Naciones Unidas A/72/315

Asamblea General

Distr. general
11 de agosto de 2017
Español
Original: árabe/español/francés/
inglés/ruso

Septuagésimo segundo período de sesiones
Tema 95 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/72/150.

17-13876 (S) 210917 250917

Se ruega reciclar

I. Introducción

1. El 5 de diciembre de 2016, la Asamblea General aprobó la resolución 71/28 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. En el párrafo 3 de esa resolución, la Asamblea invitaba 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 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 2 de la 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 16 de febrero de 2017 se envió una nota verbal a todos los Estados Miembros para invitarlos a proporcionar información sobre el tema, seguida de otra nota verbal de fecha 12 de junio de 2017. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en la sección II. Las respuestas que se reciban después del 31 de julio de 2017 se publicarán en el sitio web de la Oficina de Asuntos de Desarme (https://www.un.org/disarmament/es/) en el idioma original.

II. Respuestas recibidas de los Gobiernos

Afganistán

[Original: inglés]
[26 de mayo de 2017]

El Ministerio de Comunicaciones y Tecnología de la Información de la República Islámica del Afganistán ha informado de lo siguiente en relación con el párrafo 3 de la resolución 71/28 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

Logros

A fin de promover la seguridad de la tecnología de la información a nivel internacional y la autenticidad de las transacciones electrónicas, el Ministerio de Comunicaciones y Tecnología de la Información ha establecido un dispositivo de infraestructura de clave pública. El Ministerio también ha creado un sistema de centro de operaciones de la red y tiene la intención de conectar este sistema con el de los Estados Miembros con fines de identificación y verificación de las estadísticas y la corriente de datos en Internet.

El Ministerio ha elaborado proyectos de legislación contra la ciberdelincuencia, que ha enviado al Ministerio de Justicia para su examen. En cuanto a soluciones fundamentales, a la luz de dicha legislación, se pueden realizar transacciones electrónicas más seguras y se puede prevenir la ciberdelincuencia.

El Ministerio ha creado una ciberestrategia nacional para intercambiar información segura, establecer un marco de seguridad de la tecnología de la información para el proyecto NIXA que será ejecutado por el Ministerio y afrontar y descubrir los delitos cibernéticos.

Propuestas

El Ministerio de Comunicaciones y Tecnología de la información pide a los países desarrollados que tienen policía cibernética que presten su asistencia y cooperación al Ministerio en el establecimiento de dicho cuerpo.

A fin de hacer frente a los delitos cibernéticos y luchar firmemente contra este fenómeno, debería establecerse un sistema coherente (que favorezca la circulación de información sobre los delitos) a nivel internacional.

Una solución importante para la seguridad de Internet es establecer la gobernanza de Internet, mediante la cual se puede proporcionar una base para el intercambio de información y datos confidenciales entre todos los departamentos y oficinas del Gobierno de cara a la implementación de la red mencionada. A este respecto, el Ministerio solicita la cooperación de todos los Estados Miembros.

El Ministerio también solicita a los Estados Miembros que apoyen al personal del Ministerio en sus esfuerzos por combatir la delincuencia cibernética y mejorar la seguridad de la información proporcionándole programas de formación profesional y técnica.

Alemania

[Original: inglés]
[30 de mayo de 2017]

El desarrollo de la tecnología de la información y las comunicaciones (TIC) ofrece numerosas oportunidades económicas, sociales y científicas. Asegurar el acceso al ciberespacio y mantener la integridad, la autenticidad y la confidencialidad de los datos en el ciberespacio se han convertido en cuestiones fundamentales del siglo XXI.

En un mundo cada vez más interconectado, los Estados, las infraestructuras vitales, las empresas y las personas dependen del funcionamiento fiable de la tecnología de la información y las comunicaciones. Las consecuencias de su uso indebido no solo afectarían al ciberespacio, podrían causar daños sociales, económicos, políticos y de otro tipo. Por ejemplo, los ataques contra las instituciones del Estado o los procesos políticos y democráticos pueden afectar a la seguridad y el orden público.

Alemania está haciendo frente a esos desafíos promoviendo un uso de la TIC por los Estados respetuoso del derecho internacional, acorde con las normas y que fomente la confianza en los tres niveles siguientes:

a) A nivel mundial, Alemania apoya los esfuerzos encaminados a acordar la manera en que el derecho internacional se aplica al uso de la TIC por los Estados y a desarrollar normas, reglas o principios voluntarios y no vinculantes sobre un comportamiento responsable de los Estados que permita lograr un entorno de TIC abierto, seguro, estable, accesible y pacífico. A este respecto, la labor de los sucesivos Grupos de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional es especialmente importante. Los expertos alemanes han participado activamente en esos Grupos y Alemania está decidida a promover sus recomendaciones. Ha llegado el momento de ampliar el debate y lograr la participación de un mayor número de

Estados Miembros de las Naciones Unidas, con miras a la universalización de la labor relativa a la TIC en el contexto de la seguridad internacional. Alemania apoya el liderazgo de las Naciones Unidas y el fortalecimiento de su capacidad en esta esfera. El intercambio de información y la cooperación a nivel internacional en la atribución de los ataques cibernéticos son algunas de las cuestiones que deben debatirse más a fondo. Es necesario establecer normas claras y de obligado cumplimiento con respecto al uso malintencionado de las capacidades cibernéticas, así como el espionaje en línea con fines económicos;

b) A nivel regional, las medidas de fomento de la confianza ayudan a mitigar el riesgo de que los incidentes relacionados con la TIC se conviertan en crisis políticas o incluso militares. En el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Alemania ha participado activamente durante años en la definición y aplicación de medidas de fomento de la confianza encaminadas a incrementar la seguridad en el uso de la tecnología de la información y las comunicaciones por los Estados. Durante la Presidencia alemana de la OSCE en 2016, los Estados participantes acordaron nuevas medidas de ese tipo. El Consejo Ministerial de la OSCE celebrado en 2016 en Hamburgo aprobó estas medidas y no solo dio instrucciones para su aplicación, sino también para continuar trabajando en este ámbito. Esta labor no debe limitarse a los aspectos políticos y militares, sino que debe abarcar las múltiples dimensiones de la seguridad. Fuera de la OSCE, Alemania también apoya actividades similares en las organizaciones regionales de otros continentes;

c) En el plano bilateral, Alemania mantiene diálogos y celebra consultas periódicamente con múltiples asociados en la esfera cibernética. Sobre la base de las relaciones de colaboración ya establecidas, Alemania también apoya las iniciativas de desarrollo de la capacidad en materia de ciberseguridad de otras naciones. Al actualizar su estrategia de seguridad cibernética en noviembre de 2016, el Gobierno de Alemania decidió trabajar en pro del establecimiento de un instituto alemán de ciberseguridad internacional, con miras a sistematizar e impulsar esas iniciativas.

Las actividades de Alemania con respecto a la información y las telecomunicaciones en el contexto de la seguridad internacional son parte de una intensa labor más amplia de promoción de la seguridad de la TIC. Las recientes medidas de tipo normativo adoptadas a nivel nacional, como la Ley de Seguridad de la Tecnología de la Información de 2015 y la revisión de la estrategia nacional de ciberseguridad de 2016, tienen por objeto mejorar la seguridad general en el ámbito de la TIC en Alemania.

