades de que se produzcan las amenazas antes mencionadas:

- Escasos conocimientos informáticos de los usuarios de los recursos de información y los servicios del ciberespacio;
- Carencia de un marco conceptual internacional común para la seguridad de la información;
- Diversidad de enfoques en la legislación nacional para las medidas de protección de la información diseñadas para establecer y actualizar (restaurar) la infraestructura de la información;
- Niveles dispares de uso de computadoras y de seguridad de la información en los distintos países;
- Peligro de vincular recursos potencialmente destructivos con sistemas de información y telecomunicaciones;
- El hecho de que las fuentes de actividades no autorizadas en el ciberespacio pueden no estar claramente identificadas.

2. Esfuerzos adoptados a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en esta esfera

Los principales órganos estatales de Ucrania responsables en materia de la seguridad de la información y sus componentes son el Ministerio de Interior, el Servicio de Seguridad y el Servicio Estatal de Comunicaciones Especiales y Protección de la Información. Estas agencias son muy activas en la regulación de las diversas esferas de la seguridad de la información. Se da especial importancia al marco jurídico y normativo de los componentes cibernéticos (ciberseguridad).

En Ucrania actualmente están en vigor las siguientes disposiciones legislativas acerca de las relaciones sociales en cuestiones relacionadas con la seguridad de la información:

En virtud del artículo 17 de la Constitución de Ucrania, la seguridad de la información es una función crucial del Estado, junto con la protección de la soberanía y la integridad territorial, y con el mantenimiento de la seguridad económica.

Con arreglo al artículo 3 de la Ley sobre la información de Ucrania, velar por la seguridad de la información de Ucrania es una de las principales esferas de la política del Estado en materia de información.

En el sistema de seguridad de Ucrania en su conjunto, la seguridad de la información ocupa una posición especial, dado que las relaciones y los procesos de información forman parte de todos los procesos de la sociedad y del Estado. En este contexto, la seguridad de la información se define como la situación del espacio (entorno) de la información que consta de tecnologías de la información, recursos de información y relaciones en materia de información entre los agentes pertinentes, que garantiza la evolución y el uso del espacio de la información en beneficio del individuo, de la sociedad y del Estado.

Las prioridades de la seguridad nacional, que están vinculadas a los intereses de desarrollo social, determinan los objetivos principales de la seguridad de la información. Tales objetivos son los siguientes:

- Velar por la soberanía de la información nacional de Ucrania a medida que aumenta la globalización de los flujos de información y que otros países compiten por la influencia en la esfera de la información;
- Crear un entorno de información que apoye el desarrollo cultural, moral e intelectual de las personas y del conjunto de la sociedad;
- Mantener los recursos informativos de Ucrania en un nivel suficiente para garantizar el funcionamiento y el desarrollo sostenibles de las personas, la sociedad y el estado;
- Proteger la información de las personas físicas y jurídicas y del Estado contra amenazas externas e internas, lo que incluye hacer frente a los delitos informáticos;
- Garantizar la validez y el respeto de los derechos de los interesados en el sector de la información en Ucrania a crear y utilizar los recursos, las tecnologías y la infraestructura nacionales en materia de información.

Con la finalidad de reforzar la seguridad de la información se están poniendo en marcha un marco jurídico y normativo y un sistema de capacitación profesional, y se han coordinado las actividades de los organismos estatales responsables de la seguridad de la información. Esta coordinación incluye la cooperación con el equipo de respuesta a emergencias cibernéticas de Ucrania (CERT-UA) y el Foro de equipos de seguridad y respuesta a incidentes (FIRST), una organización acreditada a nivel internacional.

Con arreglo a la legislación de Ucrania, el CERT-UA pertenece al Servicio Estatal de comunicaciones especiales y protección de la información y coordina la labor de empresas, instituciones y organizaciones, independientemente de su

estructura de propiedad, a fin de prevenir y analizar las consecuencias de las acciones no autorizadas dirigidas a los recursos de información del Estado en los sistemas de la información y las telecomunicaciones, y responder en consecuencia.

