Naciones Unidas A/68/156/Add.1

Asamblea General

Distr. general
9 de septiembre de 2013
Español
Original: inglés

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

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

Informe del Secretario General

Adición **

Índice

* A/68/150.
** La información que figura en el presente informe se recibió después de la publicación del informe principal.

13-47548X (S)

II. Respuestas recibidas de los gobiernos

Armenia

[Original: inglés]

[5 de julio de 2013]

El concepto de seguridad de la información se aprobó por medio del Decreto núm. NK-97 del Presidente de la República de Armenia, de 25 de junio de 2009. En este Decreto se establece que la seguridad nacional de la República de Armenia depende considerablemente de la seguridad de la información, la cual abarca componentes como los sistemas de información, comunicaciones y telecomunicaciones. Este concepto también incluye una evaluación general de los problemas de seguridad de la información de la República de Armenia, así como de los retos y amenazas actuales y sus causas y peculiaridades, además de métodos para afrontarlos en distintas esferas de la vida pública.

Se creó un comité intergubernamental encargado de coordinar la aplicación de programas relacionados con el concepto de seguridad de la información.

El concepto sobre la "formación de la sociedad cibernética" se aprobó mediante una Decisión del Gobierno de la República de Armenia el 25 de febrero de 2010. Se creó el Consejo de Gobernanza Electrónica de la República de Armenia y se definió el alcance general de la seguridad cibernética en el marco del concepto sobre la "formación de la sociedad cibernética". En el anexo 4 del concepto se establecen las actividades orientadas a garantizar la seguridad cibernética del Estado. Se formaron un comité y un grupo de expertos a nivel estatal con el fin de intentar conseguir los objetivos mencionados.

También se adoptaron las medidas siguientes a escala nacional con objeto de reforzar la seguridad de la información.

De conformidad con el Decreto del Gobierno núm. 479-N, de 30 de abril de 2009, se creó y está en funcionamiento un centro especial de comunicaciones que se ocupa de la seguridad de Internet. Este centro vela por la seguridad de la información pública de los organismos gubernamentales publicada en Internet y por la conexión segura de los sistemas de información de dichos organismos a Internet.

A principios de 2012, el grupo de expertos elaboró un proyecto de programa nacional sobre la creación de un sistema de seguridad cibernética en la República de Armenia. El proyecto de programa está siendo debatido por el Gobierno de Armenia.

En 2006, la República de Armenia ratificó el Convenio sobre la Ciberdelincuencia, abierto a la firma en Budapest en 2006, y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en 2012. El Servicio de Seguridad Nacional y la Policía de la República de Armenia son los organismos gubernamentales competentes que aplican las disposiciones de dichos convenios. En la actualidad, el grupo intergubernamental de expertos está llevando a cabo actividades encaminadas a armonizar la legislación nacional pertinente con el Convenio.

La República de Armenia promueve la cooperación activa en materia de seguridad cibernética en el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE). Actualmente, la delegación armenia participa en las negociaciones en el marco del grupo de trabajo oficioso para elaborar un conjunto de medidas de fomento de la confianza sobre la seguridad cibernética.

La delegación armenia ha incluido una iniciativa con siete medidas complementarias en la esfera de la defensa cibernética en su Plan de Acción Individual de la Asociación 2011-2013, que se está aplicando en cooperación con la Organización del Tratado del Atlántico Norte.

Canadá

[Original: inglés]

[3 de septiembre de 2013]

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, el Canadá quisiera compartir con el Secretario General sus opiniones y evaluaciones sobre las cuestiones siguientes.

1. Seguridad de la información

Al Canadá le preocupan las amenazas reales y crecientes que plantean las actividades cibernéticas malintencionadas y reconoce que hacer frente a este tipo de actividades requiere cooperación a escala nacional, regional e internacional.

El Canadá tiene un interés estratégico en preservar un ciberespacio abierto, dada su importancia para la prosperidad del país, la seguridad y los valores de la democracia y los derechos humanos. Los sectores público y privado del Canadá dependen de una infraestructura de información segura, resistente y estable para llevar a cabo sus operaciones diarias. Los sistemas informáticos, junto con sus conexiones a Internet y redes, constituyen la columna vertebral de gran parte de la infraestructura esencial del Canadá, que incluye a los sectores energético, financiero, industrial y de telecomunicaciones y los sistemas de información del Gobierno. El buen funcionamiento de la infraestructura esencial respalda nuestra forma de vida y el bienestar económico, político y social del Canadá.

Ámbito nacional

Desde 1996, el Gobierno del Canadá ha reconocido que los sistemas de vital importancia para gestionar la infraestructura esencial del Canadá podrían ser objeto de ataques cibernéticos y que el Gobierno debe intervenir para proteger estos sistemas de dichos ataques. Desde entonces, el Gobierno ha tomado medidas. Tras examinar su capacidad para evaluar y reducir las vulnerabilidades en la infraestructura, desarrolló y aplicó un enfoque de gran alcance dirigido a proteger la infraestructura esencial del Canadá mediante alianzas, y vigiló y analizó los ataques y amenazas cibernéticos contra los sistemas del Gobierno federal. En 2010, el Gobierno anunció su Estrategia y Plan de Acción Nacionales para la Infraestructura Esencial y hace unos meses su Plan de Acción 2010-2015 para la Estrategia de Seguridad Cibernética del Canadá, que pretende asegurar los sistemas del Gobierno,

establecer alianzas que protejan los sistemas cibernéticos fuera del Gobierno federal y ayudar a los canadienses a usar Internet de forma segura.

Ámbito internacional

Desde 2007, el Canadá ha sido uno de los principales contribuyentes al Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA), que ayuda a los Estados de América a prevenir y vigilar las amenazas cibernéticas y responder a ellas potenciando la planificación y coordinación a nivel nacional y también la cooperación regional. A través de su Programa de Fortalecimiento de Capacidades Contra el Terrorismo, el Canadá ha ayudado a varios Estados miembros de la OEA a desarrollar sus propias estrategias nacionales de seguridad cibernética y a incorporarse a la Red Hemisférica de Equipos de Respuesta a Incidentes de la OEA.

Desde 2012, el Canadá y otros Estados participantes de la Organización para la Seguridad y la Cooperación en Europa (OSCE) han trabajado con miras a desarrollar medidas de fomento de la confianza y de la seguridad para reducir los riesgos de percepción errónea, escalada y conflicto que puedan derivarse del uso de las tecnologías de la información y las comunicaciones.

El Canadá también participa activamente en iniciativas internacionales de lucha contra la ciberdelincuencia en varios foros, entre ellos el Grupo de los Ocho, la Oficina de las Naciones Unidas contra la Droga y el Delito y la OEA. Asimismo, el Canadá participó en las actividades más recientes del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (2012-2013).

2. Conceptos internacionales

El derecho internacional convencional y consuetudinario en vigor es aplicable al uso de las tecnologías de la información y las comunicaciones por parte de los Estados y es esencial para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. Entre el derecho internacional vigente en relación con el ciberespacio figuran la Carta de las Naciones Unidas, el derecho internacional de los derechos humanos y el derecho internacional humanitario. Al Canadá le ha complacido comprobar que, en el informe más reciente del Grupo de Expertos Gubernamentales de las Naciones Unidas, los Estados afirman claramente la aplicabilidad del derecho internacional en el ciberespacio como piedra angular de las normas y principios para un comportamiento estatal responsable.

El Canadá también considera que abordar la seguridad de las tecnologías de la información y las comunicaciones debe ir de la mano del respeto de los derechos humanos y las libertades fundamentales, como el derecho a expresar opiniones sin ser molestados, así como los derechos a la libertad de expresión, asociación y reunión y al respeto de la intimidad. El derecho a la libertad de expresión se establece en la Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos. Estos instrumentos disponen que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija.

3. Medidas posibles para fortalecer la seguridad de la información en todo el mundo

El Canadá trabaja estrechamente con asociados internacionales, entre ellos importantes organizaciones multilaterales y asociaciones del sector privado, con el fin de fortalecer la seguridad de la información en las redes de las que dependen la prosperidad económica y la seguridad del Canadá. El Canadá también está intensificando la colaboración y compartiendo información con algunos de sus asociados principales y dentro de organizaciones multilaterales sobre la seguridad cibernética.

El Canadá ha desarrollado un nuevo proceso para coordinar una respuesta nacional a los incidentes cibernéticos más importantes y lograr que los propietarios y operadores de su infraestructura esencial desarrollen y apliquen su propia estrategia de seguridad cibernética.

Entre otros países existe un interés generalizado por mejorar la seguridad cibernética y prevenir la ciberdelincuencia. El principal instrumento internacional que se ocupa específicamente de la ciberdelincuencia es el Convenio del Consejo de Europa sobre la Ciberdelincuencia, que el Canadá firmó en 2001. Este documento, también conocido como Convenio de Budapest, sirve como orientación para elaborar legislación nacional de gran alcance contra la ciberdelincuencia y como marco para la cooperación internacional entre los Estados.

