Naciones Unidas A/71/172

Asamblea General

Distr. general
19 de julio de 2016
Español
Original: árabe/chino/español/
francés/inglés/ruso

Septuagésimo primer 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

Informe del Secretario General

Índice

* A/71/150.

16-12486 (S) 050816 150816

I. Introducción

1. El 23 de diciembre de 2015, la Asamblea General aprobó la resolución 70/237, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”. En el párrafo 4 de esa resolución, la Asamblea invitó a todos los Estados Miembros, 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/70/174), a seguir 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 promover la cooperación internacional en ese ámbito;

c) El contenido de los conceptos mencionados en el párrafo 3 de esa resolución;

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

2. En cumplimiento de esa solicitud, el 15 de febrero de 2015, se envió una nota verbal a todos los Estados Miembros en que se les invitó a proporcionar información sobre el tema. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en la sección II. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe. El texto completo de todas las respuestas puede consultarse en la siguiente dirección: www.un.org/disarmament/topics/informationsecurity.

II. Respuestas recibidas de los Gobiernos

Albania

[Original: inglés]
[15 de abril de 2016]

La prioridad fundamental de Albania en el ámbito de la seguridad y la protección de la información clasificada es el acuerdo suscrito entre el Gobierno de la República de Albania y la Unión Europea, a saber, el acuerdo sobre los procedimientos de seguridad para el intercambio y la protección de la información clasificada, que fue firmado el 3 de marzo de 2016 en Tirana, y se espera que sea ratificado a su debido tiempo por la Asamblea de la República de Albania.

En el contexto de la puesta en marcha y la aplicación de las medidas pertinentes en Albania para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito, se emprendió un examen de los estatutos jurídicos:

– Decisión núm. 188 del Consejo de Ministros, de 4 de marzo de 2015, “Sobre la aprobación de normas que garantizan la seguridad del personal”

– Decisión núm. 189 del Consejo de Ministros, de 4 de marzo de 2015, “Sobre la seguridad física de la información clasificada como “secreto de Estado” perteneciente a la Organización del Tratado del Atlántico Norte”

– Decisión núm. 190 del Consejo de Ministros, de 4 de marzo de 2015, “Modificaciones y adiciones varias a la decisión núm. 81 del Consejo de Ministros “Sobre la definición de los criterios y procedimientos para destruir información clasificada”’

– Decisión núm. 701 del Consejo de Ministros, de 22 de octubre de 2014, “Sobre la aprobación de normas para asegurar la información clasificada en la zona industrial”

Albania tiene un conjunto más completo de disposiciones jurídicas que abordan la seguridad física de la información clasificada. A esos efectos, las “áreas de seguridad” se han redefinido y ubicado teniendo en cuenta los diferentes niveles de confidencialidad de la información.

Tras la aprobación de la nueva decisión relativa a la seguridad del personal, finalmente se han reforzado la cooperación interinstitucional, la supervisión y la inspección de las instituciones del Estado. Los organismos estatales han puesto en marcha un proceso de revisión de las listas de deberes del personal y expedición de los certificados de seguridad pertinentes según la esfera de responsabilidad.

Con respecto a la seguridad industrial, Albania se ha centrado en examinar la política de seguridad de la información, examinando las prácticas del Consejo de Ministros por decisión núm. 701, de 22 de octubre de 2014.

Otra medida importante en que hemos hecho hincapié ha sido la redacción de una nueva ley sobre la información clasificada, una ley eficaz y actualizada que aplica las normas europeas más rigurosas. El examen de la legislación nacional en esta esfera se lleva a cabo teniendo en cuenta el acervo de la Unión Europea y, en particular, la decisión 2013/488/UE del Consejo sobre las normas de seguridad para la protección de la información clasificada de la Unión Europea.

Australia

[Original: inglés]
[31 de mayo de 2016]

Australia acoge con beneplácito esta oportunidad, en respuesta a la invitación formulada en la resolución 70/237 de la Asamblea General, de proporcionar opiniones sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. La información que aquí se presenta se basa en la proporcionada por Australia en respuesta a las resoluciones 68/243, en 2014, y 65/41, en 2011.

La ciberseguridad está tan intrínsecamente vinculada a la innovación como a la seguridad nacional, y es cimiento de la innovación, el crecimiento y la prosperidad. La ciberseguridad es una oportunidad mundial que los gobiernos, el

sector privado y la comunidad están decididos a lograr y de la que pueden beneficiarse.

La comunidad mundial no debe equivocarse con respecto a la ciberseguridad. Es preciso que todos —los gobiernos, las empresas y los particulares— trabajen de consuno para construir un entorno de confianza en Internet, no solo para proteger la información crítica, sino también para ofrecer el entorno que permita que la innovación florezca, impulsar el avance de la industria tecnológica y aprovechar la creciente necesidad mundial de mejores soluciones, equipo y personas capacitadas en ciberseguridad.

Australia reconoce que una ciberseguridad sólida es fundamental para el crecimiento y la prosperidad en una economía mundial. En 2015, Australia examinó su enfoque de la ciberseguridad y el 21 de abril de 2016 puso en marcha su nueva estrategia en este ámbito.

Australia considera que, como tarea prioritaria, la comunidad internacional debería determinar la forma en que el derecho internacional se aplica al comportamiento de los Estados en el ciberespacio, sobre todo en situaciones en que no hay un conflicto. Es necesario seguir trabajando para llegar a entendimientos sobre la forma en que conceptos fundamentales, como la soberanía y la jurisdicción, se aplican al ciberespacio, teniendo en cuenta nuestro interés común en preservar el carácter mundial de Internet. Hay margen para seguir perfeccionando las normas voluntarias que figuran en el informe de 2015 del Grupo de Expertos Gubernamentales en relación con la protección de la infraestructura crítica, los equipos de respuesta a emergencias cibernéticas, la responsabilidad de los Estados de prestar asistencia, la cooperación en materia de ciberdelincuencia y la prevención de la proliferación de instrumentos y técnicas cibernéticas malintencionadas. Es importante que la labor relativa a las medidas de fomento de la confianza pase a la próxima etapa: de la promoción de la transparencia a la aplicación de medidas de cooperación.

Canadá

[Original: inglés]
[27 de mayo de 2016]

En cuanto a las cuestiones cibernéticas, el Canadá considera lo siguiente:

- Un ciberespacio libre, abierto y seguro es fundamental para la seguridad mundial, la prosperidad económica y la promoción de los derechos humanos, la democracia y la inclusión.
- Cualquier enfoque para hacer frente a las amenazas cibernéticas debe ir de la mano del respeto de los derechos humanos y las libertades fundamentales.
- El derecho internacional vigente se aplica al uso de la tecnología de la información y las comunicaciones por los Estados.
- La promoción de normas en tiempos de paz contribuye a mantener un entorno en el que el comportamiento responsable orienta las acciones de los Estados, sostiene asociaciones y apoya un ciberespacio estable.

- Las medidas prácticas de fomento de la confianza son un método que ha demostrado reducir las tensiones y el riesgo de conflicto armado.

En el plano nacional, desde que publicó su estrategia de ciberseguridad en 2010, el Gobierno del Canadá ha seguido trabajando para ayudar a fortalecer la seguridad de los sistemas cibernéticos del país y proteger a los canadienses conectados a Internet, y ha puesto en marcha la campaña de concienciación pública sobre la ciberseguridad "Get Cyber Safe". En fecha reciente, el Gobierno se comprometió a examinar las medidas vigentes para proteger a los canadienses y a nuestra infraestructura crítica de las amenazas cibernéticas.