Es más, el CERT-UA coopera con los órganos y las organizaciones pertinentes extranjeros e internacionales, y las obligaciones del equipo con sus contrapartes extranjeras (miembro pleno de FIRST y miembro de la Alianza Internacional Multilateral contra las Ciberamenazas de la Unión Internacional de Telecomunicaciones) estimulan la cooperación internacional en materia de seguridad de la información.

De conformidad con la Ley de Ucrania sobre las enmiendas a la Ley por la que se ratifica el Convenio sobre la Ciberdelincuencia, el Ministerio de Interior es el órgano autorizado para establecer y supervisar la red de puntos de contacto permanentes para asistencia en caso de emergencia con sistemas informáticos e investigación de delitos relacionados con los datos, el enjuiciamiento de las personas acusadas de esos delitos y la recopilación de pruebas electrónicas.

La dependencia competente, que gestiona la red de respuesta permanente a la ciberdelincuencia de la División de Lucha contra la Ciberdelincuencia, pertenece al Ministerio de Interior y es responsable de ejecutar las actividades y operaciones correspondientes, entre las que figuran las siguientes:

- Resolver ataques de denegación de servicio;
- Luchar contra delitos penales cometidos mediante tarjetas de pago o datos de cuentas bancarias;
- Luchar contra interferencias no autorizadas en las operaciones de servicios de banca electrónica entre el banco y el cliente;
- Contrarrestar la difusión de contenido ilegal en Internet (incumplimiento de derechos de autor);
- Impedir la difusión de pornografía por Internet, incluida la pornografía infantil;
- Hacer frente a los delitos relacionados con las telecomunicaciones;
- Hacer frente a delitos relacionados con el acceso no autorizado a redes de transmisión de datos vía satélite;
- Luchar contra el fraude financiero o de otro tipo perpetrado en Internet;
- Hacer frente a delitos penales o de otro tipo relacionados con el comercio electrónico;
- Gestionar las operaciones de respuesta a la ciberdelincuencia de los puntos de contacto de la red permanente.

En la actualidad están en marcha medidas encaminadas a actualizar la legislación nacional en materia de seguridad de la información a fin de establecer un marco jurídico y normativo armonizado con las normas internacionales.

En Ucrania se está elaborando un proyecto de ley sobre ciberseguridad, de conformidad con el Decreto Presidencial Núm. 1119, de 10 de diciembre de 2010, sobre la decisión adoptada el 17 de noviembre de 2010 por el Consejo Nacional de

Defensa y Seguridad de Ucrania relativa a los desafíos y las amenazas a la seguridad nacional de Ucrania en 2011.

Las siguientes esferas normativas pueden ser objeto de mayor atención en virtud de los actos normativos y jurídicos vigentes:

1) el Decreto Presidencial Núm. 1119, de 10 de diciembre de 2012, sobre la decisión del Consejo Nacional de Defensa y Seguridad de 17 de noviembre de 2010 relativa a los desafíos y las amenazas a la seguridad nacional de Ucrania en 2011 (párrafo 4); el Decreto Presidencial Núm. 388, de 8 de junio de 2012, sobre la decisión del Consejo Nacional de Defensa y Seguridad de 25 de mayo de 2012 relativa a las actividades para reforzar la lucha contra el terrorismo en Ucrania (párrafo 1); el Decreto Presidencial Núm. 389, de 8 de junio de 2012, sobre la decisión del Consejo Nacional de Defensa y Seguridad de 8 de junio de 2012 relativa a la actualización del Consejo Nacional de Estrategia de Seguridad (apartados 3.1.1, 3.3 y 4.3); y el Decreto Presidencial Núm. 390, de 8 de junio de 2012, sobre la decisión del Consejo Nacional de Defensa y Seguridad de 8 de junio de 2012 relativa a la actualización de la doctrina militar de Ucrania (apartados 7 y 19), tienen los siguientes objetivos:

- Establecer un sistema nacional de ciberseguridad;
- Establecer un sistema nacional unificado para luchar contra la ciberdelincuencia;
- Preparar y aprobar un registro de sitios web cruciales para la seguridad y la defensa nacionales considerados prioritarios en la protección contra ciberataques;
- Redactar y presentar al Parlamento un proyecto de ley sobre ciberseguridad nacional;
- Definir la ciberseguridad como una de las amenazas fundamentales para la estabilidad internacional y la seguridad nacional de Ucrania;
- Aprobar, como meta estratégica y objetivo primario para la política de seguridad nacional, la preparación de normas y reglamentos técnicos nacionales para el uso de las tecnologías de la información y las comunicaciones, y su armonización con las normas correspondientes de los Estados miembros de la Unión Europea;
- Definir el término “ciberterrorismo”;
- Establecer un mecanismo eficaz en Ucrania para responder a las amenazas más nuevas para la seguridad nacional (fenómenos y tendencias que, en ciertas condiciones, podrían poner en peligro los intereses nacionales) relacionadas con el uso de la tecnología de la información en un mundo globalizado, especialmente las “ciberamenazas”;
- Analizar los ciberataques dirigidos contra instalaciones nucleares y químicas, instalaciones de la industria militar y otras ubicaciones potencialmente peligrosas en una muestra de fuerza militar contra Ucrania que pudiera desencadenar un conflicto militar;

2) Los actos normativos y jurídicos del Gabinete de Ministros: Orden Núm. 720-r, de 22 de agosto de 2012, por la que se aprueba la cooperación entre el

Programa Anual Nacional de Ucrania y la Organización del Tratado del Atlántico Norte (OTAN) para 2012, así como la Instrucción Núm. 24066/1/1-12, de 15 de junio de 2012, bajo la Decisión del Consejo Nacional de Seguridad y Defensa antes mencionada relativa al Decreto Presidencial Núm. 388 de 8 de junio de 2012, que también establece la elaboración de un acto legislativo relativo a la ciberseguridad;

3) El Parlamento de Ucrania está examinando la posibilidad de redactar legislación para enmendar algunas leyes relativas a la ciberseguridad nacional. Estos proyectos de ley establecen, entre otras cosas, el empleo en la legislación nacional de conceptos tales como "ciberseguridad del Estado", "sitios críticos de la infraestructura", "sitios críticos de la infraestructura de la información" y "ciberespacio", y la definición de las ciberamenazas primarias para la seguridad nacional, las principales esferas de la política del Estado y las tareas de las entidades responsables de la seguridad nacional en este ámbito.

3. Aprobación de marcos internacionales destinados a fortalecer la seguridad mundial de los sistemas de información y telecomunicaciones

Ucrania cuenta con un marco jurídico y normativo para proteger los datos de los sistemas de información y telecomunicaciones cuyos principios y enfoques relativos a la estructura de la protección están armonizados con la norma de la Organización Internacional de Normalización ISO 15408: Criterios comunes para la evaluación de la seguridad de las tecnologías de la información.

Dado que la delincuencia informática ha aumentado hasta superar las fronteras nacionales y se ha convertido en un fenómeno internacional, Ucrania coopera permanentemente con los organismos extranjeros del orden público.

Además, Ucrania trabaja para garantizar la seguridad de la información a escala internacional en proyectos y programas realizados en colaboración con la Organización para la Seguridad y la Cooperación en Europa, la Asamblea Parlamentaria del Consejo de Europa, la Asociación para la Paz de la OTAN y el Consejo de Europa, así como en el contexto de acuerdos bilaterales.

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

Debido a la índole transnacional de la delincuencia informática, puede ser el momento de elaborar un conjunto de principios internacionales destinados a fortalecer la seguridad de las redes de información y telecomunicaciones y la política de seguridad internacional en su conjunto, así como de mejorar las formas, los medios y los recursos para detectar, evaluar y prever amenazas a la seguridad de la información.

Uno de los principales ámbitos de seguridad de la información a nivel mundial está relacionado con la elaboración y aprobación de instrumentos jurídicos internacionales que permitan eliminar la terminología imprecisa sobre la seguridad de la información. Un aspecto importante de ello sería determinar la condición jurídica del ciberespacio y consagrar, en instrumentos jurídicos y normativos, la

jurisdicción de los Estados en relación con los componentes nacionales de ese espacio (comparable con el espacio aéreo y las aguas territoriales de los Estados) además de impulsar la regulación de cuestiones relacionadas con la ciberguerra y la ciberagresión, entre otras.