Armenia

[Original: inglés]
[31 de mayo de 2017]

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

Habida cuenta del ritmo de desarrollo de la sociedad electrónica en la República de Armenia, las cuestiones relativas a la seguridad de la información están adquiriendo considerable relevancia y tienen enormes repercusiones en todos los aspectos de la seguridad nacional.

Las tendencias de la tecnología de la información y las comunicaciones (TIC) plantean amenazas y desafíos cualitativamente nuevos, que requieren una coordinación sistemática y nuevos enfoques para velar por la utilización segura de la TIC. Teniendo en cuenta las técnicas de “guerra de información” utilizadas en diferentes entornos de conflicto, Armenia otorga gran importancia a garantizar la

seguridad de la información para el mantenimiento de la paz y la seguridad internacionales.

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

Armenia ha emprendido actividades destinadas a salvaguardar los intereses públicos y del Estado en el ámbito de la seguridad de la información y la armonización de la legislación pertinente con las normas internacionales. Varias disposiciones normativas que rigen este ámbito han entrado en vigor, en particular la estrategia nacional de seguridad y el concepto de seguridad de la información, así como diversas leyes sobre la lucha contra el terrorismo; los secretos de Estado y oficiales; los documentos electrónicos y las firmas digitales; la protección de los datos personales; la libertad de información; y los medios de comunicación.

De conformidad con las decisiones pertinentes del Gobierno:

a) Se han tomado varias medidas prácticas para asegurar la protección de la información de acceso público de órganos del Gobierno en Internet y dotar a sus sistemas de información de una conexión segura a Internet;

b) Se han establecido requisitos mínimos para los sitios web oficiales de órganos del Estado.

Armenia ha aprobado y aplicado un conjunto de normas ISO relativas a la seguridad de la información. En octubre de 2006, se ratificó el Convenio sobre la Ciberdelincuencia del Consejo de Europa, con las consiguientes enmiendas posteriores de la legislación nacional.

Armenia participa activamente en los programas, cursos de capacitación e iniciativas de cooperación pertinentes que se llevan a cabo en diferentes marcos internacionales, como la Comunidad de Estados Independientes, la Organización del Tratado de Seguridad Colectiva, la Unión Europea y la Organización del Tratado del Atlántico Norte. En particular, en 2016 se celebró el ejercicio conjunto en dos etapas de los Estados miembros de la Comunidad de Estados Independientes contra el terrorismo cibernético. A principios de 2017 se propuso para su aprobación interdepartamental a nivel nacional un proyecto de acuerdo sobre cooperación entre los Estados miembros de la Organización del Tratado de Seguridad Colectiva para velar por la seguridad de la información.

Contenido de los conceptos mencionados en el párrafo 2

El concepto de seguridad de la información de la República de Armenia define el término “seguridad de la información” como la protección de los intereses nacionales en la esfera de la información, que están vinculados al equilibrio de la totalidad de los intereses de las personas, la sociedad y el Estado.

Teniendo en cuenta el rápido desarrollo de la tecnología de la información y las comunicaciones, se ha establecido un grupo de trabajo interinstitucional para que prepare un nuevo concepto de cómo velar por la seguridad de la información y asegurar una política de información en la República de Armenia para finales de 2017.

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

Armenia subraya la importancia de una cooperación internacional mejorada y eficaz en materia de seguridad de la información y hace hincapié en el papel de la Unión Internacional de Telecomunicaciones.

Belarús

[Original: ruso]
[5 de junio de 2017]

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

La situación actual de la seguridad de la información internacional es insatisfactoria. Se producen intentos de utilizar la tecnología de la información con fines políticos.

Belarús se enfrenta a una serie de problemas relacionados con la seguridad de la información:

a) La protección insuficiente del segmento nacional en lo relativo a la exposición al riesgo de ataques de denegación de servicio (DDoS) a nivel de la base de proveedores de red dorsal y los proveedores nacionales, e incluso las plataformas de hospedaje;

b) La posibilidad de que aparezcan capacidades y vulnerabilidades no declaradas en productos de seguridad de la información y la falta de capacidad para detectarlas de manera oportuna, lo que a menudo obstaculiza el efecto de las medidas para proteger la información;

c) El peligro de ataques por intrusos contra las infraestructuras vitales y las infraestructuras de tecnología de la información, como los sistemas de suministro de energía y los sistemas automatizados de gestión de la producción y el transporte.

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

Dichas medidas son las siguientes:

a) Trabajar en todo el sistema para actualizar los requisitos de protección técnica y criptográfica de la información, cuya difusión o disposición está restringida;

b) Organizar y aplicar normas y estándares técnicos relativos a la protección técnica y criptográfica de la información;

c) Aplicar acuerdos de intercambio de información con empresas punteras en seguridad de la información;

d) Cooperar periódicamente con organizaciones y organismos estatales para facilitar respuestas rápidas a incidentes específicos relacionados con la seguridad de la información;

e) Mantenimiento por parte de los países de sus propios paquetes de detección de programas malignos;

f) Colaboración con países de la Organización del Tratado de Seguridad Colectiva a través del centro de coordinación de consultas.

Examen de los conceptos internacionales encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones

Un enfoque fundamental que utiliza Belarús con respecto a la seguridad de la información internacional se refiere a la necesidad de prevenir el posible uso indebido de la tecnología de la información y las comunicaciones (TIC) con el objetivo de socavar la seguridad y la estabilidad nacionales y la seguridad internacional.

Belarús participa activamente en los debates sobre la seguridad de la información internacional en los foros de diversas organizaciones internacionales, en particular las Naciones Unidas, la Organización del Tratado de Seguridad Colectiva y la Organización para la Seguridad y la Cooperación en Europa.

Belarús apoya la iniciativa de aprobar un instrumento universal sobre la seguridad de la información internacional en el marco de las Naciones Unidas.

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

En el plano internacional es crucial promover gradualmente el principio de no injerencia en los asuntos internos de los Estados soberanos y el rechazo mutuo de las acciones agresivas en la esfera de la información. Esto debe lograrse principalmente mediante el apoyo a la soberanía en materia de información de los Estados Miembros de las Naciones Unidas, con los siguientes propósitos:

a) Defender los derechos de los ciudadanos a recibir, almacenar y difundir información completa, fidedigna y oportuna;

b) Desarrollar una sociedad de la información en la que los Estados Miembros de las Naciones Unidas participen en las relaciones mundiales de información sobre una base de igualdad;

c) Asegurar una política intergubernamental eficaz de gestión de la información a fin de prevenir la proliferación de ideas terroristas y extremistas;

d) Velar por el funcionamiento resiliente de las infraestructuras vitales.

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

a) Establecer mecanismos para la cooperación internacional, de conformidad con las disposiciones de los instrumentos actuales y futuros del derecho internacional;

b) Sentar las bases de una cooperación efectiva entre la comunidad internacional y las empresas multinacionales que controlan la gran mayoría de la tecnología de la información y las comunicaciones, a fin de detectar y bloquear las fuentes de amenazas para la seguridad de la información.

Brunei Darussalam

[Original: inglés]
[29 de junio de 2017]

Brunei Darussalam reconoce que las tendencias mundiales han ido cambiando al hilo de avances cada vez más importantes en la esfera de la información y las telecomunicaciones. Al mismo tiempo, esta situación ha dado lugar a nuevas amenazas y desafíos en forma de piratería, ciberdelincuencia y ciberterrorismo, que ponen en peligro servicios, redes e infraestructuras vitales en todo el mundo. Su

naturaleza transnacional e intangible hace que se precise la colaboración de la comunidad mundial para crear un entorno en línea seguro y fiable.