Alemania

[Original: inglés]

[25 de junio de 2013]

Evaluación general de los temas relacionados con la seguridad de la información

No solamente se está produciendo la digitalización de las interacciones económicas, administrativas y privadas, sino que también se está acelerando. Esta circunstancia ofrece oportunidades sin precedentes tanto a los países industrializados como a los países en desarrollo. Al mismo tiempo, la creciente dependencia de las tecnologías de la información y las comunicaciones genera vulnerabilidades y deficiencias sistémicas. Asimismo, existe una nueva interconexión por parte de todos los agentes, desde el usuario particular hasta las empresas y las organizaciones gubernamentales. Con respecto a los ataques cibernéticos, la tendencia avanza claramente hacia actividades malintencionadas más sofisticadas como, por ejemplo, las amenazas persistentes avanzadas o el *software* maligno muy sofisticado, que persiguen objetivos de gran valor. Estas actividades se rigen por el interés en conseguir beneficios o información sobre, respectivamente, el control de activos, sistemas e infraestructuras esenciales con graves consecuencias para gobiernos, numerosas empresas y organizaciones, entre ellos los proveedores de servicios críticos de infraestructura. Las actividades malintencionadas sofisticadas son especialmente difíciles de detectar. La velocidad de la innovación suele aventajar a los intentos de proteger las tecnologías existentes. Un hecho que agrava los riesgos es que los instrumentos y métodos malintencionados se puedan obtener con relativa facilidad, ya que se encuentran a la venta en el mercado negro o no reglamentado. No es posible proteger nuestros entornos actuales de tecnologías de la información

solamente mediante los enfoques convencionales de seguridad de las tecnologías de la información.

Delincuentes sumamente profesionales dedican considerables medios técnicos y financieros a detectar las deficiencias existentes en los sistemas de tecnologías de la información y las comunicaciones y aprovechan esas deficiencias para sus propios fines. La dificultad de establecer una atribución fiable y las oportunidades resultantes para los "ataques de falsa bandera" plantean nuevos riesgos a la seguridad nacional e internacional, en particular a través de malentendidos y errores de cálculo. Las intrusiones dirigidas a conseguir información en un principio no suelen parecer distintas de las que tienen fines destructivos. Esto aumenta aún más el riesgo de percepciones erróneas sobre los ataques recibidos y su posible vulneración de la prohibición del uso de la fuerza en las relaciones internacionales.

La ambigüedad imperante en torno a qué normas aplicar en el ciberespacio crea una situación todavía más imprevisible.

Los sistemas de control de procesos para las infraestructuras esenciales han demostrado ser especialmente vulnerables a las operaciones malintencionadas de las tecnologías de la información y las comunicaciones. Los riesgos de que se produzcan daños colaterales incontrolables a escala mundial son elevados, como la infección de sistemas de control industrial con efectos que podrían ocasionar daños materiales. Un solo ataque cibernético contra la infraestructura básica de telecomunicaciones podría causar más perturbaciones mundiales que un ataque físico.

Independientemente de los diversos grados de capacidad y seguridad de las tecnologías de la información y las comunicaciones de los distintos Estados, a menudo las medidas concretas para aumentar la resistencia se aplazan o se suprimen de la agenda por completo a causa de la incertidumbre que rodea a los riesgos de seguridad cibernética y cómo hacerles frente con eficacia, la complejidad y novedad de los ataques digitales y el secretismo que oscurece los distintos incidentes.

Medidas adoptadas a escala nacional

En 1991 se creó la Oficina Federal para la Seguridad de la Información (*Bundesamt für Sicherheit in der Informationstechnik, BSI*) como principal proveedor de servicios centrales de seguridad de las tecnologías de la información para el Gobierno federal. En esta función, la BSI publica normas mínimas vinculantes en materia de seguridad de las tecnologías de la información para la administración federal y actúa como su oficina central en materia de tecnologías de la información para la notificación de incidentes. Además, opera como oficina neutral para asesoramiento y apoyo en el ámbito de la seguridad de las tecnologías de la información. Los logros principales del trabajo realizado por la oficina fueron, por ejemplo, la norma de gestión de la seguridad de las tecnologías de la información (*IT-Grundschutz*), el equipo de respuesta a emergencias cibernéticas para los organismos federales (*CERT-Bund*) como plataforma para la gestión de incidentes y el intercambio de información (que se remonta a 1994) y el Equipo de Respuesta a Emergencias Cibernéticas de los Ciudadanos (*Buerger-CERT*), creado en 2006, como instrumento para abordar sectores más amplios de la sociedad y concienciar a los ciudadanos. Además, la BSI emite advertencias sobre *software* maligno y vulnerabilidades de la seguridad de productos y servicios de tecnologías de la información, informa a las partes interesadas (incluidos los proveedores de

tecnologías de la información y el público en general) y formula recomendaciones de contramedidas.

Al plan nacional de 2005 para la protección de infraestructuras de la información, que iba dirigido al Gobierno y la industria, le siguió la estrategia de seguridad cibernética adoptada por el Gobierno federal en febrero de 2011. Su base es la protección de infraestructuras críticas.

Desde 2008, el Gobierno alemán y los operadores alemanes de infraestructuras críticas han cooperado en una alianza entre el sector público y el privado. Este "Plan de aplicación de la protección de infraestructuras críticas" (UP KRITIS) mantiene grupos de trabajo para abordar distintos aspectos de la seguridad cibernética, como la gestión de situaciones de crisis, actividades y la disponibilidad de servicios esenciales.

El Centro Nacional de Situación de las Tecnologías de la Información (*Nationales IT-Lagezentrum*), que está administrado por la BSI, realiza un seguimiento de las condiciones de seguridad nacional y mundial de las tecnologías de la información a fin de detectar y analizar con rapidez los principales incidentes de seguridad de las tecnologías de la información y recomendar medidas de protección. En caso de que se produzca una crisis relacionada con las tecnologías de la información, este organismo amplía su capacidad y se convierte en el Centro de Reacción ante Situaciones de Crisis en materia de las Tecnologías de la Información (*Nationales IT-Krisenreaktionszentrum*), que concentra las capacidades para gestionar las crisis de las tecnologías de la información y abarca todos los aspectos nacionales, incluidas las redes gubernamentales y las infraestructuras esenciales.

En consonancia con la estrategia de seguridad cibernética de 2011, todas las autoridades gubernamentales que se ocupan de cuestiones de seguridad cibernética colaboran estrecha y directamente entre sí y con el sector privado en el marco del Centro Nacional de Respuestas Cibernéticas (*Nationales Cyber-Abwehrzentrum*), que está dirigido y albergado por la BSI.

En materia de política, el Consejo Nacional de Seguridad Cibernética (*Nationaler Cyber-Sicherheitsrat*), que tiene nivel de secretaría de Estado, aborda los principales problemas de seguridad cibernética y la posición de Alemania al respecto. Ello incluye la coordinación de la política exterior en materia cibernética, lo que incluye aspectos como política exterior, defensa, economía y seguridad.

Por otro lado, en octubre de 2012 se puso en marcha una plataforma para la cooperación y el intercambio de información a nivel nacional: la Alianza para la Seguridad Cibernética (*Allianz für Cybersicherheit*) facilita la estrecha cooperación entre asociados en los ámbitos económico, académico y administrativo y, en particular, con empresas de interés público especial.

En la actualidad el Plan de aplicación de la protección de infraestructuras críticas se está modernizando después de cuatro años de actividad. Estará abierto a un mayor número de operadores de infraestructuras críticas y creará varios grupos de trabajo en los sectores de las infraestructuras críticas. Asimismo, se iniciará la cooperación con la nueva Alianza para la Seguridad Cibernética.

Las interconexiones internacionales en el ciberespacio imponen como factor esencial una acción coordinada a nivel internacional. Por lo tanto, dentro de la Unión Europea y en los organismos internacionales, Alemania promueve firmemente una mayor seguridad cibernética al mismo tiempo que protege los beneficios sociales y económicos en el ciberespacio.

En su estrategia de seguridad cibernética, dado el carácter de interconexión mundial de las tecnologías de la información, Alemania aboga por que se elaboren normas de conducta del Estado en el ciberespacio, que sean amplias, no contenciosas y políticamente vinculantes. Deben ser aceptables para una gran parte de la comunidad internacional e incluir medidas para fomentar la confianza y aumentar la seguridad.

Medidas de fomento de la confianza y la seguridad en el ciberespacio

El ciberespacio es un bien público y un espacio público. Como tal, la seguridad del ciberespacio se debe considerar en términos de resistencia de la infraestructura, así como protección contra fallos de la integridad y seguridad de los sistemas y los datos que contiene. Al ser un espacio público, los Estados tienen que promover la seguridad en el ciberespacio, en particular en lo que respecta a la protección contra la ciberdelincuencia y las actividades malintencionadas, amparando a quienes optan por utilizar medios de confirmación de autenticidad contra la suplantación de identidad, y asegurando la integridad y la confidencialidad de los datos y las redes.