En el plano internacional, el Canadá participa activamente de distintas formas en las cuestiones cibernéticas:

- El Canadá seguirá promoviendo la elaboración de normas en tiempos de paz para el comportamiento de los Estados en el ciberespacio, incluidos los documentos finales de los Grupos de Expertos Gubernamentales de las Naciones Unidas de 2012-2013 y de 2014-2015. El Canadá ha sido seleccionado para participar en el Grupo de 2015-2016.
- El Canadá ratificó el Convenio de Budapest en julio de 2015, y alienta a los países a que se adhieran a ese Convenio o lo utilicen como modelo para aplicar sus propias leyes de lucha contra la ciberdelincuencia.
- Desde 2007, el Canadá se ha comprometido a aportar 8,25 millones de dólares para apoyar proyectos de desarrollo de la capacidad en materia de ciberseguridad en América y Asia Sudoriental.
- El Canadá es socio fundador del Foro Mundial de Competencia Cibernética.
- El Canadá está colaborando con los Estados Unidos para armonizar sus iniciativas relacionadas con campañas de concienciación pública sobre ciberseguridad mediante la coalición "Stop. Think. Connect".
- El Canadá también está colaborando con los Estados Unidos para aplicar el plan de acción del Canadá y los Estados Unidos sobre ciberseguridad, que tiene por objeto aumentar la resiliencia de nuestra ciberinfraestructura.
- El Canadá ha venido trabajando para elaborar medidas de fomento de la confianza en diversos foros, entre ellos, la Organización para la Seguridad y la Cooperación en Europa y el Foro Regional de la Asociación de Naciones del Asia Sudoriental.
- El Canadá apoya las iniciativas de la Organización del Tratado del Atlántico Norte (OTAN) para fortalecer la ciberseguridad de la Alianza y de los aliados, y ha aportado 1 millón de dólares al Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN.
- El Canadá ha apoyado el uso de las tecnologías de la información y las comunicaciones (TIC) como instrumento del desarrollo, entre otras cosas para ayudar a las organizaciones comunitarias a prestar servicios esenciales como la asistencia de emergencia en los conflictos.
- El Centro Internacional de Investigaciones para el Desarrollo del Canadá ha contribuido a promover el desarrollo en todo el mundo mediante el uso de las

TIC para las investigaciones relacionadas con el desarrollo y el fomento de la capacidad.

Colombia

[Original: español]
[13 de junio de 2016]

De la mano del Plan “Vive Digital” (2010-2014) y el nuevo “Vive Digital – para la gente” (2014-2018), se ha generado una revolución digital del país que en solo cinco años logró que pasáramos de 2,2 millones de conexiones de Internet a más de 12,2 millones; Colombia es el primer país de Latinoamérica con Internet de alta velocidad que cubrirá todos los municipios del país. En el mismo periodo, se entregaron más de 2 millones de terminales a entidades educativas, logramos que el 74% de las microempresas y pequeñas y medianas empresas se conectaran a Internet (el 7% estaban conectadas en 2010), se logró el 90% de crecimiento en conexión a los hogares, y se llevó Internet al campo y a los lugares más apartados con 7.621 Kioscos Vive Digital (ubicados en centros rurales poblados de más de 100 habitantes). Además, contamos con la comunidad de emprendedores digitales más grande de América Latina, con más de 100.000 participantes, entre otros muchos logros.

El Gobierno Nacional reconoce que no es posible maximizar el aprovechamiento y los beneficios de las tecnologías de la información y las comunicaciones, si los ciudadanos o las empresas no pueden confiar en ellas, esto es, si no tienen una percepción de seguridad en el entorno digital. Esta percepción se ve cada vez más afectada por los crecientes incidentes que se presentan.

a) Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito:

Colombia acaba de emitir una nueva política nacional de Seguridad Digital consignada en el documento CONPES 3854 de 2016, la cual pretende lograr que el Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los individuos, en general, en Colombia, puedan contar con un entorno digital confiable y seguro que maximice los beneficios económicos y sociales, impulsando la competitividad y productividad en todos los sectores de la economía. La política es resultado de un proceso que permitió la participación de múltiples partes interesadas y es una de las primeras políticas nacionales en el mundo —y primera en la región— en acoger las recomendaciones en gestión de riesgos de seguridad digital, emitidas en septiembre de 2015 por la Organización de Cooperación y Desarrollo Económicos.

La política prevé, en primer lugar, que se establecerá un marco institucional claro en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el Gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional. En segundo lugar, se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas, y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos

responsables en el entorno digital. Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. Por último, y no menos importante, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

b) Sobre el contenido de los conceptos mencionados en el párrafo 3 de la resolución 70/237:

Colombia, como miembro del último Grupo de Expertos Gubernamentales (2014-2015), comparte plenamente la necesidad de profundizar en el estudio de los conceptos relacionados con la seguridad de la información y los sistemas mundiales de telecomunicaciones y aspectos relacionados con la aplicación del derecho internacional en el ciberespacio.

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

En concordancia con el punto anterior, compartimos plenamente las importantes recomendaciones emitidas por consenso por los expertos que conformaron el Grupo de Expertos Gubernamentales, que incluyen la adopción voluntaria de medidas y buenas prácticas, así como el desarrollo de capacidades y cooperación por parte de los Estados para promover el uso pacífico de las tecnologías de la información y las comunicaciones, de forma que se mantengan como herramientas de desarrollo económico y social para los países, especialmente para aquellos menos desarrollados tecnológicamente.

Cuba

[Original: español]
[6 de mayo de 2016]

Cuba comparte la preocupación que se expresa en la resolución 70/237 respecto a la posibilidad de que las tecnologías y los medios de información se utilicen con propósitos incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales y afecten negativamente la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar.

Igualmente, dicha resolución enfatiza adecuadamente la necesidad de impedir que los recursos y las tecnologías de la información se utilicen con fines delictivos o terroristas.

En este contexto, Cuba reitera su preocupación por el empleo encubierto e ilegal, por individuos, organizaciones y Estados, de los sistemas informáticos de otras naciones para agredir a terceros países, por sus potencialidades para provocar conflictos internacionales.

El único camino para prevenir y enfrentar estas amenazas y evitar que el ciberespacio se convierta en un teatro de operaciones militares es la cooperación mancomunada entre todos los Estados.

El uso 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 que pudieran afectar la paz y la seguridad internacionales.

Las Jefas y los Jefes de Estado y de Gobierno de América Latina y el Caribe, en la II Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), celebrada en La Habana, en enero de 2014, proclamaron a la región de América Latina y el Caribe como Zona de Paz, entre otros objetivos, para fomentar las relaciones de amistad y de cooperación entre sí y con otras naciones, independientemente de las diferencias existentes entre sus sistemas políticos, económicos y sociales o sus niveles de desarrollo, practicar la tolerancia y convivir en paz como buenos vecinos.

Durante la IV Cumbre de la CELAC, celebrada en Quito, en enero de 2016, se destacó nuevamente la importancia de las tecnologías de la información y comunicaciones, incluida Internet, como herramientas para fomentar la paz, promover el bienestar humano, el desarrollo, el conocimiento, la inclusión social y el crecimiento económico. Igualmente, se reafirmó el uso pacífico de las tecnologías de la información y las comunicaciones de forma compatible con los propósitos y principios de la Carta de las Naciones Unidas y el Derecho Internacional, y nunca con el objetivo de subvertir sociedades o crear situaciones con el potencial de fomentar conflictos entre Estados.

