Naciones Unidas A/70/172

Asamblea General

Distr. general
22 de julio de 2015
Español
Original: árabe/español/inglés

Septuagésimo período de sesiones
Tema 93 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/70/150.

15-12333 (S) 050815 240815

I. Introducción

1. El 2 de diciembre de 2014, la Asamblea General aprobó la resolución 69/28, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”. En el párrafo 3 de la resolución, la Asamblea invitó a todos los Estados Miembros, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe de la Cuarta Conferencia Mundial sobre el Ciberespacio (A/68/98), 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 2 de febrero de 2015 se envió a todos los Estados Miembros una nota verbal en la que se les invitó a proporcionar información sobre el tema. En la sección II figuran las respuestas recibidas hasta el momento de preparar el presente informe. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los gobiernos

Alemania

[Original: inglés]
[27 de mayo de 2015]

El acceso abierto, libre, seguro y fiable a Internet ofrece grandes oportunidades para el crecimiento económico, el desarrollo social y el progreso científico, así como para la promoción de la democracia, la buena gobernanza y el Estado de derecho. Al mismo tiempo, aumenta la preocupación por los riesgos para la seguridad internacional que se originan en el ciberespacio. En los últimos meses se ha observado un incremento del uso de programas informáticos maliciosos contra blancos muy visibles, como medios de comunicación. Los ataques contra infraestructuras esenciales, en particular, podrían tener consecuencias graves.

Por el momento no parece probable que se desate una guerra cibernética en toda regla. Sin embargo, el uso limitado de las capacidades cibernéticas como parte de una empresa bélica más amplia, incluso en el contexto de conflictos híbridos, ya es una realidad. Además, los incidentes que ocurren en el ciberespacio pueden acabar en conflictos en el mundo real.

Alemania propone que se adopte una estrategia en tres vertientes para maniobrar en ese entorno: acordar normas de comportamiento responsable de los

Estados en el ciberespacio, adoptar medidas de fomento de la confianza y aumentar la resiliencia en el ciberespacio.

Las Naciones Unidas son el foro apropiado para establecer normas de comportamiento responsable de los Estados en el ciberespacio. Un punto de partida importante es el consenso al que llegó el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2012-2013 en el sentido de que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable en el ciberespacio. El Grupo de Expertos Gubernamentales de 2014-2015, en el que Alemania ha vuelto a participar activamente, ha seguido trabajando sobre esa base.

Un entendimiento común de las reglas, normas y principios de comportamiento responsable de los Estados en el ciberespacio podría aumentar la transparencia y la previsibilidad en el plano internacional y contribuir así a la paz y la estabilidad. Sería útil, por ejemplo, fomentar una mejor comprensión de la manera en que el derecho de los conflictos armados se aplica al uso de las capacidad cibernéticas militares que viene desarrollando un número cada vez mayor de Estados.

En cuanto al fomento de la confianza, Alemania concede gran importancia a las organizaciones regionales. En 2013, la Organización para la Seguridad y la Cooperación en Europa acordó un conjunto inicial de medidas de fomento de la confianza en el ámbito del ciberespacio. Su aplicación avanza sin trabas y se está negociando un segundo conjunto de medidas relativas al fomento de la confianza y la cooperación. Alemania prevé priorizar la ciberseguridad durante el período en que ocupe la presidencia de la organización.

Alemania está preparando una ley de seguridad de las tecnologías de la información para aumentar la resiliencia en el ciberespacio a nivel nacional. En el anteproyecto de ley se definen los requisitos mínimos para garantizar la seguridad informática de las infraestructuras esenciales. Se establece también la obligación de informar sobre incidentes significativos a fin de reforzar la seguridad de los sistemas y la protección del público en general. Además, Alemania ofrece su apoyo a otros Estados para que aumenten su capacidad de gestionar riesgos en materia de ciberseguridad.

El texto completo de la presentación de Alemania puede consultarse en www.un.org/disarmament/topics/informationsecurity/.

Canadá

[Original: inglés]
[4 de junio de 2015]

El ciberespacio ha mejorado la interacción social y ha transformado las industrias y los gobiernos y sigue siendo un motor del crecimiento económico, la innovación y el desarrollo social. También ha introducido nuevas amenazas y desafíos en nuestra sociedad.

El Canadá reitera la afirmación clara hecha por los Estados en el informe de 2013 del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional sobre la

aplicabilidad del derecho internacional al ciberespacio como piedra angular de las normas y los principios de comportamiento responsable de los Estados, y alienta a que continúe la labor con respecto a las normas en tiempos de paz.