Otro aspecto fundamental de la definición de normas en este ámbito sería la aprobación de un concepto unificado de ciberdelincuencia, así como una clasificación clara de los delitos correspondientes.

Otras medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a nivel mundial podrían incluir la armonización del marco jurídico y normativo de protección de la información; la formulación de criterios y métodos convenidos para evaluar la eficacia de los sistemas y recursos de seguridad de la información; el reconocimiento de los certificados de seguridad de la información de otros países; y la mayor cooperación para ocuparse de cuestiones de investigación, técnicas y jurídicas relacionadas con la seguridad de la información. Al mismo tiempo, para lograr el éxito, es crucial intensificar la cooperación entre los organismos nacionales del orden público a fin de prevenir, suprimir y enjuiciar delitos informáticos.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[16 de mayo de 2013]

El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con satisfacción la oportunidad de responder a la resolución 67/27 de la Asamblea General, titulada "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional".

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

En el presente documento, el Reino Unido utilizará de preferencia el término "ciberseguridad" y conceptos conexos, que denotan los esfuerzos encaminados a conservar la confidencialidad, la disponibilidad y la integridad de la información en el ciberespacio. El término "seguridad de la información" es utilizado con frecuencia por empresas y organizaciones de normalización con el mismo significado y también es aceptado en el Reino Unido con este significado concreto. Aun así, puede existir cierto margen de confusión en el uso del término "seguridad de la información", ya que algunos países y organizaciones lo emplean como parte de una doctrina que considera la información propiamente dicha una amenaza frente a la cual se necesita protección adicional. El Reino Unido no reconoce la validez del término "seguridad de la información" cuando se emplea en ese contexto, ya que podría utilizarse para intentar legitimar controles a la libertad de expresión más allá de lo convenido en la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos.

El ciberespacio es un ámbito que ofrece grandes oportunidades, pero también plantea amenazas reales y posibles. Más de 2.000 millones de personas están conectadas ya al ciberespacio a través de Internet, número que continuará creciendo a medida que las tecnologías móviles permitan a los países en desarrollo aprovechar

sus enormes ventajas a menor costo. Internet aporta un motor para el crecimiento económico, abre el acceso a la educación, refuerza la interacción y el entendimiento entre las personas, rompe barreras culturales y geográficas, permite prestar servicios en línea y refuerza la democracia haciendo que los gobiernos rindan cuentan a sus ciudadanos de maneras innovadoras y dinámicas. Por ejemplo:

- Las actividades basadas en Internet ya ascienden al 8% del producto interno bruto del Reino Unido. Garantizar que las empresas y los clientes se sientan seguros cuando hacen negocios en el ciberespacio es crucial para el crecimiento económico.
- El Reino Unido puso en marcha en 2011 un servicio de peticiones electrónicas que permite a cualquier persona presentar o firmar una petición sobre una cuestión cuya responsabilidad corresponde al Gobierno. Todas las peticiones que consiguen 100.000 firmas o más se someten a debate en el Parlamento. En el primer año, se presentaron más de 15.600 peticiones, de las cuales 10 superaron el umbral de las 100.000 firmas. Todas ellas se han debatido o se han incluido en el calendario del Parlamento.

El Reino Unido, como muchos otros países, depende del ciberespacio en numerosas esferas de servicios nacionales cruciales, como la energía, las finanzas y el transporte. Si estos servicios sufren fallos importantes, ya sea accidentales o como resultado de intrusiones deliberadas, podrían provocar graves trastornos, daños económicos o pérdida de vidas.

El panorama de las amenazas es complicado y dinámico. Los sistemas gubernamentales del Reino Unido, al igual que los de empresas y ciudadanos privados, son objeto de intentos de intrusión cotidianos. Los motivos abarcan el espionaje político e industrial, la ciberdelincuencia, los trastornos provocados o el control de las redes, o la negación de servicio. Los responsables abarcan desde Estados nación, intermediarios de Estados, agentes no estatales y bandas de delincuencia organizada, hasta personas que actúan de manera oportunista. La interconexión del ciberespacio implica que las actividades que causan trastornos en un sistema pueden tener efectos no deseados e imprevisibles en otros. Los intentos de contrarrestar esas amenazas se ven obstaculizados por la dificultad de atribuir de manera fiable un ciberincidente a una fuente concreta, el potencial de que los perpetradores se oculten tras una identidad falsa, la poca madurez en la comprensión de lo que constituye un comportamiento aceptable del Estado en el ciberespacio, la escasa resiliencia de la ciberinfraestructura en algunos países, y la ausencia de enfoques armonizados internacionales para detectar, perseguir y enjuiciar a los ciberdelincuentes.