Sin embargo, esos esfuerzos siguen siendo amenazados por las continuadas transmisiones radiales y televisivas del Gobierno de los Estados Unidos hacia Cuba, que contravienen los propósitos y principios de la Carta de las Naciones Unidas y varias disposiciones de la Unión Internacional de Telecomunicaciones, y laceran la soberanía de Cuba.

Mediante transmisiones radiales y televisivas ilegales, se ha estado agrediendo de modo permanente el espacio radioeléctrico cubano, difundiendo programaciones especialmente diseñadas para incitar al derrocamiento del orden constitucional establecido por el pueblo cubano. A modo de ilustración, solo en el primer trimestre de 2016 se transmitieron de manera ilegal contra Cuba, como promedio, 1880 horas semanales a través de 23 frecuencias.

Cuba espera que se ponga fin de inmediato a estas políticas agresivas que resultan, además, incompatibles con el desarrollo de vínculos respetuosos y de cooperación entre Cuba y los Estados Unidos, tal como ambos Gobiernos acordaron al restablecer las relaciones diplomáticas.

También espera que se levante el bloqueo económico, comercial y financiero, que ha causado serios daños al pueblo cubano, con efectos nocivos en el área de la información y las comunicaciones, entre otras esferas de la vida cotidiana del pueblo cubano.

La cooperación internacional es fundamental para enfrentar los peligros del uso indebido de las tecnologías de la información y las comunicaciones. Le corresponde a la Unión Internacional de Telecomunicaciones un importante papel en la discusión intergubernamental sobre las cuestiones de ciberseguridad.

Cuba apoyó la resolución 70/237, y continuará contribuyendo al desarrollo global pacífico de las tecnologías de la información y las telecomunicaciones y a su empleo en bien de toda la humanidad.

El Salvador

[Original: español]
[26 de abril de 2016]

La Fuerza Armada de El Salvador ha renovado el equipo informático de seguridad perimetral, habiendo implementado políticas de seguridad para el acceso a los recursos en la red informática (cambios periódicos de contraseñas de usuario, restricción del acceso a los puertos USB y unidades lectoras de DVD y CD, así como el bloqueo del acceso a la Unidad C de los equipos).

España

[Original: español]
[26 de mayo de 2016]

España considera que las tecnologías de la información y las comunicaciones (TIC) brindan inmensas oportunidades, y que su importancia para la comunidad internacional es cada vez mayor. Sin embargo, existen tendencias preocupantes que generan riesgos para la paz y la seguridad internacionales. Es esencial que exista una cooperación eficaz entre los Estados con el fin de evitar la aplicación de prácticas perjudiciales en el ciberespacio y no permitir deliberadamente que sus territorios sean utilizados para que se cometan hechos internacionalmente ilícitos mediante dichas tecnologías.

En julio 2015, el Consejo Nacional de Ciberseguridad aprobó nueve Planes Derivados del Plan Nacional de Ciberseguridad que desarrollan las diferentes líneas de acción previstas en la Estrategia del Ciberseguridad Nacional de 2013.

España participa activamente en todas las iniciativas de carácter estratégico que afectan a la ciberseguridad en la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa, la Organización del Tratado del Atlántico Norte, el Consejo de Europa y la Organización de Cooperación y Desarrollo Económicos.

En 2015, España ingresó en la Freedom Online Coalition y el Global Forum on Cyber Expertise.

España apoya el documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, adoptado en diciembre 2015.

La mayor conectividad, innovación y acceso a las TIC ha desempeñado una función esencial a los efectos de facilitar los progresos en relación con los Objetivos de Desarrollo del Milenio. España estima necesario que exista una estrecha armonización entre el proceso de la Cumbre Mundial sobre la Sociedad de la Información y la Agenda 2030 para el Desarrollo Sostenible, pues el acceso a las

TIC se ha convertido también en un indicador de desarrollo y en una aspiración en sí y por sí misma.

España defiende el proceso tendente a alcanzar un consenso internacional en materia de ciberseguridad, y considera que los Estados deben seguir profundizando en la interpretación y aplicación de los principios y normas del derecho internacional en el ciberespacio, especialmente los relativos a la amenaza o uso de la fuerza, al derecho humanitario y a la protección de los derechos y libertades fundamentales de las personas.

España apoya las aspiraciones de la comunidad internacional de lograr el uso pacífico de las TIC para el bien común de la humanidad, y considera que la Carta se aplica en su totalidad, manifestando que los Estados tienen el derecho inmanente de adoptar medidas compatibles con el derecho internacional pudiendo ejercer la respuesta oportuna, legítima y proporcionada ante amenazas o agresiones que puedan afectar a su seguridad nacional.

Finlandia

[Original: inglés]
[31 de mayo de 2016]

Finlandia acoge con beneplácito la oportunidad de proporcionar información sobre la resolución 70/237 de la Asamblea General. En el plano nacional, se han adoptado las medidas siguientes:

a) La estrategia nacional de ciberseguridad de Finlandia (2013) y su programa de aplicación (2014) definen directrices y medidas clave para el fortalecimiento de la ciberseguridad y la resiliencia. El programa de aplicación se está actualizando mediante un proceso consultivo en el que participan múltiples interesados, y esa actualización deberá finalizarse en 2016.

b) Desde que se aprobó la estrategia nacional de ciberseguridad, Finlandia ha establecido el Centro Nacional de Ciberseguridad y el Centro de Prevención de la Ciberdelincuencia, y ha nombrado una Embajadora para Asuntos Cibernéticos. En febrero de 2016, se aprobó la estrategia nacional de seguridad de la información.

c) Como parte de su cooperación para el desarrollo, Finlandia apoya diversos proyectos de tecnología de la información y las comunicaciones (TIC) para el desarrollo y de creación de capacidad cibernética, es socio fundador del Foro Mundial de Competencia Cibernética, y se ha sumado a la iniciativa Global Connect, dirigida por los Estados Unidos, que tiene la intención de conectar a Internet a 1.500 millones de personas a más tardar en 2020. Finlandia se propone sumarse al nuevo Digital Development Partnership Trust Fund del Banco Mundial, y apoya la gobernanza de Internet sobre la base de un modelo de múltiples interesados.

d) Finlandia participa activamente en el diálogo internacional sobre cuestiones cibernéticas en los foros multilaterales y regionales, y en sus contactos bilaterales. En el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Finlandia procura fortalecer la confianza, la seguridad y la

estabilidad en el ciberespacio, y aplica las medidas de fomento de la confianza y la seguridad convenidas.

e) Finlandia ha hecho suyo el informe de 2015 del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Ha participado activamente en los debates sobre el derecho internacional en el ciberespacio, por ejemplo, en las consultas sobre el Manual de Tallin 2.0, y los talleres del Instituto de las Naciones Unidas de Investigación sobre el Desarme. Finlandia se sumó a la Coalición para la Libertad de Expresión en Internet en 2012 y contribuye a la Digital Defenders Partnership.

f) Finlandia es parte en el Convenio de Budapest desde 2007. El nuevo plan estratégico de la policía, que destina recursos a la prevención de los delitos informáticos y al desarrollo de conocimientos especializados en ciberseguridad, se puso en marcha en 2015. También existe un plan integral de prevención de la ciberdelincuencia.