El ciberespacio es global por naturaleza. La garantía de la seguridad cibernética, la aplicación efectiva de los derechos y la protección de infraestructuras críticas de la información requieren un gran esfuerzo del Estado, a escala nacional y en cooperación con socios internacionales. A escala nacional, Alemania posee una cultura bien definida de cooperación entre numerosos equipos de respuesta a emergencias cibernéticas en todos los organismos económicos, académicos y administrativos. En este contexto, el *CERT-Bund* se ha consolidado como coordinador de contacto para estos equipos. A escala europea e internacional, el *CERT-Bund* coopera estrechamente con un grupo de equipos gubernamentales de respuesta a emergencias cibernéticas, con la red del Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) que es el foro mundial más importante para que los equipos de respuesta a emergencias cibernéticas estén interconectados en el ciberespacio.

En este contexto, Alemania está dispuesta a elaborar un conjunto de normas de conducta que aborden el comportamiento de un Estado hacia otro Estado en el ciberespacio, que incluyan en particular medidas de fomento de la confianza, la transparencia y la seguridad, y velar por que sean suscritas por el mayor número posible de países. Por lo tanto, Alemania participó activamente en el Grupo de Expertos Gubernamentales de 2012/2013 encargado de continuar “examinando las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo…” (Resolución 66/24 de la Asamblea General).

En la conferencia de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre seguridad cibernética, celebrada los días 9 y 10 de mayo de 2011, Alemania señaló algunos posibles elementos de dicho código de conducta basado en normas internacionales, como los siguientes:

Confirmación de los principios generales de disponibilidad, confidencialidad, competitividad, integridad y autenticidad de los datos y las redes, y privacidad y protección de los derechos de propiedad intelectual;

Respeto de la obligación de proteger las infraestructuras críticas;

Mejora de la cooperación, con miras a fomentar la confianza, adoptar medidas de reducción del riesgo y promover la transparencia y la estabilidad, mediante:

i) El intercambio de estrategias nacionales, mejores prácticas y percepciones nacionales referentes a la reglamentación internacional del ciberespacio;

ii) El intercambio de puntos de vista nacionales acerca de las normas jurídicas internacionales relativas al uso del ciberespacio;

iii) La configuración y notificación de puntos de contacto;

iv) El establecimiento de mecanismos de alerta temprana y el fortalecimiento de la cooperación, entre otras cosas, entre los equipos de respuesta ante emergencias informáticas;

v) La actualización de los enlaces de comunicación en situaciones de crisis, para abarcar los incidentes cibernéticos, y el apoyo a la elaboración de recomendaciones técnicas que promuevan infraestructuras cibernéticas mundiales resistentes y seguras;

vi) La responsabilidad de luchar contra el terrorismo, que incluye el intercambio de prácticas y una mayor cooperación para hacer frente a los actores no estatales;

vii) La asistencia para la creación de capacidad en materia de seguridad cibernética en los países en desarrollo, y el establecimiento de medidas voluntarias en apoyo de la seguridad cibernética para acontecimientos de gran escala.

En este sentido, Alemania presentó un documento de posición al Grupo de Expertos Gubernamentales de las Naciones Unidas en julio de 2012. Acogemos con gran satisfacción las recomendaciones formuladas por los expertos sobre las normas, reglas o principios de conducta responsable de los Estados y las medidas de fomento de la confianza en el ciberespacio, así como la importancia que los expertos conceden a un enfoque de la seguridad cibernética basado en la participación de las diversas partes interesadas.

En 2011 y 2012, Alemania respaldó proyectos sobre seguridad cibernética internacional y medidas de fomento de la seguridad y la confianza, desarrollados por el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) y el Instituto de Investigaciones sobre la Paz y Políticas de Seguridad de la Universidad de Hamburgo. La primera Conferencia Cibernética de Berlín, celebrada en diciembre de 2011, proporcionó una plataforma para el debate internacional sobre los riesgos, las estrategias y el fomento de la confianza en la seguridad cibernética internacional. La segunda Conferencia Cibernética de Berlín, celebrada

en septiembre de 2012, se centró en Internet y los derechos humanos. Una de las conclusiones principales fue que la seguridad, la libertad y la privacidad en línea son conceptos complementarios. Alemania también contribuyó a la Conferencia sobre Seguridad Cibernética de 2012 del UNIDIR, celebrada en Ginebra los días 8 y 9 de noviembre de 2012, que se centró en medidas de fomento de la confianza para asegurar la estabilidad cibernética.

Por otra parte, percibimos la necesidad de iniciar un debate sobre una cooperación internacional en el marco de la atribución de los ataques cibernéticos, habitualmente difíciles de rastrear, la responsabilidad del Estado por los ataques cibernéticos lanzados desde su territorio, cuando los Estados no hacen nada para poner fin a estos ataques a pesar de estar informados acerca de ellos, y la responsabilidad de los Estados de no permitir zonas de ilegalidad en el ciberespacio, por ejemplo, tolerar a sabiendas el almacenamiento de datos personales recogidos ilegalmente en su territorio.

Los días 27 y 28 de junio de 2013, la tercera Conferencia Cibernética de Berlín, centrada en el tema de "Asegurar la libertad y la estabilidad del ciberespacio: el papel y la importancia del derecho internacional" y organizada por la Oficina Federal de Relaciones Exteriores en estrecha cooperación con la Universidad de Potsdam, trató de ofrecer evaluaciones jurídicas internacionales de operaciones cibernéticas que no traspasan el umbral de ataque armado y que por tanto no vulneran el derecho sobre conflictos armados. De acuerdo con las normas y los principios internacionales vigentes, los Estados son responsables de las acciones de quienes dentro de su esfera de control perjudiquen a la seguridad y estabilidad de las tecnologías de la información y las comunicaciones. Todos los Estados deberían plantearse formas de minimizar o suprimir la actividad cibernética malintencionada que se origine en su esfera de control o que viaje por sus redes. Los Estados son responsables de la actividad cibernética internacionalmente ilícita que se les pueda atribuir, como la actividad internacionalmente ilícita en el ciberespacio de cualquier representante respaldado por el Estado que actúe según las instrucciones de este o bajo su dirección o control, de conformidad con las normas vigentes de responsabilidad estatal en el marco del derecho internacional consuetudinario. Los Estados deben tomar todas las medidas necesarias para cerciorarse de que sus territorios no son utilizados por otros Estados o por agentes no estatales con el propósito de usar las tecnologías de la información y las comunicaciones de forma ilegal contra otros Estados y sus intereses. Estas medidas necesarias deberían incluir los correspondientes marcos legislativos y normativos nacionales que se precisan para cumplir con las responsabilidades internacionales. La actividad cibernética internacionalmente ilícita puede afectar a los Estados principalmente de tres formas: 1) como países de origen de actividad cibernética malintencionada con posibles efectos dañinos; 2) como países de tránsito, cuyas infraestructuras de tecnologías de la información y las comunicaciones sirven de instrumento para actividades cibernéticas malintencionadas; y 3) como países afectados, donde se producen los daños causados por actividades cibernéticas malintencionadas. En todas estas situaciones, los Estados están obligados a actuar con la diligencia debida, que puede ser de naturaleza material y procesal, y puede abarcar desde la prevención, es decir, el período que precede al daño potencial, hasta la contención, es decir, el comienzo de la actividad cibernética perjudicial en curso, y el seguimiento, esto es, el período posterior a la ejecución de la actividad cibernética malintencionada.

Seguridad cibernética en la Organización para la Seguridad y la Cooperación en Europa

La Organización de la Seguridad y la Cooperación en Europa analiza los problemas de la seguridad cibernética desde hace varios años. En la Cumbre de la OSCE celebrada en 2010 en Astaná, los Jefes de Estado y de Gobierno de los 56 Estados participantes en la OSCE subrayaron que se debía lograr una mayor unidad de propósito y de actuación para hacer frente a las nuevas amenazas transnacionales. La Declaración conmemorativa de Astaná mencionó las "ciberamenazas" como una de estas nuevas amenazas transnacionales.

Alemania participó activamente en la Conferencia de la OSCE celebrada en Viena en 2011 en torno al "Análisis del papel de la OSCE en el futuro", sobre un enfoque integral de la seguridad cibernética. En el transcurso de la conferencia, se examinaron recomendaciones concretas para el seguimiento de las actividades de la OSCE. En mayo de 2012, se creó un grupo de trabajo oficioso en virtud de la Decisión núm. 1039 del Consejo Permanente (PC.DEC/1039) y se le encargó elaborar un conjunto de medidas de fomento de la confianza con objeto de mejorar la cooperación, la transparencia, la previsibilidad y la estabilidad interestatales, así como de reducir los riesgos de percepción errónea, de escalada y de conflicto, que puedan derivarse del uso de las tecnologías de la información y las comunicaciones. En junio de 2012, Alemania presentó al grupo un texto oficioso que incluía sugerencias alemanas para un primer conjunto de medidas de fomento de la confianza en el marco de la OSCE. Alemania lamenta que no fuera posible alcanzar un consenso para la adopción de este primer conjunto de medidas de fomento de la confianza en el Consejo Ministerial de Dublín en diciembre de 2012, pero le complace que el grupo reanudara su labor en 2013.