El Canadá también considera que abordar la cuestión de la seguridad de la tecnología de la información y las comunicaciones debe ir de la mano con el respeto de los derechos humanos y las libertades fundamentales. Los derechos que las personas disfrutan cuando no están conectados también deben ser protegidos en línea.

El Canadá expresa su determinación de mantener el carácter libre, abierto y seguro de Internet con las medidas siguientes:

a) La aplicación de la estrategia y el plan de acción sobre ciberseguridad del Canadá sigue siendo una de las tareas principales en el plano nacional. De esa manera se procura garantizar la seguridad de los cibersistemas del país y proteger a los canadienses en línea mediante una colaboración activa con los sectores de infraestructuras esenciales (por ejemplo, las finanzas, el transporte y la energía);

b) El Canadá ha desarrollado un marco de gestión de incidentes cibernético que constituye un enfoque nacional unificado de la gestión y coordinación de la respuesta a amenazas e incidentes cibernéticos reales o potenciales;

c) La nueva legislación contra el envío de correos basura (*spam*) del Canadá contribuye a aclarar las obligaciones en materia de derechos y las funciones respectivas de los organismos gubernamentales y a reforzar las disposiciones legislativas relativas a la aplicación de la ley y la colaboración internacional;

d) En el plano internacional, el Canadá se ha comprometido a aportar 8 millones de dólares canadienses para proyectos de desarrollo de la capacidad en materia de seguridad cibernética, principalmente en América y en el sudeste de Asia. El Canadá también ha proporcionado más de 3,6 millones de dólares canadienses por conducto de la Organización de los Estados Americanos (OEA) (2007-2016) para el desarrollo de la capacidad en países de la OEA, asistencia que incluye la creación de equipos de respuesta a incidentes de seguridad informática. El Canadá también se incorporó, como miembro fundador, al Foro Mundial de Competencia Cibernética;

e) El Canadá apoya los esfuerzos que despliega la Organización del Tratado del Atlántico del Norte para fortalecer la ciberseguridad de la alianza y de los distintos países aliados;

f) El Canadá trabaja en el marco del Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN) para crear capacidad en lo que atañe a la importancia de las medidas de transparencia y fomento de la confianza para lograr la estabilidad en el ciberespacio;

g) Mediante el plan de acción sobre seguridad cibernética entre el Canadá y los Estados Unidos de América, el Canadá colabora con los Estados Unidos para mejorar la capacidad de adaptación de nuestra infraestructura informática, así como los contactos, la colaboración y el intercambio de información a nivel operacional y estratégico;

h) El Canadá también participa en iniciativas para combatir el delito cibernético en el Grupo de los Siete, la Oficina de las Naciones Unidas contra la

Droga y el Delito, la OEA y la ASEAN y es miembro de la Alianza Mundial contra el Abuso Sexual de los Niños en Línea;

i) El Canadá recomienda que todos los Estados Miembros que deseen aumentar la ciberseguridad y prevenir la ciberdelincuencia se remitan al Convenio sobre la Ciberdelincuencia del Consejo de Europa;

El texto completo de la presentación del Canadá puede consultarse en www.un.org/disarmament/topics/informationsecurity/.

Cuba

[Original: español]
[26 de mayo de 2015]

Cuba comparte la preocupación que se expresa en la resolución 69/28 ante 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 hace énfasis en la necesidad de impedir la utilización de los recursos y las tecnologías de la información con fines delictivos o terroristas.

En este contexto, Cuba expresa su gran 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 novedosas 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 desfavorables para 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 III Cumbre de la CELAC, celebrada en Belén (Costa Rica) los días 28 y 29 de enero de 2015, se destacó la importancia de las tecnologías de la información y comunicación, incluido el Internet, así como de la innovación, como herramientas para fomentar la paz, promover el bienestar, el desarrollo humano, el conocimiento, la inclusión social y el crecimiento económico, subrayando su

contribución a la mejora de la cobertura y calidad de los servicios sociales. Igualmente se reafirmó el uso pacífico de las tecnologías de la información y las comunicaciones de forma compatible con la Carta de las Naciones Unidas y el derecho internacional, y nunca con el objetivo de subvertir sociedades ni crear situaciones con el potencial de fomentar conflictos entre Estados.

Sin embargo, esos esfuerzos son 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. Además, y no menos importante, laceran la soberanía de Cuba.