Esferas prioritarias en que la comunidad internacional debe seguir trabajando:

a) Finlandia asigna gran importancia a la labor del nuevo Grupo de Expertos Gubernamentales y está decidida a contribuir a su éxito, lo que incluye seguir trabajando en la determinación de normas de comportamiento responsable de los Estados en el ciberespacio, con especial hincapié en las actividades en tiempo de paz;

b) Seguir elaborando y aplicando medidas de fomento de la confianza en el plano regional en el marco de la OSCE;

c) Seguir apoyando el fomento de la capacidad cibernética con miras a fortalecer la resiliencia y la seguridad en el ciberespacio;

d) Finlandia seguirá apoyando y alentando el diálogo entre múltiples interesados. Fortalecer las alianzas público-privadas en los planos nacional e internacional es una prioridad.

India

[Original: inglés]
[9 de junio de 2016]

Si bien la tecnología de la información facilita el crecimiento económico y la conectividad social, hay graves problemas que deben abordarse. El crecimiento del sector de la tecnología de la información y las comunicaciones (TIC) también va acompañado del aumento de las amenazas cibernéticas, que van desde los ataques cibernéticos hasta la ciberdelincuencia, el ciberterrorismo, el espionaje y el blanqueo de dinero. Las pruebas demuestran que los grupos terroristas, como el Estado Islámico en el Iraq y el Levante, utilizan Internet y las plataformas de los medios sociales para sus actividades nefandas, incluidos el reclutamiento, la recaudación de fondos, la propaganda y la radicalización. El uso indebido de los medios sociales es motivo de gran preocupación. Si bien esos medios facilitan una

gran conectividad, también pueden utilizarse indebidamente para avivar la discordia étnica y social.

Es importante que la comunidad internacional llegue a un entendimiento común sobre el comportamiento de los Estados en el ciberespacio, y apruebe las medidas de fomento de la confianza y desarrollo de la capacidad recomendadas en el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas. No se debería permitir que la cuestión de la gobernanza de Internet quedara atascada en debates divisivos sobre cuestiones de semántica. Si bien los diversos interesados tienen un papel que desempeñar en sus respectivos ámbitos de actividad, los gobiernos desempeñan una función primordial en las cuestiones de la ciberseguridad relativas a la seguridad nacional. Es necesario elaborar mecanismos adecuados para el intercambio de información sobre las amenazas cibernéticas, la ciberdelincuencia y el ciberterrorismo. También es preciso que exista cooperación en tiempo real entre los organismos gubernamentales para hacer frente a la ciberdelincuencia. Además, la cuestión de la guerra cibernética, las ciberdoctrinas y su repercusión en la seguridad internacional deberían examinarse en todos los foros internacionales. Si bien aún no se han adoptado normas de comportamiento responsable de los Estados en el ciberespacio, un entendimiento común sobre las medidas de fomento de la confianza que se enumeran en el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas podría utilizarse para adoptar medidas apropiadas a fin de crear capacidad en el ámbito de la ciberseguridad. En este sentido, el marco elaborado por el Foro Mundial de Competencia Cibernética ofrece orientaciones útiles.

La India es una parte interesada importante en el uso de las TIC, apoya la colaboración entre múltiples interesados en la gobernanza de Internet y participa activamente en varios foros internacionales, incluido el Grupo de Expertos Gubernamentales, el Proceso de Consultas de Participación Abierta sobre el Examen General de la Aplicación de los Resultados de la Cumbre Mundial sobre la Sociedad de la Información y la Corporación para la Asignación de Nombres y Números en Internet. En consulta con todos los interesados, la India ha adoptado un enfoque integrado que comprende una serie de medidas normativas, jurídicas, técnicas y administrativas necesarias para responder a las preocupaciones en materia de ciberseguridad y promover la cooperación internacional al respecto. Su marco jurídico está en consonancia con otros existentes en el mundo. La política nacional de seguridad cibernética (2013) se estableció con el propósito de construir un espacio cibernético seguro y resistente para los ciudadanos, las empresas y el Gobierno. Esa política hace hincapié en la creación de capacidad, el desarrollo de aptitudes y el fomento de alianzas público-privadas en el ámbito de la ciberseguridad.

Japón

[Original: inglés]
[27 de mayo de 2016]

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

El Japón considera que el ciberespacio debería ser un lugar en el que se garantizara la libertad sin restricciones innecesarias, y cuyo acceso no se negara ni impidiera a ningún agente sin un motivo legítimo. Nuestros esfuerzos se rigen por los cinco principios siguientes: la libre circulación de la información, el estado de derecho, la apertura, la autonomía y la participación de múltiples interesados.

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito

1. Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información

Sobre la base de la estrategia de ciberseguridad establecida en septiembre de 2015, el Japón procura fortalecer la seguridad de la información.

2. Medidas adoptadas a nivel nacional para fortalecer la cooperación internacional

Los esfuerzos del Japón se sustentan en los tres pilares siguientes: 1) la promoción del estado de derecho en el ciberespacio, 2) el fomento de la confianza, y 3) la creación de capacidad. Con respecto a la promoción del estado de derecho, el Japón contribuye activamente al debate internacional para promover un entendimiento común de que el derecho internacional vigente es aplicable en el ciberespacio, así como para elaborar normas no vinculantes y voluntarias de comportamiento responsable de los Estados. En cuanto al fomento de la confianza, el Japón promueve las medidas al respecto mediante el diálogo bilateral y los marcos multilaterales, como el Foro Regional de la Asociación de Naciones del Asia Sudoriental (ASEAN). En cuanto al desarrollo la capacidad, el Japón participa activamente en la prestación de asistencia y la cooperación técnica para el desarrollo de los recursos humanos, centrando la atención en la región de la ASEAN.

Contenido de los conceptos mencionados en el párrafo 3 de la resolución

La confirmación de la aplicabilidad del derecho internacional y la elaboración de normas no vinculantes y voluntarias de comportamiento responsable de los Estados en el ciberespacio son la base para garantizar la estabilidad y la previsibilidad de la comunidad internacional.

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

Con respecto a la promoción del estado de derecho, el Japón insta a seguir deliberando sobre las normas del derecho internacional en tiempos de paz, el

derecho de legítima defensa y el derecho internacional humanitario, así como elaborando normas voluntarias en el contexto del próximo Grupo de Expertos Gubernamentales. En cuanto a las medidas de fomento de la confianza y desarrollo de la capacidad, es fundamental que cada Estado y región promueva la aplicación de las recomendaciones contenidas en los informes del Grupo. Es necesario estudiar formas que conduzcan a una cooperación tangible.

Jordania

[Original: árabe]
[2 de mayo de 2016]

La tecnología de la información y las comunicaciones se ha vuelto esencial para nuestra vida cotidiana. Promueve el crecimiento social, cultural y económico y el desarrollo de las comunidades locales de diversas maneras, y ofrece numerosas posibilidades para la interacción de las personas con sus comunidades locales y con el resto del mundo.

El avance extraordinariamente rápido de la tecnología de la información y las comunicaciones la hace vulnerable a los riesgos y los problemas. Esos riesgos se deben encarar por las vías jurídica y tecnológica, a fin de hallar soluciones eficaces y prácticas que los reduzcan y evitar consecuencias que puedan ser catastróficas.