Alemania seguirá apoyando activamente los debates de la OSCE sobre un análisis del papel de la OSCE en el ámbito de la seguridad cibernética en el futuro.

Aspectos militares de la seguridad cibernética

A medida que también crece la dependencia de las fuerzas militares respecto de las tecnologías de la información para llegar a dominar hipótesis cada vez más complejas en todos los niveles de mando, la protección de la información y los medios para procesarla se han convertido en una tarea de primer orden.

Sin embargo, en el pensamiento militar, las amenazas a la seguridad de información proceden no sólo de un adversario potencial, en el sentido operativo, que utiliza de armas para la destrucción física de la infraestructura de información, sino también de los usuarios irresponsables, el mal funcionamiento de la tecnología, los delincuentes o simplemente los accidentes.

Por lo tanto, las iniciativas que deben emprenderse van desde sensibilizar a cada usuario y asegurar la fiabilidad de la cadena de oferta de tecnologías de la información, hasta poner en práctica formas de respuesta para defenderse de los ataques cibernéticos y establecer una arquitectura general de las tecnologías de la información que sea resistente.

En esencia, es necesaria una gestión integral del riesgo, con medidas para reforzar la seguridad de la información a escala nacional y global.

Las fuerzas armadas alemanas (*Bundeswehr*) han establecido arquitecturas de mando y de control resistentes, técnicas y procedimientos de seguridad, así como una organización de seguridad de las tecnologías de la información que integra a todas las secciones de las fuerzas armadas, incluido un equipo de respuesta ante emergencias informáticas independiente, con capacidad para intervenir en caso de perturbaciones críticas del funcionamiento de las tecnologías de la información. Adaptar las aptitudes personales y técnicas al constante aumento del nivel de la amenaza es una tarea permanente.

Las fuerzas armadas alemanas colaboran estrechamente con el Ministerio del Interior Federal de Alemania en sus iniciativas, y apoyan firmemente el fortalecimiento de la seguridad de la información en la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea y la formación de políticas y mejor coordinación de capacidades a ese efecto. Además, las fuerzas armadas mantienen intercambios regulares con un número de países en el contexto de seguridad de la información a escala normativa y operativa.

Las fuerzas armadas alemanas acogen con satisfacción las iniciativas y trabajan en conjunto con otros departamentos del Gobierno Federal de Alemania sobre propuestas internacionales para proteger aún más la utilidad de las redes de información en el plano mundial; por ejemplo, la elaboración de un código internacional de conducta en el ciberespacio, de carácter voluntario.

Defensa del espacio cibernético en la OTAN

La OTAN ha determinado que la seguridad del espacio cibernético es uno de los nuevos ámbitos que surgen en materia de amenazas a la seguridad. El concepto estratégico adoptado por los Jefes de Estado y de Gobierno en la Cumbre de la OTAN celebrada el 20 de noviembre de 2010 en Lisboa indica que “los ciberataques pueden llegar a un umbral que amenace la prosperidad, la seguridad y la estabilidad nacional y euroatlántica”.

De conformidad con lo dispuesto en la Declaración de la Cumbre, los Ministros de Defensa de la OTAN aprobaron una política de esta Organización sobre la defensa cibernética y un plan de acción de defensa cibernética en junio de 2011. Desde entonces, la OTAN ha aplicado el plan de acción ininterrumpidamente.

La política se centra en la protección de las redes de la OTAN y las redes nacionales de los Estados miembros que están conectadas a las redes de la OTAN o procesan información de esta Organización para sus funciones básicas (lo que incluye la elaboración de principios y criterios comunes para garantizar un nivel mínimo de defensa del ciberespacio en todos los Estados miembros). Para reducir los riesgos globales que proceden del espacio cibernético, la OTAN tiene la intención de cooperar con los países socios, los órganos internacionales pertinentes, como las Naciones Unidas y la Unión Europea, el sector privado y los círculos académicos.

Alemania celebra el compromiso de la OTAN en materia de seguridad cibernética y apoya activamente las deliberaciones al respecto.

República Islámica del Irán

[Original: inglés]

[7 de junio de 2013]

Según la República Islámica del Irán, el uso de las tecnologías y medios de información y telecomunicaciones presenta numerosas oportunidades para todos los Estados y la humanidad en su conjunto. Hoy en día la información y las telecomunicaciones son partes esenciales de las sociedades modernas. Son recursos de importancia decisiva para la riqueza y la prosperidad de las naciones. El Irán considera que se debe hacer todo lo posible, a escala nacional e internacional, para facilitar que todas las naciones utilicen de la forma más amplia posible las tecnologías y medios de información y telecomunicaciones y asegurar que esas tecnologías y medios sigan figurando entre los principales impulsos del desarrollo en todas las sociedades.

Sin duda, el logro de este noble objetivo depende, en gran medida, de que se garantice el pleno respeto por el derecho soberano de cualquier Estado en el ámbito de la información y las telecomunicaciones, lo que incluye el desarrollo, la adquisición, el uso, la importación y la exportación de las tecnologías y medios de información y telecomunicaciones y los servicios conexos, además del acceso a ellos, sin ninguna restricción o discriminación. De hecho, garantizar la disponibilidad, fiabilidad, integridad y seguridad constantes de la información y crear un entorno de información y telecomunicaciones seguro redunda en beneficio de todas las naciones y, por lo tanto, resulta de suma necesidad. Es un hecho innegable que la adopción de cualquier medida que deniegue o restrinja la transferencia de conocimientos técnicos, tecnologías y medios de información y telecomunicaciones, además de la provisión de servicios de información y telecomunicaciones, a los países en desarrollo tendría efectos perjudiciales para su desarrollo global y por tanto debería evitarse.

Al mismo tiempo, las tecnologías y medios de información y telecomunicaciones ofrecen la posibilidad de ser utilizadas para fines ilegales, incluso para perjudicar a las infraestructuras e intereses sociales, culturales, económicos, políticos y de seguridad de los Estados. Por un lado, la creciente dependencia de las sociedades de la disponibilidad de información y la infraestructura de telecomunicaciones, y por otro, la explotación de las tecnologías y medios de información y telecomunicaciones para fines ilegales, en particular por parte de delincuentes y terroristas, lo que incluye el terrorismo de Estado, demuestra las vulnerabilidades existentes y los efectos de gran magnitud de cualquier posible amenaza derivada de la información y las telecomunicaciones. En consecuencia, es fundamental que se adopten todas las medidas jurídicas, técnicas y de infraestructura convenientes a nivel nacional para fortalecer la seguridad de las tecnologías y medios de información y telecomunicaciones y para impedir que se usen con fines ilegales.

No obstante, debido al carácter complejo y las singularidades de las tecnologías y medios de información y telecomunicaciones, como son el espacio sin fronteras, el dinamismo, el anonimato, la velocidad y los rápidos avances tecnológicos, así como la creciente interconexión entre las redes básicas de información y telecomunicaciones, parece que resulta imposible garantizar la seguridad de la información y las telecomunicaciones simplemente mediante la

adopción de medidas nacionales. Por este motivo, y teniendo en cuenta que en muchos países cada vez se dan más casos de uso de estas tecnologías y medios con fines ilegales, todos los Estados deberían actuar en el ámbito nacional y cooperar en el plano internacional.

Al tiempo que observa los esfuerzos constantes de las Naciones Unidas y otras organizaciones internacionales en las cuestiones relacionadas con la información y las telecomunicaciones, la República Islámica del Irán opina que el mecanismo internacional más apropiado para considerar los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional consiste en iniciar un proceso en el marco de las Naciones Unidas con la participación equitativa de todos los Estados. El Irán cree firmemente que la finalidad principal de ese proceso debería ser desarrollar un entendimiento común entre los Estados sobre la importancia de potenciar la seguridad de la información y las telecomunicaciones, la naturaleza, el alcance y la gravedad de las amenazas a las tecnologías y medios de información y telecomunicaciones, y hallar maneras y medios para prevenir esas amenazas. Un proceso de este tipo puede conducir a la adopción de un programa de acción que establezca las medidas necesarias que deben tomar los Estados Miembros y que se desarrolle mediante la celebración de conferencias internacionales cada cinco años para producir resultados políticos que abarquen desde declaraciones hasta códigos de conducta. Sin embargo, el objetivo final de ese proceso debería ser el desarrollo progresivo de una sólida base jurídica internacional que refuerce y garantice la seguridad de la información y las telecomunicaciones en todo el mundo y prevenga el uso de las tecnologías y medios de información y telecomunicaciones con fines ilegales.