Cuba reitera que el empleo de la información con fines propagandísticos y desestabilizadores, con el propósito de subvertir el orden interno de otros Estados, violar su soberanía y realizar actos de intromisión e injerencia en sus asuntos internos, resulta una acción ilegal y debe cesar.

Reiteramos nuestro más enérgico rechazo al uso de las tecnologías de la información y las comunicaciones en contravención del derecho internacional y a todas las acciones de este carácter. Subrayamos la importancia de garantizar que el uso de dichas tecnologías sea plenamente compatible con los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional, en particular la soberanía, la no injerencia en los asuntos internos y las normas de convivencia entre los Estados, internacionalmente reconocidas.

Cuba reitera que la cooperación internacional es fundamental para enfrentar los peligros del uso indebido de las tecnologías 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.

Cuba espera que en el nuevo contexto de las relaciones bilaterales entre los dos países a partir de los anuncios realizados el 17 de diciembre de 2014 por los Presidentes Raúl Castro Ruz y Barack Obama, que incluyeron la decisión de restablecer las relaciones diplomáticas y de iniciar un proceso hacia la normalización de las relaciones, se ponga fin a estas políticas agresivas, así como 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.

Como parte del programa de informatización en Cuba, se celebró en nuestro país, del 18 al 20 de febrero del 2015, el primer taller de informatización y ciberseguridad bajo el tema “Por una sociedad informatizada”, el cual contó con la participación de más de 11.500 profesionales de las tecnologías de la información y las comunicaciones de todo el país. Una de las temáticas de este evento trató el tema de la seguridad, supervisión y enfrentamiento de las tecnologías de la información y las comunicaciones.

En Cuba, fue creado el Consejo de Informatización y Ciberseguridad, dirigido por la máxima instancia del Estado, el Gobierno y el Partido Comunista de Cuba, el cual tiene como finalidad proponer, coordinar y controlar las políticas y estrategias integrales sobre este proceso. Asimismo se trabaja en la creación de la unión de informáticos de Cuba.

Cuba apoyó la resolución 69/28 y continuará contribuyendo al desarrollo global pacífico de las tecnologías de la información y las telecomunicaciones y su empleo en bien de toda la humanidad.

El Salvador

[Original: español]
[21 de abril de 2015]

La Fuerza Armada de El Salvador, en el marco de la seguridad de la información y las telecomunicaciones, ha implementado la centralización de telecomunicaciones de voz, video y datos independientes a la red pública. Se ha adquirido y configurado un equipo perimetral de seguridad informática; asimismo, se cuenta con un sistema de encriptado para el manejo de la información de carácter oficial con el fin de proteger toda la información de cualquier agente externo que pretenda infiltrarse, así como de ataques cibernéticos.

España

[Original: español]
[29 de mayo de 2015]

España considera que las tecnologías de la información y las comunicaciones son sustento esencial de todas las sociedades en el mundo, pero su globalización conlleva serios riesgos y amenazas tales como el ciberespionaje, el ciberterrorismo, el “hacktivismo” y la ciberguerra.

Tras la creación del Consejo Nacional de Ciberseguridad, España sigue avanzando en el desarrollo de los planes derivados del Plan Nacional de Ciberseguridad que abordan el incremento de las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas.

En cuanto a la promoción de la cooperación internacional, España sigue participando activamente y hace un seguimiento pormenorizado de todas las iniciativas de carácter estratégico que afectan a la ciberseguridad, tanto en la Unión Europea como en los principales foros internacionales, como la Organización para la Seguridad y la Cooperación en Europa, la Organización del Tratado del Atlántico Norte y el Consejo de Europa.

España sigue defendiendo la importancia de las Naciones Unidas en el proceso tendente a alcanzar un consenso internacional en materia de ciberseguridad y apoya el desarrollo de un debate institucionalizado, incluyendo otros foros internacionales, que favorezca la cooperación regional y el establecimiento de estándares globales, mejoras prácticas, normas de conducta entre Estados y medidas de fomento de la confianza, con el objetivo último de garantizar la paz y la seguridad en el uso de las tecnologías de la información.

España considera que los Estados deberían lograr consensos en cuatro ámbitos de actuación. Primero, a través de medidas de fomento de la confianza que alcancen un carácter cooperativo cuyo objeto último sea fomentar la transparencia entre los

Estados en materia de ciberseguridad y las capacidades de neutralización de eventuales ataques detectados provenientes de terceros países.

En segundo lugar, España considera que los Estados deben seguir reflexionando sobre cómo interpretar y aplicar 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.