Todos los integrantes de la sociedad tienen su papel y sus obligaciones para combatir estas amenazas. Corresponde a los gobiernos dirigir los esfuerzos internacionales para mejorar la comprensión de lo que constituye un comportamiento aceptable del Estado y hacer frente a la ciberdelincuencia pero, dado que la mayor parte de la infraestructura del ciberespacio es propiedad de empresas privadas y está operado por ellas, su participación en el debate es crucial. El Reino Unido considera que la ciberseguridad no debe mejorar a expensas de los beneficios económicos y sociales que ofrece el ciberespacio. Es especialmente importante velar por que los esfuerzos por aumentar la ciberseguridad no se desvíen para imponer nuevas restricciones a la libertad de expresión más allá de las

permitidas en los acuerdos internacionales. En este sentido, la función de las organizaciones de la sociedad civil cobra especial importancia.

Esfuerzos adoptados a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en esta esfera

Enfoques nacionales

La estrategia de seguridad nacional del Reino Unido, publicada en 2010, clasificó los ciberataques como una de las cuatro amenazas de "nivel 1", junto con las crisis militares internacionales, los accidentes o peligros naturales graves y los atentados terroristas. En noviembre de 2011, el Reino Unido publicó una estrategia actualizada de ciberseguridad, que establece la visión de extraer un enorme valor económico y social de un ciberespacio vibrante, resiliente y seguro, donde nuestras acciones, guiadas por nuestros valores básicos de libertad, justicia, transparencia y estado de derecho, mejoren la prosperidad, la seguridad nacional y una sociedad fuerte. La consecución de esta estrategia se apoya en cuatro objetivos:

- Ocuparse de la ciberdelincuencia y ser uno de los lugares más seguros del mundo para hacer negocios en el ciberespacio
- Aumentar la resiliencia a los ciberataques y tener más capacidad para proteger nuestros intereses en el ciberespacio
- Ayudar a modelar un ciberespacio abierto, estable y vibrante que el público del Reino Unido pueda utilizar con seguridad y que brinde apoyo a sociedades abiertas
- Disponer de los conocimientos, las aptitudes y la capacidad intersectoriales necesarias para apoyar todos nuestros objetivos en materia de ciberseguridad

Como apoyo al logro de estos objetivos, el Gobierno del Reino Unido asignó 650 millones de libras esterlinas de gastos adicionales a un programa cuatrienal destinado a transformar la respuesta a las ciberamenazas.

El Reino Unido ha invertido en capacidades únicas y exclusivas para proteger sus redes y servicios básicos, así como para profundizar su comprensión de las amenazas a que se enfrenta. A su vez, este mayor conocimiento le permite mejorar las prioridades y los objetivos de las iniciativas de defensa. Bajo los auspicios del Ministerio de Defensa del Reino Unido, ha establecido una dependencia de triple servicio destinada a formular nuevas tácticas, técnicas y planes para proporcionar capacidades militares en respuesta a amenazas sofisticadas. El Gobierno colabora estrechamente con las víctimas de ciberactividades que provocan trastornos y el resultado de esa labor le permite brindar asesoramiento a la industria para mejorar las medidas de ciberseguridad. En lo que respecta a sus propias redes, está desarrollando un nuevo modelo de seguridad para compartir servicios, entre los que figuran una autenticación más sofisticada de los empleados, mejor vigilancia del cumplimiento y una mayor resiliencia de la red.