Según la República Islámica del Irán, la consideración de las cuestiones relacionadas con los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional debería llevarse a cabo sobre la base de los siguientes principios y elementos:

a) Como principio general, el derecho internacional es aplicable y, por lo tanto, debe aplicarse al uso de las tecnologías y medios de información y telecomunicaciones por parte de los Estados. Por esta razón, al usar estas tecnologías y medios, los Estados deben respetar los propósitos y principios de las Naciones Unidas y sus obligaciones con arreglo a su Carta, en particular el artículo 2, párrafo 3, relativo a dirimir controversias internacionales por medios pacíficos; la prohibición contemplada en el artículo 2, párrafo 4, de recurrir a la amenaza o al uso de la fuerza en cualquier forma incompatible con los propósitos de las Naciones Unidas; y la prohibición establecida en el artículo 2, párrafo 7, de la intervención e interferencia en los asuntos internos de los Estados;

b) Nada deberá menoscabar el derecho soberano de los Estados en el ámbito de la información y las telecomunicaciones, lo que incluye el desarrollo, la adquisición, el uso, la importación y la exportación de conocimientos técnicos, tecnologías y medios de información y telecomunicaciones y los servicios conexos, además del acceso a ellos, sin restricción o discriminación alguna. En consecuencia, los Estados deberían abstenerse seriamente de adoptar medidas que denieguen o restrinjan la transferencia de conocimientos técnicos, tecnologías y medios de información y telecomunicaciones, así como la provisión de servicios de información y telecomunicaciones, a los países en desarrollo.

c) Garantizar que la seguridad de la información y las telecomunicaciones a escala nacional sea responsabilidad exclusiva de cada uno de los Estados. No obstante, debido al carácter mundial de la información y las telecomunicaciones, se debe instar a los Estados a cooperar en la prevención de las amenazas resultantes del uso malintencionado de las tecnologías y medios de información y telecomunicaciones;

d) Se debe respetar plenamente el derecho a la libertad de expresión. Al mismo tiempo, bajo ninguna circunstancia debe ejercerse este derecho de manera que contravenga los propósitos y principios de las Naciones Unidas, las leyes nacionales y los principios de protección de la seguridad nacional, el orden público, la salud pública o la moralidad y la decencia;

e) Los Estados son responsables de las actividades internacionalmente ilícitas relativas al uso de las tecnologías y medios de información y telecomunicaciones que les sean claramente atribuibles;

f) Crear un entorno de información y telecomunicaciones seguro en beneficio de todas las naciones debe ser el principio rector más importante y, en consecuencia, los Estados deben abstenerse, independientemente de las circunstancias, del uso de las tecnologías y medios de información y telecomunicaciones con fines hostiles, restrictivos o cualquier otro fin ilegal, como el desarrollo y uso de armas de información; de socavar o desestabilizar sistemas políticos, económicos o sociales de otros Estados o erosionar sus valores culturales, morales, éticos o religiosos; y la difusión transfronteriza de información en contravención del derecho internacional, incluidos la Constitución y los reglamentos de la Unión Internacional de Telecomunicaciones, o la legislación nacional de los países afectados;

g) Los Estados deben concienciar a los ciudadanos, a escala nacional e internacional, sobre la necesidad de preservar y mejorar la seguridad de la información y las telecomunicaciones mediante el uso responsable de las tecnologías y medios pertinentes, con el objeto de desarrollar una cultura común internacional de seguridad de la información y las telecomunicaciones.

Japón

[Original: inglés]

[12 de agosto de 2013]

Evaluación general de los temas relacionados con la seguridad de la información

El Japón opina que el ciberespacio sirve como infraestructura básica para las actividades socioeconómicas de los sectores público y privado. El ciberespacio facilita el crecimiento económico, el empleo y el desarrollo, además de la democracia y la protección de los derechos humanos, asegurando el flujo libre de información y la libertad de expresión de este. El uso del ciberespacio resulta esencial para la vida de las personas y se ha impuesto a escala global.

Al mismo tiempo, existe una necesidad creciente de proteger la privacidad y los derechos de propiedad intelectual y velar por la seguridad del ciberespacio a fin de disfrutar plenamente de los beneficios del “lado positivo” del ciberespacio. Además,

se han producido ataques electrónicos en todo el mundo y se han convertido en amenazas mundiales transnacionales. Estos ataques pueden llevarse a cabo por medio de diversas entidades y métodos desde cualquier parte del mundo. No es posible que un país por sí solo haga frente al creciente número de delitos y ataques cibernéticos; la cooperación de la comunidad internacional, incluidos los Estados e interesados pertinentes, es fundamental para afrontar estos retos.

Sobre la base de estas perspectivas, el Japón se esfuerza por crear un ciberespacio seguro y fiable centrándose principalmente en proteger la libertad del flujo de información y la libertad de expresión, al tiempo que presta la debida atención al equilibrio entre la protección de la privacidad y la garantía de la seguridad.

Medidas a escala nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera

Medidas a escala nacional para fortalecer la seguridad de la información

Los riesgos que afectan al ciberespacio se han agravado recientemente, y el mantenimiento de la seguridad cibernética se ha convertido en un objetivo importante, con respecto a nuestra seguridad nacional y nuestra gestión de situaciones de crisis y prosperidad social y económica, además de la seguridad y la paz de la población japonesa.

En este contexto, el Japón elaboró una estrategia de seguridad cibernética en junio de 2013, que abarca el período de 2013 a 2015. Con esta estrategia, el país tomará medidas para aumentar la seguridad de la información de los organismos del Gobierno y las infraestructuras críticas y para reforzar la capacidad de adoptar contramedidas contra los ataques cibernéticos.

En concreto, el Japón ha incorporado las siguientes medidas a la estrategia: promover el intercambio de información relativa a los ataques cibernéticos con alianzas entre el sector público y el privado; mejorar los conocimientos básicos sobre seguridad de la información no solamente en el caso del Gobierno y los diferentes sectores económicos, sino también de la población japonesa; concienciar sobre la seguridad cibernética; fortalecer la capacidad de adoptar contramedidas contra los ataques cibernéticos mediante la cooperación internacional; y aumentar nuestra contribución a la elaboración de normas internacionales relacionadas con la seguridad cibernética.

Medidas a escala nacional para contribuir a la cooperación internacional

En relación con el desarrollo de normas internacionales sobre el uso del ciberespacio, debemos empezar de forma inmediata a elaborar normas de conducta realistas y viables que aborden los problemas actuales de forma jurídicamente no vinculante a fin de afrontar el desafío del rápido avance de las tecnologías cibernéticas. El Japón seguirá participando de forma activa en estas medidas en los foros internacionales.

En cuanto a las medidas de fomento de la confianza, el Japón participa activamente en consultas bilaterales con Estados interesados y en diálogos regionales, como el Foro Regional de la ASEAN, con el objetivo de mejorar la transparencia y promover el intercambio de información. Igualmente, con la idea de no generar deficiencias de seguridad en el ciberespacio, el Japón está prestando asistencia en la creación de

capacidad a países en desarrollo en Asia, Oceanía y África; por ejemplo, creando y reforzando equipos de respuesta a emergencias cibernéticas. El Japón también está promoviendo el intercambio de información a escala internacional impulsando la coordinación con los equipos de respuesta a emergencias cibernéticas de otros Estados. El Japón considera que estas medidas contribuyen a fomentar la confianza con los Estados interesados.

Contenido de los conceptos mencionados en el párrafo 2 de la resolución 67/27

El Japón considera que el derecho internacional vigente, en particular la Carta de las Naciones Unidas y el Derecho internacional humanitario, es aplicable al uso del ciberespacio. Sin embargo, dadas las características singulares de las tecnologías de redes de información y comunicaciones, es necesario examinar más a fondo la forma en que se aplicarían las normas y los principios específicos.

Considerando el importante papel que ha desempeñado el Derecho internacional para conseguir estabilidad jurídica y previsibilidad en la comunidad internacional, creemos que definir y aclarar cómo se aplica el derecho internacional vigente al ciberespacio complementaría la elaboración de normas internacionales específicas sobre el ciberespacio y también contribuiría a crear un ciberespacio estable.

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

Normas internacionales para el uso del ciberespacio

No existen normas internacionales que regulen los ataques cibernéticos o el espionaje cibernético en los ámbitos económico, social y de la seguridad. Además, la validez de las normas jurídicamente vinculantes en el ciberespacio sigue siendo poco clara por ahora. Es difícil determinar el panorama futuro del ciberespacio en este momento, ya que la tecnología cibernética se desarrolla a gran velocidad. Por otra parte, llegar a un consenso sobre normas jurídicamente vinculantes llevará mucho tiempo. Por lo tanto, con respecto al carácter jurídico de las normas, el Japón considera que es importante empezar por debatir la creación de normas de conducta generales no vinculantes.