Asimismo, como tercer bloque de actuaciones, España considera que se debe reforzar la cooperación internacional mejorando los canales de comunicación, estableciendo mecanismos de coordinación de equipos de respuesta a emergencias cibernéticas, realizando ejercicios conjuntos, etc., y promoviendo mecanismos de cooperación judicial y policial.

Por último, se debe seguir fomentando el desarrollo de capacidades en los países que lo necesiten y prestar asistencia a los Estados beneficiarios para el desarrollo de leyes nacionales que establezcan normas de seguridad cibernética.

El texto completo de la presentación de España puede consultarse en www.un.org/disarmament/topics/informationsecurity/.

Georgia

[Original: inglés]
[26 de mayo de 2015]

El Gobierno de Georgia concede una gran prioridad a la información y la ciberseguridad en su agenda política y considera la lucha contra las amenazas cibernéticas parte integrante de la política nacional de seguridad, especialmente en vista de la amplia reforma de gobierno electrónico emprendida en todo el país y la mayor dependencia de instrumentos de tecnología de la información y las comunicaciones en su infraestructura esencial. Como expresión de esas preocupaciones, y a fin de reforzar la seguridad de la información, el Gobierno de Georgia ha introducido varias medidas estratégicas, jurídicas, organizativas e institucionales.

La primera estrategia nacional de ciberseguridad está expuesta en la estrategia y plan de acción sobre ciberseguridad para 2013-2015, que es el principal documento en que se esboza la política estatal de ciberseguridad y se establecen los objetivos estratégicos y principios rectores y las medidas y tareas. La ciberseguridad es una de las principales prioridades de la política de seguridad del Estado y la protección del ciberespacio se considera tan importante para la seguridad nacional como la protección del territorio, las aguas y el espacio aéreo.

Se dio un paso más en la institucionalización de la seguridad de la información con la creación en 2010 del Organismo de Intercambio de Datos del Ministerio de Justicia de Georgia, como principal entidad gubernamental encargada de elaborar y aplicar políticas y normas en el ámbito de la informática y la ciberseguridad y, en particular, de:

- Adoptar y aplicar políticas y normas de seguridad de la información en el sector público y la infraestructura esencial

- Cumplir el mandato relativo a la ciberseguridad creando el equipo nacional de respuesta a emergencias cibernéticas
- Prestar servicios de consultoría sobre la informática y la ciberseguridad, realizar auditorías de seguridad de la información y brindar servicios de ciberseguridad
- Realizar actividades de sensibilización sobre cuestiones de seguridad de la información y ciberseguridad

El marco jurídico y reglamentario de Georgia sobre la seguridad informática está formado por la Ley de Seguridad de la Información y su reglamentación complementaria aprobadas entre 2011 y 2012. Los principales conceptos empleados en las disposiciones legislativas de Georgia en que se detallan las políticas de seguridad de la información se derivan de la serie de normas 27000 de la Organización Internacional de Normalización. La Ley destaca determinados derechos y obligaciones con respecto a las infraestructuras esenciales en el proceso de aplicación de las políticas de seguridad de la información y establece mecanismos de cooperación con los equipos gubernamentales de respuesta a emergencias informáticas a nivel nacional.

Georgia ha adoptado medidas importantes para fomentar la cooperación internacional y compartir con sus asociados el conocimiento acumulado. Un ejemplo notable son los acuerdos de cooperación bilateral y memorandos de entendimiento concertados entre el Organismo de Intercambio de Datos y el Estado Mayor de la Unión Europea (Austria, Estonia, Polonia y otros países), así como con países vecinos (Azerbaiyán, Armenia, la República de Moldova, Turquía, etc.).

Georgia reconoce que los mecanismos de cooperación regionales e internacionales han cobrado una mayor importancia para hacer frente a los problemas de seguridad de la información. Con esa perspectiva, deberá trabajar para ampliar el número de actividades internacionales dedicadas a tratar esos temas de gran importancia, aumentar el nivel de confianza con los principales interesados y seguir elaborando doctrinas estratégicas y conceptos jurídicos en colaboración con la comunidad internacional.