El ejército jordano ha desempeñado un papel activo e influyente en la promoción de la seguridad y la paz a los niveles nacional, regional y mundial, perfeccionando la tecnología que emplea para garantizar la seguridad de la información y las comunicaciones alámbricas e inalámbricas. A esos efectos:

a) Ha actualizado sus sistemas de información y comunicaciones mediante la instalación de redes protegidas, que utilizan tecnología de cifrado IP en todo el Reino, en particular en las fronteras, con lo que refuerza la seguridad nacional y regional;

b) Coopera con la comunidad internacional en cuestiones de seguridad utilizando sistemas de comunicaciones que son compatibles con los utilizados por la Organización del Tratado del Atlántico Norte y el ejército de los Estados Unidos, y que cumplen las normas internacionales de cifrado de tipo 1;

c) Ha mejorado su capacidad técnica mediante la adquisición de un sistema de comunicaciones independiente que utiliza para mantener la seguridad nacional en las zonas de conflicto, los campamentos de refugiados y los lugares apartados. El ejército jordano también utiliza esa tecnología en apoyo de las operaciones de mantenimiento de la paz en las zonas de conflicto de todo el mundo;

d) Capacita y certifica a todos los usuarios de los sistemas de comunicaciones y al personal de mantenimiento y apoyo, sin depender de la empresa proveedora, a fin de garantizar una fiabilidad óptima en todo momento;

e) Aplica las normas más altas de control y mando a todos los sistemas utilizados por el ejército, con el fin de elevar el nivel de coordinación y cooperación con respecto a la seguridad en los ámbitos nacional y regional;

f) Participa activamente en las conferencias internacionales y sigue de cerca sus resultados a fin de aumentar la complementariedad entre los ejércitos amigos, evitar la interferencia entre los sistemas de comunicación utilizados por los Estados vecinos en la región, y coordinar el control y la vigilancia de las fronteras internacionales.

Es necesario que siempre se preste atención al conocimiento por los ciudadanos de las amenazas cibernéticas generalizadas y la forma en que la aplicación de medidas de seguridad cibernética al utilizar los sistemas electrónicos puede minimizar o eliminar esas amenazas. Una elevada conciencia de la seguridad en el manejo de todo tipo de información no debe interferir con los beneficios de la tecnología.

Para proteger las redes de información nacional que resultan vitales, se han adoptado las medidas siguientes:

a) El uso de técnicas de cifrado en todos los sistemas de comunicación de voz, datos y vídeo;

b) El uso de redes cerradas (Intranet);

c) La instalación de dispositivos periféricos independientes para el enlace con otros organismos de seguridad;

d) La aplicación de medidas de seguridad de la información y las comunicaciones y del principio de “la necesidad de saber”. La verificación constante de los permisos de acceso y de la identidad de los usuarios;

e) El uso de redes virtuales mediante las cuales los usuarios interactúan con una pantalla vinculada a la red sobre la base de permisos para acceder a la información. La prohibición del acceso o la conexión mediante otros dispositivos, como las memorias USB;

f) La elaboración o aprobación de las disposiciones siguientes en materia de ciberseguridad:

1) Aprobación de la Ley sobre los delitos cibernéticos;

2) Aprobación de la Ley sobre las transacciones electrónicas;

3) Elaboración del proyecto de estrategia nacional de ciberseguridad;

4) Elaboración de proyectos de políticas nacionales de ciberseguridad;

5) Aprobación por el Consejo de Ministros, en 2012, de la estrategia nacional de ciberseguridad.

Proponemos que se adopten las siguientes medidas a nivel mundial:

a) Clasificar las redes de comunicaciones y la información según su importancia;

b) Aplicar medidas de ciberseguridad;

c) Aplicar el principio de la necesidad de saber;

d) Aplicar medidas técnicas, como el cifrado y el salto de frecuencia;

e) Verificar los usuarios y los permisos de acceso a la red y clasificarlos por categoría;

f) Utilizar dispositivos periféricos independientes para conectar las redes;

g) En algunos casos, usar conexiones de Intranet, y evitar el uso de Internet en la medida de lo posible;

h) Mejorar la Intranet de las Naciones Unidas, separarla de las redes públicas, y protegerla con medidas técnicas y de seguridad como el cifrado, las salvaguardias y la verificación de los permisos de acceso;

i) Promover la cooperación entre los equipos de respuesta a emergencias cibernéticas para hacer un seguimiento de las violaciones, instalar salvaguardias y subsanar las deficiencias;

j) Publicar las medidas de seguridad y los procedimientos para enfrentar las violaciones.

Hacemos hincapié en que la tecnología de la información y las comunicaciones puede promover el desarrollo sostenible, especialmente en las zonas más pobres y distantes, de la siguiente manera:

a) Acelerando la erradicación de la pobreza, por ejemplo, a través de la banca móvil, que ha reportado beneficios directos y tangibles a millones de personas de todo el mundo que no tienen experiencia bancaria.

b) Las tecnologías modernas y los nuevos medios de comunicación pueden mitigar los efectos de las hambrunas proporcionando información esencial a los agricultores sobre los cultivos.

Recomendaciones:

a) Se deberían formar equipos internacionales de respuesta y recuperación para hacer frente a los incidentes, las crisis y los desastres en relación con la ciberseguridad;

b) Se debería incluir a un representante de Jordania en el Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional que habrá de crearse en 2016;

c) Se debería incrementar la cooperación en los ámbitos de la ciencia y la investigación y el intercambio en materia de la capacitación entre los miembros del Consejo de Seguridad.

Líbano

[Original: árabe]
[24 de mayo de 2016]

En la era moderna, la ciberseguridad afecta a una diversidad de cuestiones económicas, sociales, políticas, militares y humanitarias. En el futuro, el ciberterrorismo será una de las amenazas más graves para las superpotencias y los Estados en desarrollo por igual.

La guerra cibernética se libra en diversos frentes, entre ellos los siguientes: los sitios web de reclutamiento y movilización, la guerra psicológica, el intercambio y la difusión de información por Internet, la piratería informática, y el ciberterrorismo.

La amenaza que plantea el ciberterrorismo está aumentando en todos los Estados. El Líbano ha sido víctima de una serie de ataques cibernéticos dirigidos fundamentalmente al sector bancario (el virus Gauss) y al sector de las comunicaciones. La mayoría de los servicios electrónicos son blanco de ataques frecuentes.

Entre las medidas adoptadas a nivel nacional para promover la seguridad cibernética y la cooperación internacional se incluyen las siguientes:

- En 1999 se promulgaron la Ley núm. 140, sobre la confidencialidad de las telecomunicaciones, y la Ley núm. 75, sobre la propiedad intelectual, cada una de las cuales combate la piratería informática en determinada medida.
- En 2006, la División de Investigaciones Criminales de la Dirección General de las Fuerzas de Seguridad Interna creó una oficina para luchar contra la ciberdelincuencia y proteger la propiedad intelectual.
- En 2007, se estableció una Autoridad Reglamentadora de las Comunicaciones, que se ha convertido en un miembro activo de la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT).
- En 2009, el mando del ejército estableció una división de informática forense en la Dirección de Inteligencia.
- El Ministerio de Defensa Nacional está trabajando, en colaboración con órganos nacionales y mundiales, para establecer un equipo nacional de respuesta a emergencias cibernéticas, y ha participado en todas las iniciativas pertinentes, y celebrado conferencias y cursos de capacitación en la materia.
- En 2012, el Consejo de Ministros decidió establecer un comité de seguridad nacional encargado de administrar los sitios web del Gobierno, en el que participa un representante del Ministerio de Defensa Nacional.
- En 2013, el Consejo de Ministros creó un comité, presidido por el Ministerio de Defensa Nacional e integrado por diversos ministerios competentes, para estudiar la amenaza que planteaban las torres de comunicaciones del enemigo israelí emplazadas frente al territorio libanés.
- En 2015, el ejército libanés creó una división dedicada a la ciberseguridad.
- En la actualidad, el Parlamento está examinando un proyecto de ley sobre las transacciones electrónicas.