A escala nacional, bajo los auspicios del Comité de Seguridad Nacional, el país mantiene fuertes lazos de cooperación con un gran número de organismos locales de seguridad con el fin de gestionar las amenazas internas para la ciberseguridad. El equipo nacional de respuesta ante emergencias cibernéticas de Brunei Darussalam se estableció en mayo de 2004 y pasó a ser el organismo único del país al que se remiten los incidentes relacionados con la seguridad cibernética y de Internet. Por medio de la afiliación mundial con otros equipos de respuesta a emergencias cibernéticas, el equipo nacional adquiere información valiosa sobre las amenazas para la seguridad en relación con la tecnología de la información y las comunicaciones (TIC) e intercambia información sobre los riesgos de seguridad detectados dentro de la infraestructura nacional de TIC.

Brunei Darussalam está decidido a trabajar con los asociados regionales e internacionales para mantener un estado de disponibilidad constante que permita hacer frente a las principales amenazas cibernéticas internacionales. En el marco de la estructura regional de la Asociación de Naciones de Asia Sudoriental (ASEAN), Brunei Darussalam participará en el Grupo de Trabajo de Expertos sobre Ciberseguridad de la Reunión de los Ministros de Defensa de la ASEAN con homólogos de otros países (ADMM-Plus), que reúne a 18 países con el fin de promover una cooperación práctica y eficaz y aumentar su capacidad de proteger el ciberespacio de la región y hacer frente a los desafíos para la seguridad cibernética.

El Gobierno es consciente de la existencia de amenazas en todos los escenarios cibernéticos, como el de la computación en la nube y los sistemas de telefonía móvil, que representan una parte sustancial de las prioridades de seguridad y defensa de Brunei Darussalam.

Canadá

[Original: inglés]
[17 de julio de 2017]

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

a) Un ciberespacio libre, abierto y seguro es fundamental para promover la seguridad, la prosperidad y los derechos humanos;

b) El derecho internacional vigente se aplica al uso de la tecnología de la información y las comunicaciones por los Estados;

c) 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;

d) Las medidas prácticas de fomento de la confianza son un método que ha demostrado reducir el riesgo de conflicto armado.

En el plano nacional, el Gobierno del Canadá publicó su estrategia de ciberseguridad en 2010, centrada en fortalecer la seguridad de los sistemas cibernéticos del país y proteger a los canadienses conectados a Internet. El Gobierno finalizó recientemente un examen de las medidas vigentes en materia de ciberseguridad. Sobre esta base, está previsto publicar el nuevo enfoque nacional de la seguridad cibernética a finales de 2017.

La política de defensa de 2017 incluye nuevas inversiones y una nueva orientación normativa para aprovechar mejor las capacidades cibernéticas en apoyo de las operaciones militares. Las capacidades cibernéticas activas de las Fuerzas

Armadas del Canadá estarán sujetas al mismo control riguroso que otros instrumentos militares, incluidas las disposiciones aplicables del derecho nacional e internacional y las reglas de enfrentamiento.

En el plano internacional, el Canadá participa activamente de distintas formas:

a) Sigue 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 sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2012-2013 y de 2014-2015;

b) Ratificó el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) en julio de 2015. El Canadá alienta a los países a que se adhieran a ese Convenio o lo utilicen como modelo para elaborar sus propias leyes de lucha contra la ciberdelincuencia;

c) Desde 2007, se ha comprometido a aportar 11 millones de dólares para apoyar proyectos de desarrollo de la capacidad en materia de ciberseguridad;

d) 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 su ciberinfraestructura;

e) Ha venido trabajando para aplicar 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 de Asia Sudoriental;

f) Apoya los esfuerzos que despliega la Organización del Tratado del Atlántico del Norte para fortalecer la ciberseguridad de la Organización y de los países aliados.

Cuba

[Original: español]
[5 de abril de 2017]

Tal y como se afirma en la resolución 71/28 de la Asamblea General, los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y hay que impedir que estos avances afecten la seguridad internacional.

Es necesario promover a nivel multilateral el examen de las amenazas reales y potenciales en la esfera de la seguridad de la información y de posibles estrategias para prevenirlas y enfrentarlas.

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

Cuba apoya el trabajo del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, creado a partir de la resolución 58/32, y en el que participa un experto cubano.

Consideramos necesario establecer un marco regulador internacional jurídicamente vinculante, complementario al derecho internacional existente, aplicable a las tecnologías de la información y las comunicaciones.

Los sistemas de información y telecomunicaciones pueden convertirse en armas cuando se diseñan o emplean para causar daños a la infraestructura de un Estado. Todos los Estados deben respetar las normas internacionales existentes en esta esfera. Los accesos a los sistemas de información o de telecomunicaciones de

otro Estado deben corresponderse con los acuerdos de cooperación internacional alcanzados, sobre la base del principio del consentimiento del Estado concernido. Las formas y alcance de los intercambios deben respetar la legislación del Estado a cuyo sistema se accederá.

El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia y constituye un uso ilegal e irresponsable de estos medios, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales y afectar negativamente la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar.

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

Mediante transmisiones radiales y televisivas ilegales se ha estado agrediendo de modo permanente desde el exterior el espacio radioeléctrico cubano, difundiendo programaciones especialmente diseñadas para incitar al derrocamiento del orden constitucional establecido por el pueblo cubano. En promedio, durante 2016 se transmitieron de manera ilegal contra Cuba 1.875 horas semanales a través de 25 frecuencias desde el territorio de los Estados Unidos de América. Las continuadas transmisiones radiales y televisivas desde los Estados Unidos hacia Cuba contravienen los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional y las disposiciones de la Unión Internacional de Telecomunicaciones.

Una vez más Cuba exhorta a que se ponga fin de inmediato a estas políticas agresivas y lesivas a la soberanía de Cuba, que resultan, además, incompatibles con el desarrollo de vínculos respetuosos y de cooperación entre los Estados.

Cuba 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.

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 V Cumbre de la CELAC, celebrada en Punta Cana (República Dominicana) en enero de 2017, se destacó nuevamente la importancia de la tecnología de la información y las comunicaciones, incluida Internet, como herramientas para fomentar la paz, el bienestar humano, el desarrollo, el conocimiento, la inclusión social y el crecimiento económico.

Cuba reitera que la cooperación internacional es fundamental para enfrentar los peligros del uso indebido de la tecnología de la información y las comunicaciones. Al mismo tiempo, subraya la importancia que tiene la Unión Internacional de Telecomunicaciones en la discusión intergubernamental sobre las cuestiones de ciberseguridad.

Ecuador

[Original: español]
[28 de julio de 2017]

El Ecuador considera que la seguridad en las relaciones internacionales debe basarse en la confianza y el respeto entre los Estados. Las continuas revelaciones de los masivos e indiscriminados sistemas de espionaje de las comunicaciones de todas las ciudadanas y ciudadanos del planeta, así como una utilización de las tecnologías de la información y las comunicaciones contrarias al derecho internacional atentan contra los principios del respeto a la soberanía y la no interferencia en los asuntos internos de los Estados, son acciones que inyectan un grave elemento de inestabilidad en las relaciones entre los Estados y que afectan por lo tanto a la seguridad internacional. Estos sistemas de espionaje atentan además contra varios derechos fundamentales de las personas.