El Gobierno del Reino Unido ha invertido en fortalecer las capacidades de aplicación de la ley y enjuiciamiento para prevenir, interrumpir e investigar ciberdelitos y llevar a los responsables ante la justicia. La Dependencia Central de Ciberdelincuencia de la Policía ha triplicado su tamaño, se han establecido tres equipos de cibervigilancia regionales y se ha elaborado capacitación sobre la lucha contra la ciberdelincuencia para agentes de policía. El Organismo contra la

Delincuencia Organizada Grave se fusionará con la Dependencia Central de Ciberdelincuencia a finales de 2013 para constituir la Dependencia Nacional de lucha contra la Ciberdelincuencia del Organismo Nacional contra la Delincuencia, un nuevo paso hacia la mejora de la capacidad de mantenimiento del orden público del Reino Unido contra la ciberdelincuencia.

La industria del Reino Unido es la mayor víctima de la ciberdelincuencia, incluida la extendida práctica de robo de la propiedad intelectual. El Gobierno colabora con la industria y el sector académico para promover la conciencia sobre la necesidad de hacer frente a las ciberamenazas y, en 2012, elaboró un documento de orientación para los altos ejecutivos de la industria en la que indicaba la manera en que estos debía adoptar estrategias para proteger sus activos de información más valiosos. Además, el Gobierno ha culminado satisfactoriamente una iniciativa experimental de intercambio de información destinada a establecer una plataforma fiable para que las organizaciones compartan información sobre amenazas actuales e incidentes en la gestión. En ella participaron en torno a 160 empresas de los sectores de defensa, finanzas, farmacéutico, energía y telecomunicaciones.

En colaboración con la industria, el Gobierno del Reino Unido se ha dedicado activamente a sensibilizar a la industria y el público sobre la amenaza, de manera que adopten medidas, que con frecuencia son sencillas, para protegerse y exigir mayor seguridad en los productos y servicios electrónicos. Entre estas iniciativas figuran “Get Safe Online Week” (Semana sobre la protección en línea, en colaboración con la Unión Europea y el Canadá), campañas concretas sobre el fraude en línea puestas en marcha por el Organismo Nacional Antifraude y la campaña “The Devil’s in your details” (el problema está en tus detalles) en 2012.

El Reino Unido está invirtiendo en capacidades e investigación para mantenerse al día con este problema en el futuro. Las ocho primeras universidades del Reino Unido en realizar investigaciones en el ámbito de la ciberseguridad han sido clasificadas centros de excelencia académicos en investigación sobre ciberseguridad. Se está elaborando material de enseñanza interactivo para los alumnos más jóvenes y se ha puesto en marcha un plan de aprendizaje técnico para detectar y desarrollar talentos entre los estudiantes de nivel escolar y universitario. Para velar por que quienes trabajan en la esfera de la ciberseguridad reciban la educación y la capacitación adecuadas, un plan de certificación para profesionales de la seguridad de la información ayudará al Gobierno y a la industria a contratar a profesionales del ámbito de la ciberseguridad con las habilidades adecuadas y el nivel necesario para los puestos de trabajo correspondientes.

Enfoques internacionales

El Reino Unido se ha situado en la vanguardia de los esfuerzos internacionales encaminados a mejorar la transparencia, la previsibilidad y la estabilidad del ciberespacio. En noviembre de 2011, el país organizó la primera Conferencia Internacional sobre el Ciberespacio, que reunió a representantes de más de 60 países y de empresas y organizaciones de la sociedad civil para debatir sobre las formas de ampliar los beneficios económicos y sociales del ciberespacio, la cooperación para hacer frente a la ciberdelincuencia, el acceso seguro y fiable a Internet, y la seguridad internacional. El impulso generado por esa reunión continuó en la Conferencia celebrada en 2012 en Budapest y ya se está planificando la Conferencia de 2013, que tendrá lugar en Seúl.

El Reino Unido es un miembro activo del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y del grupo de trabajo oficioso de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre el establecimiento de medidas de fomento de la confianza para el ciberespacio.

En octubre de 2012, el Reino Unido anunció una iniciativa para crear un centro para la creación de capacidad mundial sobre ciberseguridad, con una financiación de 2 millones de libras esterlinas anuales, que incluirá diversas iniciativas multilaterales y bilaterales. Ese centro ofrecerá a otros países asesoramiento independiente y conocimientos especializados sobre la manera de construir infraestructuras nacionales más seguras y resilientes, y de transformarse en coordinadores de investigación de primera categoría y para la colaboración internacional en esta cuestión vital.