Entre las medidas que la comunidad internacional podría adoptar para fortalecer la ciberseguridad a escala mundial figuran las siguientes:

- Las resoluciones aprobadas por las Naciones Unidas y la Cumbre Mundial sobre la Sociedad de la Información para difundir una cultura de la información se deberían cumplir, y se debería establecer un marco de

cooperación con los órganos internacionales pertinentes a fin de asegurar el intercambio de información y mejores prácticas.

- Las leyes y los reglamentos nacionales sobre la lucha contra los delitos informáticos se deberían armonizar con las normas mundiales, con miras a prevenir los refugios digitales.
- Se debería establecer un sistema mundial para gestionar las crisis informáticas, y adoptar una legislación internacional sólida con miras a reforzar la capacidad de las leyes nacionales para combatir la ciberdelincuencia mundial e internacional.

Polonia

[Original: inglés]
[18 de julio de 2014]

1. Opinión general

La ciberseguridad es fundamental para mantener el crecimiento económico y el funcionamiento de la sociedad civil. Los ataques cibernéticos pueden afectar, no solo al sector privado y a la administración pública, sino también a los sistemas de automatización industrial en instalaciones críticas de la infraestructura.

Es necesario disponer de un sistema coherente de seguridad de la información y las telecomunicaciones, habida cuenta de la naturaleza de las amenazas y de la creciente dependencia que tienen las empresas, la administración y la sociedad con respecto a la tecnología de la información. Todas las partes interesadas, incluidos el Estado, las empresas y las organizaciones no gubernamentales, deberían participar en la ciberseguridad y contribuir a ella.

El respeto del derecho internacional es una condición necesaria para el mantenimiento de la paz y la seguridad entre los Estados en el ciberespacio.

El fomento de la capacidad nacional es la clave para fortalecer la seguridad internacional en el ciberespacio.

El aumento de la confianza en el ciberespacio repercutirá positivamente en las relaciones entre los Estados en otras esferas.

Los derechos humanos y las libertades fundamentales deben ser protegidos por igual en el ciberespacio y en el mundo real. El respeto de las libertades fundamentales en Internet es esencial para la sociedad democrática, el crecimiento sostenible y la prosperidad.

2. Iniciativas nacionales para fortalecer la ciberseguridad y la cooperación internacional

El sistema de ciberseguridad de Polonia se basa en una red de instituciones y en la cooperación de las entidades, tanto civiles como militares, en lo relacionado con los delitos cibernéticos.

El Gobierno de Polonia está trabajando en la elaboración de una estrategia nacional de ciberseguridad y de la legislación nacional en ese ámbito. Los

elementos fundamentales del sistema de ciberseguridad de Polonia serán los procedimientos, las personas y la tecnología.

El año pasado, Polonia acogió varios eventos internacionales importantes que contribuyeron a promover la cooperación internacional: la Conferencia SECURE 2015, el Foro Europeo de la Ciberseguridad (cybersecforum.eu) y la Conferencia Internacional sobre Ciberseguridad, que examinó el tema de la seguridad más allá de las fronteras.

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

Es necesario seguir perfeccionando las medidas de fomento de la confianza en el ciberespacio que se aplican a escala mundial, regional y nacional.

La comunidad internacional debería alentar la creación de capacidad nacional en materia de ciberseguridad.

Es importante fortalecer la cooperación bilateral y regional. Un buen ejemplo de cooperación regional es la plataforma de ciberseguridad de Europa Central, en la que participan Polonia, la República Checa, Eslovaquia, Hungría y Austria.

Los ejercicios internacionales en el ámbito de la ciberseguridad permiten comprender mejor el carácter de las amenazas y los medios para responder a ellas. Un ejemplo al respecto son el ejercicio Cyber Europe y el ejercicio Locked Shields de la Organización del Tratado del Atlántico Norte.

No debe subestimarse el valor de la participación de representantes de las organizaciones no gubernamentales, las empresas y el sector académico en el diálogo internacional.

Portugal

[Original: inglés]
[31 de mayo de 2016]

En su resolución 70/237 relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, la Asamblea General recordó la función que tienen la ciencia y la tecnología en ese contexto, y reconoció que los avances científicos y tecnológicos podían tener aplicaciones civiles y militares. Si bien, por una parte, el progreso en la esfera de la información y las telecomunicaciones aumenta las posibilidades de ampliar los conocimientos, fortalecer la cooperación entre los Estados y promover la creatividad humana y la circulación de la información entre la comunidad en su conjunto, por otra, esas tecnologías y esos medios pueden ser utilizados con propósitos contrarios al mantenimiento de la estabilidad y la seguridad internacionales, y afectar negativamente a la integridad nacional de los Estados.

La resolución 70/237 invita a los Estados Miembros, teniendo en cuenta el informe de 2015 del Grupo de Expertos Gubernamentales, a comunicar opiniones y observaciones sobre cuatro cuestiones:

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 promover la cooperación internacional en ese ámbito;

c) El contenido de los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones;

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

El informe contenido en el documento A/68/98 presenta algunas recomendaciones en los ámbitos siguientes: recomendaciones sobre normas, reglas y principios de conducta estatal responsable; recomendaciones sobre medidas de fomento de la confianza y el intercambio de información; y recomendaciones sobre medidas de creación de capacidad.

En relación con esas recomendaciones, Portugal formula las siguientes observaciones:

I. Normas, reglas y principios que caracterizan el comportamiento responsable de los Estados

1. Portugal considera que la seguridad de la información en la red es importante y ha venido aumentando.

2. Debemos resaltar los progresos registrados en las iniciativas para aplicar leyes sobre seguridad e integridad de la red, mediante la adopción de métodos de evaluación de los riesgos, que exigen adoptar medidas adecuadas de cooperación en el ámbito de la seguridad, en los planos técnico e institucional, y el requisito de comunicar las violaciones de la seguridad o la pérdida de integridad que tienen repercusiones importantes en el funcionamiento de los servicios.

3. A nivel conceptual, es importante reforzar la idea de que la reglamentación debería derivarse fundamentalmente de las normas internacionales.

4. A nivel internacional, es importante reforzar el intercambio de información y la realización de ejercicios de adiestramiento sobre el terreno en zonas fronterizas.

II. Medidas de fomento de la confianza e intercambio de información

1. Es fundamental promover el intercambio de información entre todos los interesados, tanto públicos como privados, teniendo en cuenta el contexto más amplio de la globalización.

2. En el plano nacional, nuestros esfuerzos se han centrado en la realización de ejercicios conjuntos con participación de entidades públicas y privadas; la promoción de la normalización técnica; y la organización de conferencias y seminarios, en algunos casos con la participación de oradores internacionales.

III. Medidas de creación de capacidad

1. Es importante elaborar medidas de creación de capacidad. No obstante, existen dificultades relacionadas con la capacitación y el mantenimiento de los recursos humanos vinculados con estas actividades.

2. Es necesario facilitar el acceso a los conocimientos y promover, entre todos los principales interesados, la formación colectiva en diversos aspectos, incluida la seguridad.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[31 de mayo de 2016]

El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con beneplácito la oportunidad de presentar su respuesta a la resolución 70/237 de la Asamblea General, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, que parte de la respuesta que dio en 2015 a la resolución 69/28. En la presente respuesta, el Reino Unido prefiere emplear el término “ciberseguridad” y los conceptos conexos, a fin de evitar cualquier confusión, dadas las distintas interpretaciones que existen del término “seguridad de la información”.