Por esta razón, el Ecuador apoya los esfuerzos que se han realizado para continuar estudiando las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, así como la manera en que el derecho internacional debe ser aplicado al uso de las tecnologías de la información y las comunicaciones por los Estados, además de las normas, reglas y principios de conducta estatal responsable en esta materia.

El Salvador

[Original: español]
[24 de mayo de 2017]

Con relación al cumplimiento de las obligaciones adquiridas con la Organización de las Naciones Unidas, El Salvador respetuosamente informa respecto a la resolución 71/28 de la Asamblea General, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, que su Fuerza Armada adquirió en 2016 un sistema de encriptación de la documentación institucional, para fortalecer la seguridad de la información, el cual se encuentra en proceso de implementación.

Estonia

[Original: inglés]
[31 de mayo de 2017]

Estonia reconoce que la seguridad en el mundo cibernético se ha convertido en una cuestión fundamental en el contexto más amplio de la seguridad internacional. Por lo tanto, el papel y la intervención de las Naciones Unidas cada vez adquieren mayor importancia.

La seguridad en Internet ha sido una de las mayores prioridades del Gobierno de Estonia. El principal documento de orientación sobre esta cuestión es la estrategia nacional de ciberseguridad (2014-2017). El Consejo de Ciberseguridad del Comité de Seguridad del Gobierno apoya la cooperación entre organismos a nivel estratégico y supervisa la aplicación de los objetivos de la estrategia de ciberseguridad. El Centro de Excelencia de Cooperación en Ciberdefensa de la Organización del Tratado del Atlántico del Norte se estableció en Tallin y al 30 de mayo de 2017 había 20 Estados Miembros contribuyentes.

Estonia considera que la amplia utilización de servicios digitales exige un alto grado de ciberseguridad y opina que el aspecto socioeconómico y el aspecto político y militar de la seguridad cibernética están interrelacionados. Asimismo, considera

que es fundamental que los países se abstengan de atacar las infraestructuras vitales nacionales. Estonia también hace un llamamiento a mantener un comportamiento responsable con respecto a la infraestructura mundial de comunicaciones para promover el acceso a la información y la confianza en la tecnología de la información y las comunicaciones (TIC). Considera que es responsabilidad de cada país elaborar y aplicar leyes nacionales que ayuden a controlar el uso malicioso de la TIC por agentes no estatales y buscar formas de mejorar la formulación, difusión y promoción de políticas, discursos y argumentos responsables y activos.

Por cuarta vez consecutiva, Estonia es miembro 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 Grupo ha sido un foro muy productivo, y en el futuro podría ser un instrumento útil, no solo para estudiar las amenazas cibernéticas y sus posibles soluciones, sino también para comprender cómo aplican los diferentes países el derecho internacional vigente y las normas, reglas y principios. A juicio de Estonia, el Grupo debería proseguir su labor de promoción del diálogo entre los Estados Miembros, que facilita el intercambio de información y mejores prácticas. Además, debería examinar medidas y mecanismos prácticos de cooperación para promover la creación de capacidad en los Estados Miembros, con el objetivo final de dotar a estos de la competencia y la capacidad necesarias para abordar todos los aspectos de los desafíos de Internet.

Es importante incrementar los progresos logrados en las reuniones de 2014 y 2015 del Grupo de Expertos Gubernamentales mediante la promoción de normas de conducta de los Estados que apoyen la apertura, la rendición de cuentas y otros valores democráticos en el ciberespacio. Estonia confía en que el Grupo presente otro informe aprobado por consenso en junio de 2017.

Finlandia

[Original: inglés]
[21 de julio de 2017]

Finlandia acoge con beneplácito la oportunidad de informar sobre la aplicación de la resolución 71/28 de la Asamblea General.

Las medidas tomadas en el plano nacional son las siguientes:

a) La estrategia nacional de ciberseguridad (2013) y su programa actualizado de aplicación (2017) definen directrices y medidas clave para el fortalecimiento de la ciberseguridad y la resiliencia;

b) Finlandia ha establecido un Centro Nacional de Ciberseguridad y un Centro de Prevención de la Ciberdelincuencia, y ha nombrado una Embajadora para Asuntos Cibernéticos en el Ministerio de Relaciones Exteriores. En 2016 se aprobó la estrategia nacional de seguridad de la información;

c) Finlandia contribuye activamente a la cooperación en relación con el ciberespacio en el marco de la Unión Europea;

d) Finlandia apoya diversos tipos de tecnología de la información y las comunicaciones para proyectos de desarrollo y de creación de capacidad relacionados con el ciberespacio. Además es socio fundador del Foro Mundial de Competencia Cibernética, Y en 2016 se sumó al fondo fiduciario de la Alianza para el Desarrollo Digital del Banco Mundial. Finlandia apoya la gobernanza de Internet sobre la base del modelo de múltiples interesados. Ha participado activamente en la Cumbre Mundial sobre la Sociedad de la Información y su proceso de seguimiento, así como en la labor del Foro para la Gobernanza de Internet y su financiación. El octavo Foro de Internet de Finlandia se celebró en Helsinki en abril de 2017;

e) Finlandia participa activamente en el diálogo sobre cuestiones cibernéticas en los foros multilaterales y regionales, y de forma bilateral. 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 convenidas en ese ámbito;

f) 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 y participa activamente en el trabajo del Grupo actual. También 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 en los talleres organizados por el Instituto de las Naciones Unidas de Investigación sobre el Desarme;

g) Finlandia se sumó a la Coalición para la Libertad de Expresión en Internet en 2012 y contribuye a la Digital Defenders Partnership. Asimismo, organizó la conferencia del Día Mundial de la Libertad de Prensa de 2016, que se celebró en Helsinki;

h) Finlandia es parte en el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Un nuevo plan estratégico de la policía (2015) destina recursos a la prevención de los delitos informáticos y al desarrollo de conocimientos especializados en ciberseguridad. También existe un plan integral de prevención de la ciberdelincuencia.

Las esferas prioritarias en que la comunidad internacional debe seguir trabajando son, entre otras, las siguientes:

a) La labor del Grupo de Expertos Gubernamentales actual, a la que Finlandia atribuye gran importancia y a cuyo éxito está dispuesta a contribuir, incluida la determinación de las 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 para fortalecer la resiliencia y la seguridad en el ciberespacio;

d) El diálogo entre múltiples interesados, que Finlandia seguirá apoyando y alentando, y el fortalecimiento de las alianzas público-privadas a nivel nacional e internacional.

Grecia

[Original: inglés]
[26 de mayo de 2017]

En el marco del Consejo de Europa, Grecia ha ratificado, en virtud de la Ley núm. 4411/2016 (Boletín Oficial A´ 142, 3 de agosto de 2016), el Convenio del sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001) y el Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la tipificación de actos racistas y xenófobos cometidos por medio de sistemas informáticos (Estrasburgo, 28 de enero de 2003).

Cabe señalar que está en marcha un proceso para integrar en la legislación la directiva de la Unión Europea relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información. Esta

directiva es de suma importancia para mejorar la resiliencia frente a los ataques cibernéticos a nivel nacional y establece una serie de obligaciones para todos los Estados miembros de la Unión Europea que son pertinentes para este fin y también incluye la adopción de una estrategia nacional sobre la seguridad de las redes y los sistemas de información.