Medidas de fomento de la confianza

Ya que una acumulación de medidas de fomento de la confianza entre los Estados puede favorecer el desarrollo de normas internacionales, la comunidad internacional debe seguir promoviendo estas medidas. A la hora de promover medidas de fomento de la confianza, es necesario garantizar la transparencia y el intercambio de información; sin embargo, el grado de las medidas adoptadas varía de un Estado a otro, ya que cada Estado tiene autoridad para determinar dicho grado a su disposición. Por ello, es necesario promover el intercambio de información a través de marcos a nivel mundial como los ya existentes bajo los auspicios de las Naciones Unidas y los marcos regionales.

Países Bajos

[Original: inglés]

[7 de agosto de 2013]

Los Países Bajos acogen con gran satisfacción la oportunidad de ofrecer su respuesta a la resolución 67/27.

Evaluación general de los temas relacionados con la seguridad de la información

Los Países Bajos manifiestan su apoyo a la seguridad y fiabilidad de las tecnologías de la información y las comunicaciones, y subrayan la necesidad de proteger una red Internet libre y abierta, en el respeto de los derechos humanos. Esto es esencial para nuestra prosperidad y bienestar, pues esas tecnologías actúan como catalizador del crecimiento económico sostenible.

El ciberespacio ofrece oportunidades, pero también hace que nuestras sociedades sean más vulnerables. El carácter transfronterizo de las amenazas subraya la necesidad de la cooperación internacional. Muchas de las medidas sólo serán eficaces si se aplican o están coordinadas en el plano internacional. En ese sentido, los Países Bajos consideran muy importantes las asociaciones de los sectores público y privado, el acercamiento a través de medidas de fomento de la confianza y la concienciación sobre la responsabilidad individual de todos los usuarios de las tecnologías de la información y las comunicaciones.

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

Los Países Bajos trabajan a escala nacional e internacional para crear un entorno digital seguro. A escala nacional, los Países Bajos aplican la estrategia nacional de seguridad cibernética, titulada “La fuerza a través de la cooperación”. Esta estrategia se actualizará en 2013 y su publicación está prevista para la segunda mitad de 2013. La estrategia revisada abordará una visión general del ciberespacio, que tendrá en cuenta las oportunidades económicas, la apertura, las libertades y la seguridad.

Los Países Bajos disponen de un Consejo Nacional de Seguridad Cibernética encargado de garantizar un enfoque de colaboración entre el sector público, el sector privado y las instituciones académicas y de investigación, y de asesorar a las personas responsables de tomar decisiones de alto nivel en la campo de la seguridad cibernética. Asimismo, disponen del Centro Nacional de Seguridad Cibernética para identificar las tendencias y las amenazas y ayudar a abordar los incidentes y crisis. El centro tiene tres funciones: analizar las amenazas cibernéticas sobre la base de la información de las partes públicas y privadas; responder ante amenazas e incidentes cibernéticos; y la coordinación operativa de las situaciones de crisis en el ámbito de las tecnologías de la información y las comunicaciones. El Centro integra al actual equipo de respuesta a emergencias cibernéticas del Gobierno. Durante el último año, ha ampliado su capacidad y ha entablado relaciones sólidas con centros clave de intercambio y análisis de la información. La conferencia internacional organizada anualmente por el Centro Nacional de Seguridad Cibernética reúne a expertos procedentes de gobiernos, empresas privadas, organismos encargados del cumplimiento de la ley y ámbitos técnicos para intercambiar mejores prácticas. Los

Países Bajos han aplicado un conjunto esencial de medidas encaminadas a mejorar la seguridad cibernética y están dispuestos a compartir los modelos que han utilizado con terceros países.

Un ejemplo de alianza entre los sectores público y privado que se está usando en el sector de la seguridad nuclear son las reuniones técnicas organizadas por el Gobierno, en las que la industria nuclear pudo indicar sus necesidades en el campo de la seguridad de la información. El Gobierno aprovechó esta información para la "amenaza basada en el diseño". Las palabras clave son "realista" y "proporcionalidad".

A escala internacional, los Países Bajos contribuyen activamente a los esfuerzos de la Unión Europea, la Organización del Tratado del Atlántico Norte (OTAN), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro para la Gobernanza de Internet y otras alianzas. Los Países Bajos valoran positivamente la Comunicación conjunta de la Comisión Europea y la Alta Representante para Asuntos Exteriores y Política de Seguridad, que insta a la creación de un ciberespacio abierto, libre y seguro para la Unión Europea y que ha sido respaldada por el Consejo Europeo. La Unión Europea asume este reto con sus asociados y organizaciones internacionales, el sector privado y la sociedad civil. Los Países Bajos apoyan plenamente los objetivos de la Unión Europea de proteger Internet al tiempo que se promueve la apertura y la libertad en Internet, promover la creación de medidas de fomento de la confianza y normas de conducta y aplicar el derecho internacional vigente en el ciberespacio. Creemos firmemente que la seguridad y el derecho de acceso son elementos fundamentales en la salvaguardia del desarrollo constante de Internet. Para ello, la Unión Europea ha tomado los valores esenciales, es decir, la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto por los derechos fundamentales, como sus principios rectores. Los Países Bajos respaldan estos valores esenciales y los considera la base de cualquier estrategia de seguridad cibernética. Los Países Bajos están de acuerdo en que, para promover un ciberespacio sólido y adaptable, los sectores público y privado deben desarrollar sus capacidades y trabajar conjuntamente con eficiencia.

En el plano operacional, los Países Bajos promueven la cooperación práctica en los centros de seguridad cibernética (como las organizaciones de equipos de respuesta a emergencias cibernéticas) y el fortalecimiento de la Red de alerta y vigilancia internacional. El rápido crecimiento de la ciberdelincuencia exhorta a velar por una aplicación efectiva de la ley para mantener la confianza en la sociedad digital. En lo que respecta a esa aplicación efectiva, los Países Bajos fomentan una mayor investigación transfronteriza con las autoridades de otros países europeos y de otras regiones. El país ha suscrito el Convenio del Consejo de Europa sobre la Ciberdelincuencia y alienta a otros a adherirse a este Convenio.

En relación con la seguridad de la información nuclear, en la Asociación de Reguladores Europeos de Seguridad Nuclear los Países Bajos comparten información sobre enfoques normativos y mejores prácticas de seguridad nuclear, incluida la esfera cibernética. Los Países Bajos participan activamente en las reuniones del Organismo Internacional de Energía Atómica (OIEA) con el objetivo de compartir información sobre la seguridad cibernética y de la información.

Los Países Bajos creen que la libertad, la transparencia y la seguridad son conceptos que van de la mano y se refuerzan entre sí. Por ese motivo iniciaron la Coalición para la Libertad en Internet (*Freedom Online Coalition*), que en la actualidad ya cuenta con 21 gobiernos miembros. Esta coalición se ha comprometido a promover la libertad de Internet y a subrayar la importancia de los derechos digitales. Para ello, la coalición de gobiernos afines coordina sus esfuerzos y trabaja con la sociedad civil y el sector privado en un proceso de múltiples interesados con miras a respaldar la capacidad de las personas para ejercer sus derechos humanos y libertades fundamentales en Internet. Para avanzar hacia el objetivo de que Internet sea un entorno abierto y libre para todos, los miembros de la coalición crearon la Alianza de Defensores Digitales (*Digital Defenders Partnership*), un fondo dirigido a respaldar soluciones innovadoras para la protección de blogueros y activistas en línea que corren peligro y para la implantación de servicios de emergencia en Internet en países donde Internet no es libre o accesible. La contribución de los Países Bajos a este fondo asciende a un millón de euros para el período comprendido entre el 1 de octubre de 2012 y el 31 de diciembre de 2014.

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

El punto de partida propuesto por los Países Bajos es una Internet abierta que promueva la innovación, estimule el crecimiento económico y proteja las libertades fundamentales. Los Países Bajos destacan la importancia de seguir dialogando sobre la elaboración de normas de conducta del Estado con miras a una utilización segura del ciberespacio. El país está dispuesto a contribuir activamente a este diálogo. Los Países Bajos reconocen la importante labor realizada por distintos agentes e interesados internacionales y regionales, como el Consejo de Europa, la Unión Europea, la OSCE y el Grupo de Expertos Gubernamentales de las Naciones Unidas con respecto a las medidas de fomento de la confianza en el ámbito de la seguridad cibernética.

En el ámbito de la Cumbre de Seguridad Nuclear, la seguridad de la información desempeña un papel fundamental. El Plan de Trabajo de la Cumbre de Seguridad Nuclear celebrada en Washington y el Comunicado de Seúl afirman que los objetivos de los Estados de la Cumbre de Seguridad Nuclear son evitar que agentes no estatales obtengan la información o tecnología necesarias para usar ese material con fines malintencionados y prevenir la perturbación de los sistemas de control basados en las tecnologías de la información en las instalaciones nucleares. Al igual que la Presidencia de la Cumbre de Seguridad Nuclear, los Países Bajos apoyan todas las iniciativas que contribuyan a estos objetivos.