El Reino Unido reconoce que el ciberespacio es un elemento fundamental de la infraestructura nacional e internacional crítica y una base indispensable para la actividad económica y social en Internet. El Reino Unido hace referencia a la evaluación de los riesgos para la seguridad nacional llevada a cabo en 2015, que confirmó que los riesgos cibernéticos seguían siendo una amenaza de nivel I para la seguridad nacional. En el período anterior (2011-2016), el Reino Unido asignó 860 millones de libras esterlinas a la estrategia nacional de seguridad cibernética, y en el próximo quinquenio le asignará 1.900 millones de libras esterlinas más. En 2016, se publicará una nueva estrategia nacional de seguridad cibernética, que incluirá el establecimiento de un nuevo centro nacional de ciberseguridad.

El Reino Unido reconoce que la colaboración internacional es fundamental para el éxito de la ciberseguridad. Seguimos promoviendo un ciberespacio libre, abierto, pacífico y seguro a fin de que sus beneficios económicos y sociales estén protegidos y disponibles para todos. El Reino Unido está a la vanguardia en el enfrentamiento de los problemas de ciberseguridad transfronteriza, mediante iniciativas como la Alianza Mundial WePROTECT para poner fin a la explotación sexual de niños en Internet. También estamos decididos a compartir las mejores prácticas a nivel internacional y a velar por que la comunidad mundial tenga acceso a asistencia en el desarrollo de sus capacidades en materia de ciberseguridad.

El Reino Unido sigue participando de forma activa y constructiva en el debate internacional sobre ciberseguridad. Hemos proporcionado expertos para los cuatro grupos de expertos gubernamentales de las Naciones Unidas y consideramos que el informe de consenso del último Grupo hizo progresos valiosos en la reafirmación de que el derecho internacional es aplicable en el ciberespacio y de que el

cumplimiento por los Estados de las normas de derecho internacional, en particular el cumplimiento de sus obligaciones con arreglo a la Carta de las Naciones Unidas, es esencial para sus actividades relacionadas con la utilización de las tecnologías de la información y las comunicaciones.

El Reino Unido acoge con beneplácito el hecho de que en la Organización para la Seguridad y la Cooperación en Europa y en otras organizaciones regionales se sigan examinando posibles medidas futuras de fomento de la confianza en el ciberespacio.

El Reino Unido se complace en participar activamente en esos importantes temas y espera con interés seguir participando en el fortalecimiento de la capacidad y de la cooperación internacional en el ámbito de la ciberseguridad.

Serbia

[Original: inglés]
[31 de mayo de 2016]

La República de Serbia comprende que es sumamente importante garantizar y aumentar la seguridad de la información, como una de las prioridades estratégicas de la sociedad de la información.

La Asamblea Nacional de la República de Serbia aprobó la Ley sobre la Seguridad de la Información en enero de 2016. Esa Ley estableció la autoridad competente en materia de seguridad de la información, que se ocupa de preparar los reglamentos de conformidad con las normas nacionales e internacionales, cooperar con las autoridades competentes de otros países, y vigilar el cumplimiento de la ley. La Ley define los sistemas de tecnología de la información y las comunicaciones (TIC) que revisten importancia particular en Serbia, cuyos operadores tienen que aplicar medidas técnicas y organizativas adecuadas a fin de garantizar la seguridad de la información. Se trata de los sistemas siguientes: a) los sistemas de TIC de los organismos públicos; b) los sistemas de TIC en que se manejan datos personales delicados; y c) los sistemas de TIC en esferas de interés público (energía, transporte, gas, banca, atención de la salud y otros).

La autoridad competente se encarga de la cooperación internacional y, en particular, de alertar sobre los riesgos y los incidentes que presentan una de las características siguientes: a) están creciendo rápidamente o tienden a plantear un peligro importante; b) superan la capacidad nacional; c) pueden afectar a más de un país.

La Ley estableció el equipo nacional de respuesta a emergencias cibernéticas, como parte del organismo encargado de reglamentar las comunicaciones electrónicas y los servicios postales. Entre otras cosas, ese equipo cooperará con organizaciones similares de otros países.

La Ley también reglamenta la criptoseguridad y la protección contra emanaciones electromagnéticas comprometedoras.

A fin de reforzar la seguridad de los sistemas mundiales de información y telecomunicaciones, los Estados deberían cooperar, en particular manteniendo mecanismos eficaces y receptivos de intercambio de información, alertas y anuncios sobre incidentes relacionados con la ciberseguridad. Con ese fin, los Estados

deberían designar coordinadores, y proporcionar información de contacto fácilmente accesible. Se debería prestar atención especial a la protección de la infraestructura crítica, sobre todo si los incidentes afectaran al territorio de más de un Estado. Los Estados también deberían cooperar en el intercambio de conocimientos y en la educación en esta esfera.

Teniendo en cuenta el aumento de los riesgos y las características de los ciberataques en el mundo interconectado, la comunidad internacional debería alentar a los Estados a cooperar y dialogar, promover la creación de capacidades compartidas en materia de seguridad cibernética y prestar apoyo a las organizaciones internacionales que promueven la cooperación en el ámbito de la seguridad de la información. La cooperación conjunta y efectiva contribuirá a aumentar la seguridad y la protección en el entorno mundial de las TIC, de manera que los Estados y los ciudadanos estén protegidos contra diversos riesgos en el ciberespacio.

Suiza

[Original: inglés]
[7 de junio de 2016]

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

La tecnología de la información y las comunicaciones (TIC) se ha convertido en un factor indispensable de las actividades sociales, económicas y políticas. Suiza está decidida a aprovechar las oportunidades que genera el uso de la TIC. Sin embargo, ese uso ha expuesto a la infraestructura de la información y las comunicaciones a problemas de uso indebido o de mal funcionamiento a manos de delincuentes, servicios de inteligencia, agentes político-militares o terroristas. Las alteraciones, la manipulación y los ataques concretos que se llevan a cabo a través de las redes electrónicas son riesgos que plantea una sociedad de la información.

2. Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en ese ámbito

En 2012, el Gobierno Federal de Suiza aprobó la estrategia nacional para la protección de Suiza contra los riesgos cibernéticos, con lo que sentó las bases para la adopción de un enfoque amplio. La estrategia nacional tiene por objeto mejorar la detección temprana de los riesgos cibernéticos y las amenazas emergentes, aumentar la resiliencia de la infraestructura suiza en su conjunto a los ataques cibernéticos, y, en general, reducir los riesgos cibernéticos. La estrategia también refleja la necesidad de una cultura de seguridad (o ciberseguridad), la responsabilidad compartida de todos los participantes y la necesidad de un enfoque basado en los riesgos. Además, promueve la coordinación a los niveles gubernamental y nacional (es decir, alianzas público-privadas) y la cooperación internacional. La estrategia comprende 16 medidas. El Gobierno Federal de Suiza aprobó un plan detallado para la aplicación de la estrategia en 2013.

3. Contenido de los conceptos mencionados en el párrafo 3 de la resolución

Para enfrentar los riesgos cibernéticos es preciso fortalecer la cooperación internacional (esfera de acción 5 definida en la estrategia). La política exterior de Suiza en el ámbito de la seguridad cibernética se centra en la elaboración de normas de comportamiento estatal responsable, medidas de fomento de la confianza y actividades de creación de capacidad. Teniendo esto presente, Suiza participa en diferentes procesos internacionales. La Organización para la Seguridad y la Cooperación en Europa (OSCE) ha adoptado medidas de fomento de la confianza en el ámbito de la ciberseguridad. Suiza considera que ese proceso es fundamental. Otro proceso importante en el que Suiza participa es el proceso de Londres. Suiza apoya una serie de proyectos de desarrollo de la capacidad.