Según la información proporcionada por el Ministerio de Defensa, el enfoque de la ciberseguridad de Grecia consiste en desarrollar una amplia gama de capacidades para defender las infraestructuras y las redes nacionales contra los ciberdelincuentes y las ciberamenazas más recientes. Esto incluye abordar la ciberdefensa al más alto nivel estratégico en el marco de las organizaciones relacionadas con la defensa del país, una mayor integración de la ciberdefensa en las operaciones y la ampliación de la cobertura a redes desplegables. Se han adoptado las siguientes medidas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional:

a) Se está elaborando un marco nacional de estrategia de defensa cibernética y la estrategia de ciberseguridad nacional que regula el marco general de seguridad cibernética y define las medidas necesarias para el mantenimiento de los requisitos mínimos de ciberseguridad se encuentra en proceso de convertirse en ley;

b) La defensa cibernética ya forma parte de los planes de operaciones de la defensa nacional y el sistema de alerta de emergencias nacional se ha incorporado en la mayoría de los documentos normativos en relación con los sistemas de información y se ha integrado en todos los grandes ejercicios nacionales. La ciberseguridad se ha incluido en los planes de operaciones para períodos de crisis de todas las organizaciones públicas;

c) Grecia ha desarrollado su capacidad de respuesta ante incidentes o emergencias bajo la dirección del Centro de Respuesta a Incidentes Informáticos Militares, y la actualiza constantemente. Los equipos de reacción rápida pueden desplegarse en un breve plazo para ayudar a responder a los incidentes cibernéticos en el ejército o las redes públicas y contribuir a la recuperación. Se han integrado instrucciones para la recuperación después de averías o ataques cibernéticos en los documentos normativos de seguridad de la información computerizada;

d) Se está construyendo un centro de operaciones de ciberseguridad para los sistemas de redes nacionales de defensa militar y a nivel nacional hay cuatro equipos de respuesta a emergencias cibernéticas, que se ocupan de los sectores público y privado.

Las medidas que podría adoptar la comunidad internacional a fin de lograr un mayor nivel de seguridad de la información son las siguientes:

a) Incremento de la capacidad de respuesta ante incidentes, la capacidad de vigilancia de redes y la defensa viable contra las amenazas cibernéticas mediante centros de operaciones nacionales de ciberseguridad en pleno funcionamiento;

b) Plena integración de la ciberdefensa en las operaciones;

c) Elaboración de estrategias nacionales de ciberseguridad y ciberdefensa;

d) Mayor concienciación sobre temas cibernéticos del personal empleado en ciberdefensa y mejora de la capacidad técnica;

e) Capacitación continua del personal empleado en organizaciones de ciberdefensa;

f) Armonización de la legislación nacional con las leyes y directrices mundiales sobre ciberseguridad.

Según la información facilitada por la policía griega, la misión de la División de Delitos Cibernéticos, de conformidad con el artículo 30 del decreto presidencial núm. 178/2014, incluye la prevención, investigación y enjuiciamiento de los delitos cometidos a través de Internet o de otros medios de comunicación electrónica. La División de Delitos Cibernéticos es un servicio central autónomo y está directamente encomendada al director del cuerpo general de la policía griega.

Una de las unidades de la División es responsable de la seguridad de las comunicaciones electrónicas y telefónicas y de la protección de los derechos de autor y los programas informáticos. Más concretamente, la unidad investiga los casos de penetración ilegal de sistemas informáticos y el robo, la destrucción o el tráfico de programas informáticos, datos digitales y obras audiovisuales en todo el país.

La División de Delitos Cibernéticos de la policía griega colabora estrechamente con la Autoridad Nacional contra los Ataques Electrónicos, que forma parte del Servicio Nacional de Inteligencia. La misión de la Autoridad Nacional es encargarse de prevenir y contrarrestar de forma activa y pasiva los ataques electrónicos contra las redes de comunicación, las instalaciones de almacenamiento de datos y los sistemas de tecnología de la información y las comunicaciones. Además, la Autoridad se ocupa de procesar los datos y notificar a las autoridades competentes.

Japón

[Original: inglés]
[27 de julio de 2017]

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. Las actividades del Japón se ajustan a los siguientes cinco principios: la libre circulación de la información, el estado de derecho, la apertura, el autogobierno y un enfoque de múltiples interesados.

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

Las iniciativas del Japón se basan en los tres pilares siguientes: la promoción del estado de derecho en el ciberespacio, las medidas de fomento de la confianza y el desarrollo de la 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 la elaboración de normas voluntarias y no vinculantes. Estas normas son la base para garantizar la estabilidad y la previsibilidad de la comunidad internacional. Habida cuenta de las características singulares de la tecnología de la información y las comunicaciones, es necesario continuar aclarando la forma en que se aplicarían las distintas normas y principios.

Para impulsar las medidas de fomento de la confianza, es preciso garantizar la transparencia y el intercambio de información; sin embargo, el nivel de las medidas adoptadas varía de un Estado a otro, ya que cada Estado tiene autoridad para determinar el nivel que puede lograr. El Japón promueve las medidas de fomento de la confianza mediante el diálogo bilateral y los marcos multilaterales, como el Foro Regional de la Asociación de Naciones de Asia Sudoriental. Es necesario estudiar formas que conduzcan a una cooperación tangible.

En lo que respecta a la creación de capacidad, el Japón ha promovido la elaboración de leyes, estatutos y marcos normativos para la ciberseguridad y ha trabajado para garantizar la seguridad cibernética de los órganos gubernamentales y los operadores de infraestructuras de información vitales; tomar medidas contra los delitos cibernéticos; desarrollar los recursos humanos a fin de contar con expertos en seguridad cibernética; y fomentar la investigación y el desarrollo de tecnologías de ciberseguridad. Sobre la base de esas experiencias y conocimientos acumulados, el Japón seguirá cooperando activamente en el desarrollo de la capacidad.

Jordania

[Original: árabe]
[23 de marzo de 2017]

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 país, en particular en las fronteras. Utiliza esas redes para fortalecer 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 denominado Ejército Árabe, 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 mejorar la 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.

Debería prestarse una atención constante a la concienciación de los ciudadanos sobre las amenazas cibernéticas dominantes y a la forma en que las medidas de ciberseguridad pueden minimizar y contrarrestar esas amenazas en el uso de sistemas electrónicos. Cuando se maneja cualquier tipo de información, es fundamental ser conscientes de la necesidad de extremar la seguridad, siempre que ello no impida hacer un uso adecuado de la tecnología.

Para proteger las redes de información nacional 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 (intranets);

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.

Jordania propone que se adopten las siguientes medidas a nivel mundial:

a) Clasificación por importancia de las redes de comunicaciones y la información;

b) Aplicación de medidas de ciberseguridad y protección;

c) Aplicación del principio de la necesidad de saber;

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

e) Verificación y categorización de los usuarios y los permisos de acceso a la red;

f) Utilización de dispositivos periféricos independientes para conectar las redes;

g) En algunos casos, utilización de conexiones de intranet, evitando el uso de Internet en la medida de lo posible;

h) Mejora de la intranet de las Naciones Unidas, separada de las redes públicas, y protegida con medidas técnicas y de seguridad como el cifrado, las salvaguardias y la verificación de los permisos de acceso;

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

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

Jordania quisiera hacer 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 sobre cultivos a los agricultores.