Países Bajos

[Original: inglés]
[29 de mayo de 2015]

La comunidad internacional comparte el interés y la responsabilidad de garantizar que el ciberespacio siga teniendo un carácter abierto, libre y seguro. En opinión de los Países Bajos, la aceptación amplia y el respeto de un conjunto de normas de comportamiento responsable de los Estados contribuirían a mantener la seguridad. El Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional ha hecho una labor ingente en ese sentido. No obstante, sería conveniente seguir trabajando en las esferas siguientes y adoptar medidas concretas:

- Lograr que entre los Estados haya una mejor comprensión de la manera en que el derecho y las normas internacionales sobre el comportamiento de los Estados se aplican al ciberespacio, sobre todo el marco jurídico internacional

aplicable a las operaciones que se realizan en el ciberespacio que no traspasan el umbral de ataque armado.

- Definir normas o medidas adicionales de autocontrol o asistencia mutua, sobre todo la idea de establecer normas de protección especial para determinados sistemas y redes, como la infraestructura esencial que proporciona servicios básicos a la población civil, las estructuras de respuesta a incidentes civiles y ciertos componentes fundamentales de Internet a nivel mundial.
- Reforzar la capacidad jurídica, diplomática y normativa y el intercambio de buenas prácticas en el ámbito de la paz y la seguridad internacionales en el ciberespacio. El Foro Mundial de Competencia Cibernética, iniciado en La Haya durante la Cuarta Conferencia Mundial sobre el Ciberespacio, puede desempeñar un papel importante a ese respecto.

Dado que Internet se ha convertido en un activo estratégico para todos, es necesario sostener un debate internacional amplio sobre estas cuestiones. Los Países Bajos seguirán participando activamente en la promoción de ese diálogo.

El texto completo de la presentación de los Países Bajos puede consultarse en www.un.org/disarmament/topics/informationsecurity/.

Panamá

[Original: español]
[3 de junio de 2015]

La tecnología de la información y las comunicaciones de hoy en día crece a un ritmo muy acelerado. Esto hace que, poco a poco, toda la población conviva con tecnología y comunicaciones, de una forma más accesible.

Es un hecho que nuestras vidas están vinculadas a esta evolución de cómo se envía una comunicación y cómo se procesa la información.

Ante este escenario, el Gobierno de Panamá ha ido de la mano de esta corriente, adaptándola a las necesidades propias de este estamento de seguridad. Es por ello que dentro de este marco se han estado realizando mejoras tecnológicas para establecer una conectividad más eficiente y segura.

Dentro de todas estas mejoras, el Gobierno de Panamá ha ido desarrollando un plan de implementación de comunicaciones, desarrollado de forma gradual, que incluye elementos de redes, seguridad y telefonía. Estos elementos cumplen con requerimientos de estándares internacionales confirmados con los fabricantes de los mismos.

El Gobierno de Panamá protege la integridad de su información en la esfera de Internet, datos y telefonía con infraestructura basada en plataformas de cortafuegos a nivel interno y con la conexión hacia la red nacional de multiservicios.

El Gobierno de Panamá cuenta con sesiones de datos a nivel de cortafuegos de seguridad para garantizar la confidencialidad y protección de la información.

Consideramos que en la medida que se adapten los avances en las soluciones de telecomunicaciones con las necesidades de seguridad a nivel de estamentos de seguridad, se podrá disponer de herramientas que contribuyan a la armonía en la

esfera de la información, basada en acciones y medidas preventivas. Esta situación tecnológica debe aprovecharse por parte de los estamentos, dado que tenemos la misión de proteger la sociedad en los niveles locales e internacionales.

Perú

[Original: español]
[30 de junio de 2015]

Evaluación general de los temas relacionados con la seguridad de la información por parte de la Dirección de Informática

- La Red Corporativa de Datos de la Policía Nacional del Perú mantiene un control de sus diferentes sistemas con políticas de seguridad en diferentes niveles de su estructura orgánica y funcional.
- En lo que respecta a la seguridad de la información, la Red Corporativa de Datos ha sido tercerizada mediante el servicio de seguridad gestionada, que se administra por un centro de operaciones de seguridad.
- Se tiene previsto realizar trabajos de ingeniería de roles e identidades, lo cual permitirá contar con control de accesos únicos para usuarios, permitiendo trazabilidad y herramientas de auditoría.

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

Medidas preventivas

- Designación de usuarios administradores de redes
- Capacitación del personal en informática
- Licenciamiento de software para los servidores del centro de datos de la Policía Nacional
- Implementación de la “nube privada”
- Respaldo de información
- Implementación de sistema eléctrico redundante (a nivel de suministro de energía ininterrumpido)
- Renovación de tableros de distribución eléctrica y acometidas eléctricas
- Tercerización de la seguridad perimetral (externa) para casos de ataque o denegación de servicio

Contenido de los conceptos mencionados en el título de la resolución

- Mejoramiento de la plataforma tecnológica de la Policía Nacional y de los sistemas de información policial, orientados a consolidar los medios de información que coadyuven eficazmente al mejoramiento de la seguridad ciudadana nacional y a contribuir en el contexto internacional con disponibilidad de servicios que garanticen la interoperabilidad entre países.