Con objeto de impulsar las iniciativas mundiales destinadas a hacer frente a la ciberdelincuencia internacional, el Reino Unido sigue promoviendo el Convenio sobre la Ciberdelincuencia y sus principios como el instrumento más eficaz en esta esfera. El Organismo contra la Delincuencia Organizada Grave continúa liderando, junto con asociados internacionales, la representación mundial de cuestiones de orden público ante la Corporación para la Asignación de Nombres y Números en Internet.

Conceptos internacionales pertinentes destinados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones

El concepto principal es el de la aplicación del derecho internacional y las normas de conducta vigentes que rigen las relaciones entre los Estados. El Reino Unido cree firmemente que esos principios se aplican con la misma fuerza al ciberespacio y la afirmación sin ambigüedades por los Estados de que sus actividades en el ciberespacio se regirán por esas leyes y normas sentará las bases para un ciberespacio más pacífico, previsible y seguro.

A este respecto, el ciberespacio presenta desafíos particulares como, por ejemplo, las dificultades para atribuir las actividades de manera fiable, la evaluación de la intención y la función de los agentes no estatales. El Reino Unido recibiría con agrado la celebración de deliberaciones internacionales sobre la manera de aplicar el derecho internacional y las normas de conducta de los Estados en este contexto.

El Reino Unido no cree que los intentos de concluir tratados multilaterales amplios, códigos de conducta o instrumentos similares hagan una contribución positiva a la mejora de la ciberseguridad en un futuro previsible. La índole compleja y amplia de cualquier acuerdo vinculante para todo un ciberespacio que evoluciona a “velocidad de Internet” significa que no podría ser eficaz ni recibir apoyo generalizado sin muchos años, posiblemente decenios, de ardua labor en materia de normas de conducta y medidas de fomento de la confianza para generar el entendimiento y la confianza necesarios entre los signatarios, y para asegurar que pueden pedirse cuentas de manera fiable sobre el cumplimiento de los compromisos contraídos. La experiencia en la celebración de esos acuerdos sobre otras materias muestra que solamente podrán ser significativos y eficaces como culminación de esfuerzos diplomáticos por llegar a entendimientos y enfoques compartidos, no como punto de partida. El Reino Unido considera que los esfuerzos de la comunidad

internacional deberían centrarse en desarrollar un entendimiento común sobre el derecho y las normas internacionales, en lugar de negociar instrumentos vinculantes que solamente provocarían la imposición parcial y prematura de un enfoque a un ámbito que, en la actualidad, es demasiado inmaduro para aceptarla.

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

La inexistencia de fronteras en el ciberespacio supone un imperativo especial para que los Estados mejoren la cooperación bilateral, regional y multilateral a fin de establecer respuestas comunes a amenazas comunes. En opinión del Reino Unido, las medidas que podrían contribuir de manera más significativa en esta etapa son las siguientes:

a) Deliberaciones continuas entre los Estados a fin de crear un marco normativo para un comportamiento estatal aceptable sobre la base de los principios vigentes del derecho internacional y las normas internacionales consuetudinarias;

b) Formulación de medidas de fomento de la confianza para el ciberespacio encaminadas a aumentar la transparencia y la previsibilidad del comportamiento de los Estados, reduciendo así el riesgo de percepciones erróneas o de una escalada no deseada de incidentes;

c) Establecimiento por los Estados de equipos de respuesta a emergencias cibernéticas como coordinadores de la gestión de incidencias y el intercambio de información, complementados por la notificación de puntos de contacto claves y mecanismos fiables de comunicación en caso de crisis;

d) Realización de ejercicios conjuntos para verificar los procedimientos comunes de comunicaciones y gestión de incidentes;

e) Formulación de enfoques jurídicos armonizados para hacer frente a la ciberdelincuencia;

f) Diálogo intensificado con representantes de empresas y de la sociedad civil para asegurar enfoques coordinados y prioritarios en un ámbito cuya propiedad y funcionamiento están principalmente en manos del sector privado;

g) Compromisos de los Estados cuyas capacidades en materia de ciberseguridad son más maduras para apoyar la creación de capacidad en otros Estados.