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 sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional que se creó en 2003;

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.

Madagascar

[Original: francés]
[20 de junio de 2017]

Las recomendaciones de las Naciones Unidas se basan en la seguridad internacional, con los propósitos siguientes:

– La realización de estudios destinados a fortalecer la seguridad de los sistemas informáticos mundiales y de los sistemas mundiales de telecomunicaciones;

– La evaluación de todas las amenazas que existen o podrían existir en la esfera de la seguridad informática y la adopción de estrategias apropiadas para hacerles frente;

– La colaboración de las instancias gubernamentales dedicadas al fortalecimiento de la seguridad informática, con el fin de elaborar una visión común de la seguridad a escala mundial;

La resolución 71/28 se refiere específicamente al ámbito de la informática y las telecomunicaciones, que está en pleno auge en Madagascar. La respuesta a esta resolución precisa la opinión de expertos en ese ámbito.

Países Bajos

[Original: inglés]
[31 de mayo de 2017]

Los Países Bajos acogen con satisfacción la oportunidad de ofrecer su respuesta a la resolución 71/28 de la Asamblea General.

El ciberespacio y en particular Internet son un recurso fundamental para el crecimiento económico y social. La creciente importancia del ciberespacio ha planteado nuevos desafíos a la comunidad mundial. Al estar profundamente interconectadas y depender de Internet y la tecnología de la información y las comunicaciones, las sociedades ahora son más vulnerables al uso indebido de estas tecnologías. Las tensiones geopolíticas se manifiestan en el ciberespacio y los Estados y otros agentes utilizan con mayor frecuencia las operaciones cibernéticas para conseguir sus intereses estratégicos. Sin embargo, esas operaciones cibernéticas pueden ser causa de inestabilidad en las relaciones internacionales y podrían suponer un riesgo para la paz y la seguridad internacionales.

La necesidad de la cooperación internacional para reducir esos riesgos está clara. En vista de lo anterior, los Países Bajos están intensificando su participación en la ciberdiplomacia para mantener la paz y la estabilidad en el ciberespacio, promover el orden jurídico internacional y fomentar una cultura de seguridad colaborativa, como se indica en su ciberestrategia internacional, titulada "Construcción de puentes digitales".

La comunidad internacional está adoptando medidas para contrarrestar esos riesgos. Los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional son sumamente importantes a ese respecto. Los Países Bajos también se precian de estar en condiciones de contribuir al Grupo de Expertos Gubernamentales de 2017.

Los Países Bajos siguen promoviendo un diálogo inclusivo sobre el comportamiento responsable de los Estados en el ciberespacio, defienden los derechos humanos en línea y fomentan el desarrollo de la capacidad mediante diversas actividades. Los Países Bajos han emprendido diversas iniciativas, en particular:

a) Siguiendo la tradición de apoyar el desarrollo del orden jurídico internacional, los Países Bajos organizaron una serie de consultas entre asesores jurídicos estatales dedicadas al Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas;

b) Los Países Bajos prestaron su apoyo al Instituto de las Naciones Unidas de Investigación sobre el Desarme en la organización de una serie de tres talleres sobre normas de comportamiento en el ciberespacio, derecho internacional y lucha contra la propagación de herramientas y técnicas malintencionadas, en los que se logró reunir a diplomáticos y representantes de la comunidad tecnológica;

c) Por último, los Países Bajos pusieron en marcha numerosas iniciativas para promover las normas de orientación, entre ellas la Comisión Mundial sobre la Estabilidad del Ciberespacio, que elaborará propuestas de normas y políticas encaminadas a mejorar la seguridad y la estabilidad internacionales.

Todos estos esfuerzos están destinados a incrementar la estabilidad y seguridad de las relaciones internacionales digitalizadas y el propio ciberespacio, que los Países Bajos consideran fundamental para reducir el riesgo de conflictos y hacer que el ciberespacio siga siendo abierto, libre y seguro.

Noruega

[Original: inglés]
[27 de julio de 2017]

Noruega es uno de los países más digitalizados del mundo y depende cada vez más de un ciberespacio seguro y que funcione adecuadamente. Está firmemente comprometida con un ciberespacio libre, abierto, pacífico y seguro, de forma que sus beneficios económicos y sociales estén protegidos y disponibles para todos. El ciberespacio no conoce fronteras nacionales y la seguridad en el ciberespacio solo puede garantizarse a escala internacional, mediante una estrecha cooperación entre los Estados y el sector privado.

Medidas adoptadas para fortalecer la seguridad de la información

Enfoques nacionales

El Gobierno ha publicado un libro blanco titulado “Seguridad de la TIC: una responsabilidad compartida” (2016-2017), que incluye planes para establecer un marco nacional con vistas a incrementar la coordinación entre los agentes pertinentes a nivel nacional y la creación de una plataforma técnica para mejorar el intercambio de información entre entidades públicas y privadas.

El 31 de marzo de 2017 se creó el Centro Combinado de Coordinación Cibernética de los servicios de seguridad e inteligencia.

Enfoques internacionales

Las amenazas cibernéticas constituyen una parte sustancial del libro blanco del Gobierno sobre los retos de seguridad mundial en su política exterior (2014-2015).

Noruega está a punto de lanzar una estrategia internacional para el ciberespacio aplicable al país.

Noruega participa en varias iniciativas de cooperación regional relacionadas con las cuestiones cibernéticas, tales como:

a) La labor en el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE) con respecto a la elaboración de normas y medidas de fomento de confianza para reducir el riesgo de conflictos derivados de la utilización de la tecnología de la información y las comunicaciones (TIC);

b) Una estrecha cooperación con el Centro de Excelencia de Cooperación en Ciberdefensa de la Organización del Tratado del Atlántico del Norte establecido en Tallin, incluida la aplicación del derecho internacional en la esfera cibernética y la formulación de la doctrina;

c) El Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Noruega respalda el trabajo de los Grupos de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

También participa en diálogos bilaterales y regionales sobre cuestiones cibernéticas, especialmente entre los Estados nórdicos.

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

Noruega considera que el derecho internacional es aplicable en el ciberespacio y que el respeto por los Estados del derecho internacional, en particular de las obligaciones contraídas en virtud de la Carta de las Naciones Unidas, es un marco

esencial para sus acciones en materia de utilización de la TIC. La comunidad internacional debe estudiar más a fondo la aplicación del derecho internacional en el ámbito cibernético, así como las normas de conducta responsable en el ciberespacio.

La sostenibilidad de Internet a nivel mundial depende de un equilibrio adecuado entre apertura, seguridad, solidez y libertad. Este equilibrio solo puede garantizarse mediante la cooperación y el diálogo internacionales, a nivel mundial y regional. Debe continuar la labor en curso sobre este tema en foros como las Naciones Unidas, la Unión Europea, la Organización de Cooperación y Desarrollo Económicos y la OSCE.

Los derechos humanos universales también son aplicables en la esfera cibernética. Los mismos derechos de que gozan las personas fuera de Internet también deben ser protegidos en línea, en particular la libertad de expresión, incluidos el derecho a la intimidad y la libertad de buscar, recibir y transmitir información.