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

Todas las medidas adoptadas por la comunidad internacional deben buscar un equilibrio entre las consideraciones de seguridad y las deliberaciones en materia de derechos humanos. Los mismos derechos que tienen las personas fuera de Internet deben garantizarse en Internet. Es preciso perfeccionar las medidas de fomento de la confianza. El conjunto de medidas de fomento de la confianza aprobadas por la OSCE reviste una importancia fundamental para reforzar la seguridad. El aumento de la transparencia mediante el intercambio de información y el fortalecimiento de la cooperación por medio de medidas concretas y la realización de actividades conjuntas contribuirán al logro de la estabilidad general en el ciberdominio.

Togo

[Original: francés]
[2 de junio de 2016]

Si bien los avances en el ámbito de las tecnologías de la información y las telecomunicaciones son un activo valioso para los países en desarrollo, también plantean una amenaza para la seguridad nacional e internacional. Se trata de un espacio virtual que a menudo se utiliza con fines delictivos o terroristas.

El Togo no es inmune a esta amenaza, y ya ha debido enfrentar delitos relacionados con las tecnologías de la información y las comunicaciones, que van desde casos de estafa y otros tipos de fraude, hasta pornografía infantil y violaciones de la libertad y la integridad de las personas.

En la era del terrorismo, la web y las redes sociales son un medio de propaganda y reclutamiento para las organizaciones terroristas. A esto se suma el hecho de que la mayoría de los países están migrando a la administración electrónica, lo que representa un gran desafío para nuestros gobiernos, que temen que los ataques cibernéticos puedan comprometer su buen funcionamiento y la seguridad en los ámbitos civil y militar.

Ante esta situación, es importante que se adopten medidas en los planos nacional e internacional para ejercer un control sobre el sector de las tecnologías de la información y las comunicaciones que permita combatir su uso con fines delictivos.

En el Togo, se han adoptado diversas medidas en ese sentido, en particular, las siguientes:

– La aprobación del Decreto núm. 2011-120/PR de 6 de julio de 2011, sobre la identificación sistemática y obligatoria de los abonados a los servicios de telecomunicaciones;

– La aprobación de la Ley núm. 2012-018 sobre las comunicaciones electrónicas, y la Ley núm. 2013-003 que la modifica;

– La elaboración de anteproyectos de ley sobre la ciberdelincuencia, la criptografía, la ciberseguridad, la protección de los datos personales y las transacciones electrónicas.

El objetivo de esas medidas es asegurar la trazabilidad de toda actividad informática y de telecomunicaciones, y establecer un dispositivo de seguridad que permita proteger las redes informáticas y de telecomunicaciones de cualquier intrusión fraudulenta.

El Togo también consideró necesario establecer un marco institucional que garantizara ese control, a saber, un equipo nacional de respuesta a las emergencias cibernéticas, con el fin de disponer, a nivel nacional, de una entidad encargada de vigilar la seguridad cibernética. Este equipo complementará la labor de la autoridad reguladora de correos y telecomunicaciones.

Además, cabe señalar que se ha emprendido una labor de fomento de la capacidad de los recursos humanos, a fin de que los encargados de hacer cumplir la ley, y las entidades públicas y privadas que se ocupan de la seguridad cibernética puedan responder con eficacia a cualquier tipo de amenaza.

Por otra parte, la cooperación internacional, en particular en el contexto de la Unión Internacional de Telecomunicaciones y de las Naciones Unidas, permitirá fortalecer la seguridad en el ámbito de las tecnologías de la información y las telecomunicaciones.

Turkmenistán

[Original: ruso]
[28 de marzo de 2016]

La neutralidad es el fundamento de la política interior y exterior de Turkmenistán, a partir de la estrecha relación que existe entre los intereses nacionales, la seguridad mundial y el progreso común. Para Turkmenistán, un elemento clave que se deriva de su condición de Estado neutral y de sus obligaciones internacionales, es el carácter pacifista de su política exterior. En consecuencia, todas las cuestiones se abordan exclusivamente por las vías política y diplomática, sobre todo en el marco de las Naciones Unidas y otras organizaciones internacionales. Turkmenistán apoya plenamente las actividades internacionales de

lucha contra la proliferación de las armas de destrucción en masa, sus sistemas vectores y las tecnologías conexas, y promueve el desarme como requisito fundamental para la seguridad mundial. En su legislación, Turkmenistán proclama su negativa a poseer, fabricar, almacenar o transportar armas nucleares, químicas o bacteriológicas, así como otros tipos de armas de destrucción en masa, incluidos nuevos tipos de armas de esa índole o tecnologías para su producción.

Turkmenistán se ha adherido a varios instrumentos internacionales de desarme, dirigidos principalmente a alentar a los Estados partes a mantener la paz, la armonía y la seguridad mundiales.

Dada la especial importancia que otorga al fortalecimiento de la paz y la seguridad internacionales, Turkmenistán pide que se reduzca el número de armas, ya que considera que cuantas menos armas haya en el mundo, más firme y tranquilo será su desarrollo y mayores serán la confianza y el entendimiento entre los países y los pueblos. El documento marco de política exterior de Turkmenistán para 2013-2017 pone de relieve que el país seguirá promoviendo activamente los procesos de desarme y la reducción de los arsenales de armas, sobre todo de armas de destrucción en masa.

En el discurso que pronunció en la reunión del Consejo de Ministros el 5 de junio de 2015, el Presidente de Turkmenistán señaló en particular las obligaciones internacionales de nuestro país con la comunidad mundial, e hizo hincapié en que neutralidad significa no adhesión a uniones o a bloques políticos, económicos o militares; tener nuestro propio ejército dotado de efectivos suficientes para proteger la paz y la libertad de la nación; rechazar las armas de destrucción en masa y prohibir su entrada en nuestro territorio nacional y nuestro espacio aéreo; defender los valores humanos universales y los principios democráticos, y salvaguardar la armonía cívica y la paz en el país; y llevar a cabo la política interior y exterior en estrecha cooperación con las Naciones Unidas y las organizaciones internacionales humanitarias.

En el sexagésimo noveno período de sesiones de la Asamblea General, celebrado el 3 de junio de 2015, 193 Estados aprobaron por unanimidad la resolución 69/285 relativa a la neutralidad permanente de Turkmenistán, lo que ilustra con claridad el reconocimiento universal de la política de nuestro país que está dirigida efectivamente a salvaguardar la paz, la seguridad y el desarrollo sostenible en los planos regional e internacional. En esa resolución se pone de relieve la importante contribución de la neutralidad permanente de Turkmenistán al fortalecimiento de la paz y la seguridad en la región y al desarrollo de relaciones amistosas y de beneficio mutuo con los países del mundo.

Como país sede del Centro Regional de las Naciones Unidas para la Diplomacia Preventiva en Asia Central, Turkmenistán pide que este órgano participe más en varios aspectos de las cuestiones regionales con el apoyo de los Estados Miembros de las Naciones Unidas y otras organizaciones (en particular, la Organización para la Seguridad y la Cooperación en Europa, la Unión Europea y la Comunidad de Estados Independientes).

En 2015 se celebró en Ashgabat un foro internacional sobre la protección de la paz, la estabilidad y la seguridad en la región de Asia Central. Turkmenistán, como parte en tratados internacionales, convenciones de las Naciones Unidas e instrumentos multilaterales en la esfera del desarme, se propone seguir haciendo todo lo posible para facilitar estos procesos, sobre todo en el plano regional, y lograr que en el país se celebren reuniones regionales periódicas sobre cuestiones de desarme en Asia Central.