En el marco de la Cumbre de Seguridad Nuclear, los Países Bajos apoyan el liderazgo del Reino Unido de Gran Bretaña e Irlanda del Norte en la aplicación y el intercambio de mejores prácticas de seguridad de la información en el sector nuclear. Esto se consigue mediante la elaboración y el refuerzo de medidas, acuerdos y capacidades nacionales para la gestión eficaz y seguridad de dicha información; la promoción de una cultura de seguridad nacional conexa; la colaboración con las comunidades científica, industrial y académica a nivel nacional para seguir desarrollando y difundiendo mejores prácticas, concienciar al respecto y mejorar el nivel profesional; y el apoyo, basándose en el OIEA y colaborando con este organismo, a otras organizaciones internacionales y países asociados fundamentales para facilitar la consecución mutua de estos objetivos. Los Países

Bajos conceden gran importancia a un modelo inclusivo de gobernanza de Internet, que implique al sector privado y las instituciones del conocimiento en este diálogo, y están dispuestos a compartir con otros sus experiencias y mejores prácticas.

Para que el ciberespacio sea más seguro y fiable, y para aprovechar plenamente todo su potencial, tanto con respecto al desarrollo como al acercamiento de las sociedades de todo el mundo, resulta esencial un intenso intercambio internacional de conocimientos e información entre todas las partes interesadas y las organizaciones. Por lo tanto, los Países Bajos acogen con satisfacción las conferencias cibernéticas celebradas en Londres y Budapest y la próxima conferencia que se celebrará en Seúl.

Por último, los Países Bajos opinan que la elaboración de normas de conducta para los Estados no requiere la modificación del derecho internacional, sino que más bien debe asegurar la coherencia en la aplicación de los marcos jurídicos internacionales vigentes. Instamos al diálogo y la reflexión constantes para llegar a un consenso sobre el efecto práctico de la aplicación del Derecho internacional y las normas vigentes al ciberespacio.

Omán

[Original: árabe]

[26 de junio de 2013]

El Ministerio de Transporte y Comunicaciones desea transmitir la siguiente información relativa a la resolución 67/27 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

1. Evaluación general de los temas relacionados con la seguridad de la información

Los rápidos avances que se han producido en las tecnologías de la información y las telecomunicaciones van acompañados de riesgos cada vez mayores. Los piratas informáticos utilizan técnicas cada vez más avanzadas para acceder a información en todo el mundo. Los retos más importantes que afrontan los Estados y las instituciones son la ausencia o insuficiencia de una cultura de seguridad de la información entre los usuarios de las tecnologías de la información y las comunicaciones, la falta de personal cualificado y las diferencias existentes en la legislación que regula las comunicaciones electrónicas en todo el mundo. Los Estados deben aunar esfuerzos y cooperar para luchar contra las amenazas a la seguridad de la información, mejorar su capacidad de respuesta, concienciar a nivel mundial sobre este problema y compartir la información y los conocimientos especializados pertinentes.

2. Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera

- La Autoridad de Regulación de las Telecomunicaciones fue creada en 2002 y la Autoridad de las Tecnologías de la Información en 2006, con el fin de regular los sectores de las telecomunicaciones y las tecnologías de la información;

- Se ha promulgado la legislación correspondiente, a saber, la Ley de transacciones electrónicas, en virtud del Decreto del Sultán núm. 69/2008, y la Ley reguladora de las telecomunicaciones, en virtud del Decreto del Sultán núm. 30/2002;
- La Unión Internacional de Telecomunicaciones y la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) han creado recientemente el primer centro de seguridad cibernética para la región árabe en Omán;
- A fin de hacer frente a las amenazas y riesgos técnicos, la Autoridad de las Tecnologías de la Información estableció un equipo nacional de respuesta a emergencias cibernéticas en abril de 2010;
- A través de la Autoridad de las Tecnologías de la Información, Omán es miembro de numerosos organismos regionales e internacionales pertinentes, entre ellos el Equipo de Repuesta a Emergencias Cibernéticas de la Organización de Cooperación Islámica (OCI), los Equipos de Respuesta a Emergencias Cibernéticas del Consejo de Cooperación del Golfo (CCG) y el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST). Muchas instituciones omaníes han conseguido la certificación ISO;
- Las instituciones competentes actualizan continuamente sus estrategias;
- Las autoridades gubernamentales tienen acceso a una serie de tecnologías y programas de seguridad de la información;
- Se ha creado un centro para proteger las redes del Gobierno;
- Se han creado servicios de hospedaje que ofrecen medidas de protección para los sitios web del Gobierno;
- Se ofrece apoyo técnico para reforzar la seguridad de la información;
- Se han adoptado varias políticas y normas sobre seguridad de la información;
- Se han celebrado varias sesiones de capacitación de especialistas sobre seguridad de la información;
- Se han organizado diversas campañas de concienciación;
- Se han ejecutado programas encaminados a evaluar la capacidad de respuesta ante emergencias relacionadas con la información;
- Se han convocado varios talleres y conferencias pertinentes a escala regional y mundial;
- Se han celebrado actividades de concienciación a nivel local;
- Todos los sectores de la sociedad han participado en las medidas de promoción de la seguridad de la información;
- En enero de 2012 se puso en marcha el Programa de Embajadores del Equipo Nacional de Respuesta a Emergencias Cibernéticas de Omán orientado a fomentar la seguridad de la información;
- Se ha creado un sitio web para reforzar la seguridad de los niños en Internet (www.cop.gov.om);

- Se han organizado visitas de concienciación a escuelas, universidades, cibercafés y otros lugares frecuentados por jóvenes;
- Se han celebrado talleres dirigidos a concienciar a los estudiantes y el personal docente;
- El Centro ha participado activamente en actos públicos con el fin de llegar a la mayor cantidad de jóvenes posible e informarles de los riesgos de seguridad y las respuestas ante ellos;
- El Centro ha ejecutado programas de capacitación de instructores para dotar a los jóvenes omaníes de las aptitudes profesionales apropiadas;
- Se ha abierto el primer centro de operaciones de seguridad de la información en el Oriente Medio.

3. El contenido de los conceptos

- Omán supervisa y examina constantemente estos conceptos internacionales con el fin de mantenerse informado de las medidas destinadas a reforzar la seguridad de los sistemas de información y telecomunicaciones a nivel mundial.
- Se ha de prestar atención a las características particulares de los países y su legislación referente a las transacciones electrónicas.
- Las partes interesadas deben atenerse a los valores y principios particulares que cada país desea defender.

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

- Regular las transacciones electrónicas y la seguridad cibernética interestatal y de la información estableciendo una organización internacional bajo los auspicios de las Naciones Unidas, como se propuso en la Conferencia sobre defensa cibernética celebrada en Omán en marzo de 2013;
- Promover la cooperación entre los Estados con miras a salvaguardar el sector de las tecnologías de la información y las comunicaciones, del cual dependen en gran medida la mayoría de países en sus esfuerzos por impulsar el desarrollo. Dicha cooperación debe tener lugar bajo los auspicios de una organización internacional;
- Mantener la coordinación entre los Estados con objeto de reforzar la seguridad de la información y compartir experiencias punteras;
- Colaborar en la respuesta ante incidentes de seguridad de la información y designar coordinadores para cada país;
- Participar en la formulación de políticas y reglamentos y compartir mejores prácticas;
- Compartir conocimientos especializados e intercambiar visitas;
- Convocar conferencias y talleres para el personal dedicado a la seguridad de la información;

- Organizar programas internacionales conjuntos que sirvan para concienciar a los ciudadanos y difundir una cultura de seguridad mundial;
- Fomentar la colaboración académica y elaborar programas y planes de estudios apropiados;
- Impulsar y promover programas conjuntos de investigación y desarrollo en este ámbito.

Turquía

[Original: inglés]

[10 de junio de 2013]

Evaluación general de los temas relacionados con la seguridad de la información

La seguridad de la información se ha convertido en una necesidad en el mundo globalizado a medida que crece el uso de las tecnologías de la información. La seguridad de la información y la seguridad cibernética son cuestiones que deben gestionarse con la cooperación de todas las partes relacionadas. En Turquía, la Junta de Seguridad Cibernética, el principal mecanismo encargado de coordinar a las partes relacionadas y realizar los estudios pertinentes, fue creada en virtud de una decisión del Gabinete sobre la ejecución, gestión y coordinación de los estudios nacionales de seguridad cibernética, que se publicó en el Boletín Oficial turco núm. 28447, de 20 de octubre de 2012.