Paraguay

[Original: español]
[31 de julio de 2017]

El Paraguay comparte la idea de que la seguridad de la información es un ámbito de creciente importancia a nivel mundial, pues existe una mayor dependencia de los Gobiernos sobre las tecnologías de la información y las comunicaciones y el ciberespacio. La respuesta a la evolución de los ataques cibernéticos debe ser conjunta, dinámica y proporcional. Sin una respuesta estratégica a nivel global, los esfuerzos de un país en materia de seguridad cibernética serán insostenibles, esporádicos, duplicados e ineficientes.

Para fortalecer la seguridad de la información a nivel nacional, en abril de 2017 el Gobierno del Paraguay aprobó el plan nacional de ciberseguridad, cuya elaboración involucró directamente a representantes de todos los sectores que tienen roles e intereses en el ciberespacio. El plan sirve como base para las políticas gubernamentales y nacionales sobre el tema y establece las líneas de acción a ser adoptadas por el Paraguay para fortalecer la seguridad de sus activos críticos y lograr un ciberespacio seguro, confiable y resiliente. Los delitos informáticos están tipificados en la legislación penal paraguaya. El Paraguay alberga desde hace cinco años el Congreso y Feria Iberoamericana de Seguridad de la Información, un foro para compartir experiencias, conocer novedades y evaluar soluciones a los desafíos que genera el crecimiento del uso de las tecnologías de la información y las comunicaciones.

En el ámbito subregional, el Mercado Común del Sur (MERCOSUR) posee una instancia permanente, llamada Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica del MERCOSUR, para proponer políticas e iniciativas comunes en el área de seguridad cibernética. Por su parte, la región de las Américas cuenta con una Estrategia Interamericana Integral de Seguridad Cibernética, que reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad, a fin de crear una cultura de seguridad cibernética.

Un marco eficaz para la protección de las redes y los sistemas de información a escala mundial que integran Internet y para responder a incidentes y recuperarse de los mismos dependerá de que la comunidad internacional adopte las siguientes medidas:

– Proporcionar información a los usuarios para que protejan sus sistemas de información contra amenazas y vulnerabilidades;

– Fomentar asociaciones públicas y privadas con el fin de incrementar la educación y la concientización;

– Identificar y evaluar normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por las redes de comunicación y promover la adopción de las mismas;

– Promover la adopción de políticas y legislación sobre delitos cibernéticos que protejan a los usuarios y prevengan y disuadan el uso indebido e ilícito de equipos informáticos, respetando a su vez la privacidad de los derechos individuales de los usuarios.

Portugal

[Original: inglés]
[27 de julio de 2017]

En su resolución 71/28 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. Los progresos en las esferas de la información y las telecomunicaciones suponen un aumento de las oportunidades para el desarrollo de conocimientos, la cooperación entre los Estados, la promoción de la creatividad humana y la difusión de la información en la comunidad en su conjunto; por otra parte, Portugal considera que estas tecnologías y estos medios podrían utilizarse de maneras contrarias a la estabilidad y la seguridad internacionales y podrían afectar negativamente a la integridad de los Estados.

En la resolución 71/28 se pidió a los Estados Miembros que proporcionasen información en cuatro esferas:

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.

En su informe de 2013 (A/68/98), el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional presentó algunas recomendaciones sobre las siguientes esferas: normas, reglas y principios de conducta estatal responsable; medidas de fomento de la confianza y el intercambio de información; y medidas de creación de capacidad.

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

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

Portugal considera que la seguridad de la información en red es importante y ha ido creciendo.

Conviene 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 conllevan el requisito de comunicar las violaciones de la seguridad o la pérdida de integridad que tengan repercusiones importantes en el funcionamiento de los servicios.

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

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

Medidas de fomento de la confianza e intercambio de información

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.

En el plano nacional, Portugal se ha centrado en la realización de ejercicios conjuntos en los que participaron entidades públicas y privadas; en la promoción de la normalización técnica; y en la organización de conferencias y seminarios, algunos de ellos con participación de oradores internacionales.

Medidas de creación de capacidad

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

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

Qatar

[Original: inglés]
[4 de mayo de 2017]

El Estado de Qatar reconoció hace algún tiempo que la seguridad de la información o ciberseguridad no es solo una cuestión de tecnología, sino también una cuestión de política nacional. A este respecto se creó en 2005 el equipo de respuesta a emergencias cibernéticas de Qatar (véase www.Qcert.org) para catalizar el cambio y, en particular, para acelerar la adopción generalizada de prácticas y políticas eficaces de ciberseguridad. En la actualidad, el equipo tiene un mandato nacional para salvaguardar los activos digitales del Estado de Qatar.

En 2013, el Primer Ministro creó un Comité de Ciberseguridad Nacional. El Comité ha elaborado una estrategia nacional de ciberseguridad con el fin de mejorar las medidas de seguridad de Qatar y asegurar la continuidad del éxito y el crecimiento de la nación basándose en cinco pilares que determinan las medidas que se adoptarán:

- Salvaguardar la infraestructura nacional de información crítica;

- Afrontar y resolver ataques e incidentes cibernéticos y recuperarse de ellos mediante el intercambio de información, la colaboración y las acciones a su debido tiempo;
- Establecer un marco jurídico y regulatorio para lograr un ciberespacio seguro y dinámico;
- Fomentar una cultura de ciberseguridad que promueva el uso seguro y adecuado del ciberespacio;
- Perfeccionar y cultivar las capacidades nacionales en materia de ciberseguridad.

El equipo de respuesta a emergencias cibernéticas ha prestado diferentes servicios de seguridad de la información para satisfacer las necesidades de los electores, las empresas y las organizaciones del país, especialmente en materia de respuesta a los incidentes, inteligencia, resiliencia, formación y sensibilización, gestión de crisis, concesión de licencias de infraestructuras públicas fundamentales e identidad, y de creación del marco nacional de cumplimiento de la seguridad de la información.

Qatar considera que actualmente existe una laguna en la capacidad de los Estados de lograr y compartir una conciencia situacional cibernética suficiente en los planos regional e internacional con vistas a permitir la adopción de decisiones eficaces. Es necesario seguir trabajando en la colaboración para la prevención con el fin de lograr una mayor seguridad cibernética en el ámbito de los servicios e infraestructuras de tipo cibernético de modo que se asegure la resiliencia, especialmente en relación con las operaciones cotidianas de los Gobiernos, servicios, empresas, consumidores y ciudadanos.

La ciberseguridad nunca es más eficaz que cuando se intercambia información. Sería muy útil que los Estados trabajasen para llegar a acuerdos de intercambio de información mediante marcos de colaboración que describan metodologías de verificación y cumplimiento.

Se producirán ataques y las naciones, los Gobiernos, las organizaciones y las empresas deben estar preparados, de forma conjunta.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[31 de julio de 2017]

El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con beneplácito la oportunidad de presentar su respuesta a la resolución 71/28 de la Asamblea General relativa a los 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 2016 a la resolución 70/237. 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 para proteger la infraestructura nacional e internacional crítica y una base indispensable para la actividad económica y social en Internet. Las amenazas reales y potenciales que plantean las actividades en el ciberespacio siguen siendo motivo de gran preocupación. La nueva estrategia nacional de ciberseguridad, publicada en octubre de 2016, dará forma en los próximos cinco años a las actividades del país destinadas

a defender sus activos, disuadir a sus adversarios y desarrollar su sector de ciberseguridad.