La estrategia y el plan de acción nacionales de seguridad cibernética para 2013 y 2014 se aprobaron el 20 de diciembre de 2012, en la primera reunión de la Junta Nacional de Seguridad Cibernética.

Los objetivos de la estrategia y el plan de acción son los siguientes:

- Establecer una infraestructura que permita la disponibilidad de los servicios, procesos y datos que proporcionan las organizaciones gubernamentales mediante las tecnologías de la información;
- Garantizar la seguridad de los sistemas de información empleados en las infraestructuras críticas administradas por el Gobierno o el sector privado;
- Determinar las medidas estratégicas de seguridad cibernética dirigidas a minimizar los efectos de los ataques cibernéticos y acortar el tiempo de recuperación después de sufrir ataques;
- Constituir una infraestructura que facilite la investigación de delitos cibernéticos por parte de las autoridades judiciales y los organismos encargados del cumplimiento de la ley.

Las esferas principales del plan de acción son las siguientes:

1. Reglamentos;
2. Estudios para facilitar los procesos judiciales;
3. Creación de un equipo nacional de respuesta a emergencias cibernéticas;
4. Fortalecimiento de la infraestructura nacional de seguridad cibernética;

5. Capacitación y concienciación de los recursos humanos sobre la seguridad cibernética;

6. Desarrollo de tecnologías nacionales para la seguridad cibernética;

7. Ampliación de los ámbitos de aplicación de los mecanismos nacionales de seguridad cibernética.

El plan de acción consta de 29 líneas de acción que se llevarán a cabo conforme a las principales esferas mencionadas.

Medidas adoptadas a escala nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera

El organismo regulador nacional de Turquía, la Autoridad de las Tecnologías de la Información y las Comunicaciones (BTK), autorizado en virtud de la Ley de comunicaciones electrónicas (núm. 5809), realiza una serie de actividades para contribuir a las medidas orientadas a cumplir con las obligaciones nacionales e internacionales en materia de seguridad de la información.

En este contexto, se exponen a continuación las actividades de la Autoridad en el campo de la seguridad cibernética.

1. Reglamentación e inspecciones

Varios requisitos de los operadores autorizados se recogen en el reglamento sobre la seguridad de las comunicaciones electrónicas y el comunicado asociado que se fundamenta en este reglamento. Los estudios correspondientes pretenden aumentar el grado nacional de seguridad cibernética de forma directa en las actividades de los operadores y aportar seguridad cibernética internacional implícitamente.

Por otro lado, la Autoridad también dispone de reglamentos sobre la firma electrónica y el correo electrónico certificado en el contexto de la Ley de firma electrónica (núm. 5070) y la Ley de comercio turca (núm. 6112). Estos reglamentos contribuyen a las medidas dirigidas a promover la seguridad y la fiabilidad de los procesos de intercambio de documentos y correo electrónico.

2. Ejercicios de seguridad cibernética

La Autoridad de las Tecnologías de la Información y las Comunicaciones organiza ejercicios de seguridad cibernética para seguir desarrollando la capacidad técnica y administrativa, concienciar a los ciudadanos y crear oportunidades de cooperación internacional.

2.1. Ejercicio nacional de seguridad cibernética 2011

El Ejercicio nacional de seguridad cibernética 2011 se celebró del 25 al 28 de enero de 2011, con la participación de 41 organizaciones públicas, privadas y no gubernamentales que incluyeron a representantes de los sectores financiero, de las tecnologías de la información y las comunicaciones, educación, defensa y sanidad, además de las dependencias judiciales y de ejecución de la ley y varios ministerios. Seis de las organizaciones mencionadas participaron en el ejercicio en calidad de observadores.

2.2 Ejercicio de protección cibernética 2012

Este ejercicio se celebró en mayo de 2012 bajo la coordinación de la Autoridad de las Tecnologías de la Información y las Comunicaciones y con la participación de doce proveedores de acceso a Internet que operan en el sector de las comunicaciones electrónicas. Los participantes fueron las empresas con mayores cuotas de mercado del sector, junto con los proveedores de acceso a Internet móvil de tercera generación (3G). En el ejercicio, los participantes experimentaron sobre todo ataques de denegación de servicio y se evaluó la idoneidad de las medidas de seguridad adoptadas contra los ataques.

2.3. Ejercicio nacional de seguridad cibernética 2013

El ejercicio nacional de seguridad cibernética 2013, que fue organizado por la Autoridad de las Tecnologías de la Información y las Comunicaciones conjuntamente con el Consejo de Investigaciones Científicas y Tecnológicas de Turquía, bajo los auspicios del Ministerio de Transporte, Asuntos Marítimos y Comunicaciones, se llevó a cabo del 24 de diciembre de 2012 al 11 de enero de 2013, con la participación de 61 organizaciones. A pesar de que la mayoría de los participantes eran organizaciones públicas, en el ejercicio también participaron organizaciones privadas y no gubernamentales. Además, el Presidente de la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) de la Unión Internacional de Telecomunicaciones (UIT) y uno de los miembros de la junta del Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST), que son plataformas de cooperación internacional sobre la seguridad cibernética, asistieron al acto de clausura del ejercicio en calidad de oradores.

3. Proyecto sobre la prevención de las amenazas cibernéticas

El proyecto sobre la prevención de amenazas cibernéticas (*Siber Tehditleri Önleme Projesi-STOP*) implica el desarrollo de los mecanismos necesarios para el establecimiento de un sistema trampa destinado a detectar amenazas cibernéticas, la instalación y mejora de un sistema de notificación de ataques cibernéticos y la producción de metadatos sobre amenazas cibernéticas. Las actividades que exige el proyecto se están llevando a cabo según los plazos previstos por el plan de acción nacional de seguridad cibernética a corto plazo. En el contexto de la dimensión de cooperación internacional del proyecto, la Autoridad de las Tecnologías de la Información y las Comunicaciones se convirtió en miembro de la IMPACT, que desarrolla su labor bajo la dirección de la UIT.

4. Proyecto sobre la prevención de correo electrónico no deseado

Este proyecto se llevó a cabo en 2009, bajo la coordinación de la Autoridad de las Tecnologías de la Información y las Comunicaciones y con la participación de proveedores de acceso a Internet y proveedores de servicios de hospedaje de sitios web. El propósito del proyecto era prevenir el envío masivo de correo electrónico no deseado que supone una amenaza para la seguridad de las redes y congestiona los recursos de estas. Al final del proyecto, el número de proveedores de servicios de Internet que difundían correos no deseados se redujo en un 99%; esta mejora se reflejó en los informes elaborados por empresas internacionales de seguridad cibernética.

5. Establecimiento de un punto nacional de intercambio de Internet

La práctica de encaminamiento que adoptan los proveedores de acceso a Internet consistente en repartir innecesariamente el tráfico de Internet entre dos extremos desde un punto remoto provoca que disminuya la calidad del servicio debido a demoras de transmisión innecesarias y que aumenten las preocupaciones por la seguridad.

En este contexto, mediante la creación de un punto de intercambio de Internet eficaz y la capacidad de los operadores para intercambiar su tráfico en unas circunstancias más convenientes, se pueden reducir esas prácticas de encaminamiento no deseadas y los problemas de seguridad que conllevan. Por lo tanto, la Autoridad de las Tecnologías de la Información y las Comunicaciones dirige junto con las partes vinculadas (proveedores de acceso a Internet de ámbito nacional y proveedores de contenidos de ámbito internacional) diversas actividades centradas en la creación de un punto nacional de intercambio de Internet que resulte eficaz.

Medidas para fortalecer la seguridad de la información a escala mundial

Creación de un equipo nacional de respuesta a emergencias cibernéticas

Hoy en día es necesario crear una organización de respuesta a incidentes que trabaje con eficacia a escala nacional para detectar la aparición de nuevas amenazas cibernéticas, adoptar las medidas necesarias para reducir o suprimir los efectos de incidentes cibernéticos potenciales y compartir información. Para ello, en febrero de 2013, el Ministerio de Transporte, Asuntos Marítimos y Comunicaciones delegó en la Presidencia de Comunicaciones la misión de establecer y dirigir un equipo de respuesta a emergencias cibernéticas de Turquía y se iniciaron diversas actividades orientadas a crear un equipo nacional de respuesta a emergencias cibernéticas que trabajará las 24 horas del día y los 7 días de la semana contra este tipo de amenazas. El USOM, el equipo de respuesta a emergencias cibernéticas que empezó a funcionar en mayo de 2013, trabajará en estrecha cooperación con los equipos de respuesta a emergencias cibernéticas de otros países y de organizaciones internacionales.

Como resultado del rápido desarrollo y la proliferación de las tecnologías de la información y las comunicaciones, las amenazas contra la seguridad de la información van más allá de las fronteras nacionales. En consecuencia, es fundamental que las organizaciones internacionales y los gobiernos promuevan la cooperación en las cuestiones relativas a la seguridad de la información y pongan en práctica esa cooperación lo antes posible.