El Reino Unido sigue desempeñando un papel principal en el debate internacional sobre ciberseguridad. Proporcionó expertos para los cinco Grupos de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A pesar de la falta de consenso en el Grupo de 2017, el país se ha comprometido a promover un marco de estabilidad internacional para el ciberespacio sobre la base de la aplicación del derecho internacional vigente, normas voluntarias acordadas de comportamiento responsable de los Estados y medidas de fomento de la confianza, con el apoyo de programas coordinados de creación de capacidad. El Reino Unido también acoge con beneplácito los esfuerzos de la Organización para la Seguridad y la Cooperación en Europa y otros foros regionales con el fin de formular propuestas para aplicar medidas de fomento de la confianza y tratará de seguir predicando con el ejemplo en la adopción de esas medidas.

Esta respuesta reafirma el trabajo que realiza el Reino Unido para apoyar y mejorar la ciberseguridad y difundir las mejores prácticas en el plano nacional y en todo el mundo, en particular mediante la colaboración con asociados internacionales para abordar la ciberdelincuencia, los grandes incidentes y la creación de capacidad. El Reino Unido espera con interés que se continúe avanzando y se complace en participar activamente en estas cuestiones. Asimismo, seguirá participando plenamente en el fortalecimiento de la capacidad y la cooperación internacional en materia de ciberseguridad.

Singapur

[Original: inglés]
[31 de julio de 2017]

Como Estado pequeño y con un alto nivel de interconexión, Singapur apoya un ciberespacio seguro y resistente, respaldado por el derecho internacional, normas bien definidas de comportamiento responsable de los Estados e iniciativas coordinadas de creación de capacidad para cumplir esas normas. Se precisa una cooperación internacional sólida para hacer frente a los nuevos desafíos planteados por las amenazas cibernéticas y Singapur desempeñará el papel que le corresponde.

Singapur creó el Organismo de Ciberseguridad en 2015 para supervisar de forma centralizada las funciones nacionales de seguridad cibernética. En la estrategia de ciberseguridad de Singapur, que se puso en marcha en octubre de 2016, se describe un enfoque holístico de la protección de los servicios esenciales frente a las amenazas cibernéticas y de la creación de un ciberespacio seguro. La estrategia se sustenta en cuatro pilares: construir una infraestructura resiliente; crear un ciberespacio más seguro; desarrollar un ecosistema de ciberseguridad dinámico; e intensificar las alianzas internacionales.

En el plano regional, Singapur está trabajando para crear e incrementar la capacidad entre sus vecinos. Ha puesto en marcha un programa de capacidad cibernética de 10 millones de dólares singapurenses en colaboración con la Asociación de Naciones de Asia Sudoriental (ASEAN) para complementar las iniciativas regionales de desarrollo de la capacidad. En el marco de este programa, Singapur organizó un taller de la ASEAN sobre normas cibernéticas en mayo de 2017 y celebrará un taller de la ASEAN sobre desarrollo de capacidad en materia de ciberseguridad en agosto de 2017. También organiza anualmente la Semana Cibernética Internacional de Singapur, que comprende la Conferencia Ministerial de la ASEAN sobre Ciberseguridad y el Simposio Internacional de Líderes

Cibernéticos, para que los dirigentes mundiales de los Gobiernos, las empresas y las instituciones académicas puedan dialogar con homólogos de la región y debatir las cuestiones emergentes y transversales.

En el ámbito de la cooperación multilateral, Singapur apoya el trabajo del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, incluidas las 11 normas que figuran en su informe de 2015. Es importante definir y aplicar las normas que gozan de un amplio acuerdo, sobre todo las normas operacionales. Estas normas incluyen, entre otras cosas, no prestar apoyo a las actividades en línea que dañen intencionadamente infraestructuras vitales; no apoyar las actividades que impidan que los equipos de respuesta a emergencias cibernéticas respondan a incidentes cibernéticos; y no utilizar esos equipos de respuesta para participar en actividades internacionales malintencionadas.

Turquía

[Original: inglés]
[31 de julio de 2017]

Las tecnologías de la información y las comunicaciones (TIC) se han convertido en parte esencial de la sociedad y la vida económica de hoy. Contribuyen a la riqueza y el desarrollo sociales, así como a la vida cotidiana de las personas. Hay un amplio espectro de usuarios, como los sectores público y privado, los sectores de infraestructuras vitales y las personas, y su utilización se ha extendido por todo el país y el mundo a pesar de los riesgos de ciberseguridad.

En este contexto, Turquía ha participado en numerosas iniciativas para contribuir a las actividades de cooperación en materia de seguridad cibernética con el objetivo de garantizar la ciberseguridad. En este contexto, se realizaron ejercicios nacionales de ciberseguridad bajo la coordinación del Ministerio de Transporte, Asuntos Marítimos y Comunicaciones, se llevó a cabo el primer Ejercicio de Escudo Cibernético Internacional en Estambul, y Turquía ha participado de forma periódica y anual en ejercicios internacionales relacionados con la seguridad cibernética, a saber, la Coalición Cibernética de la Organización del Tratado del Atlántico del Norte (OTAN), el ejercicio Locked Shields de la OTAN y el Ejercicio de Gestión de Crisis de la OTAN.

El diálogo y la cooperación con las Naciones Unidas, la OTAN, la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa y otras organizaciones internacionales y no gubernamentales, las instituciones académicas y los líderes de opinión se han intensificado. Este enfoque se refuerza con conferencias, cursos, seminarios, reuniones, cursos de posgrado y otros programas de apoyo. Turquía lidera los esfuerzos regionales de seguridad cibernética mediante la concertación de acuerdos bilaterales con diversos Estados.

El memorando de entendimiento en el que se describe la cooperación entre la OTAN y sus aliados fue aprobado por el Comité de Ciberdefensa de la OTAN y están en curso los trámites relacionados con su firma. Turquía es país patrocinador del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN. Se realiza un seguimiento de la labor del Comité de Planificación de Emergencias Civiles de la OTAN y las reuniones del Centro Regional de Asistencia para la Verificación y Aplicación de Medidas de Control de Armamentos y se coopera en varias cuestiones. Turquía es socio fundador del Foro Mundial de Competencia Cibernética y es parte en el documento marco y la Declaración de La Haya sobre el Foro Mundial.

En la Cumbre del Grupo de los 20 celebrada en Turquía los días 15 y 16 de noviembre de 2015 se adoptó una decisión sobre ciberseguridad que hacía hincapié en la labor del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

Turquía firmó el Convenio sobre la Ciberdelincuencia del Consejo de Europa en Estrasburgo en 2010 y lo ratificó mediante la Ley núm. 6533 de 2014; posteriormente se llevó a cabo su adaptación a la legislación nacional.

Como resultado de la recopilación, el examen y la evaluación de la información generada en el ámbito de las reuniones y las plataformas de sentido común, se prepararon una estrategia nacional de ciberseguridad y un plan de acción para el período 2016-2019.

El fortalecimiento de la seguridad de la información a nivel mundial y, por ende, el desarrollo de una cultura de la seguridad en el seno de la comunidad internacional son cuestiones cruciales para todos. Al mismo tiempo, cada Estado tiene derecho a adoptar medidas para protegerse del uso malintencionado de las tecnologías de la información y las comunicaciones por terroristas, extremistas, grupos delictivos organizados y piratas informáticos independientes y preservar la seguridad nacional. En ese contexto, el fortalecimiento de la legislación internacional y la mejora de los acuerdos bilaterales internacionales tienen también gran importancia.