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

- Estandarización de los medios de comunicación que involucre tipo de equipamiento y protocolos de comunicación
- Estandarización de una plataforma tecnológica que garantice alta disponibilidad, dedicada a la interoperabilidad de los países integrantes de la seguridad internacional
- Estandarización de mecanismos de seguridad de información
- Dentro del concepto de esfera de la información, definición de los factores de riesgo existentes en cada país integrante de la seguridad internacional, y posibilidad de establecer objetivos en común, que se tienen que combatir y/o minimizar, con la creación de mecanismos automatizados de información. Por ejemplo, para el caso del Estado peruano, tenemos el narcotráfico, terrorismo, delincuencia organizada, contrabando, lavado de activos, trata de personas, entre otros

Portugal

[Original: inglés]
[24 de abril de 2015]

En su resolución 69/28 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, la Asamblea General recordó la función de la ciencia y la tecnología en el contexto de la seguridad internacional y reconoció que los avances científicos y tecnológicos podían tener aplicaciones civiles y militares. Si bien el progreso en la esfera de la información y las telecomunicaciones entraña mayores posibilidades para el desarrollo de la civilización, la cooperación entre los Estados, el aumento de la capacidad creativa de la humanidad y la circulación de la información en la comunidad mundial, por otra parte existe la posibilidad de que esas tecnologías y medios se utilicen con propósitos incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales y afecten negativamente a la integridad de la infraestructura de los Estados.

En esa misma resolución, la Asamblea General pidió a los Estados Miembros que, teniendo en cuenta el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (A/68/98), presentaran contribuciones sobre las cuatro esferas 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 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 del Grupo de Expertos Gubernamentales contenía recomendaciones en las esferas siguientes: normas, reglas y principios de comportamiento responsable de los Estados; medidas de fomento de la confianza e intercambio de información; y medidas de desarrollo de la capacidad.

Atendiendo a esas recomendaciones, podemos describir nuestro contexto nacional de la manera siguiente.

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 aumentando.

Cabe destacar que se ha venido trabajando para aplicar la legislación relativa a la seguridad y la integridad de las redes y para ello se han adoptado métodos de evaluación de los riesgos, que exigen introducir medidas adecuadas de cooperación técnica e institucional en materia de seguridad e informar de violaciones de la seguridad o pérdidas de integridad que tengan repercusiones importantes para el funcionamiento de los servicios.

En el nivel conceptual, es importante reforzar la idea de que la regulación debería derivarse principalmente de las normas internacionales.

En el plano internacional, es importante reforzar el intercambio de información y la realización de ejercicios sobre el terreno en zonas fronterizas.

Medidas para fortalecer la confianza y el 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, nuestros esfuerzos se han centrado en realizar ejercicios conjuntos en los que han participado entidades públicas y privadas, promover la normalización técnica y organizar conferencias y seminarios, algunos de ellos con la participación de oradores internacionales.

Medidas de desarrollo de la capacidad

Es importante establecer medidas de desarrollo de la capacidad. No obstante, hay dificultades relacionadas con la capacitación y el mantenimiento de los recursos humanos relacionados con esas actividades.

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

Qatar

[Original: árabe]
[24 de junio de 2015]

El Estado de Qatar se mantiene vigilante ante las amenazas actuales y potenciales en el ámbito de la seguridad de la información. Ha establecido

estrategias para encarar esas amenazas de manera compatible con la necesidad de mantener el libre flujo de información. El Estado de Qatar considera que la seguridad de la información es fundamental para la seguridad nacional y mundial y, con miras a mantenerla, ha adoptado una serie de medidas para actualizar las tecnologías pertinentes y mejorar la legislación, los reglamentos y los medios de aplicación. También se ocupa de la coordinación y cooperación sobre asuntos pertinentes en los niveles regional e internacional, siempre que lo permita el derecho interno.

El Estado de Qatar considera que la comunidad internacional puede contribuir a la seguridad de la información si prosigue los trabajos de preparación de un instrumento internacional vinculante para salvaguardar la seguridad de la información. Un instrumento de ese tipo debería estipular el desarrollo de programas informáticos que estén bien protegidos contra la piratería informática y el mantenimiento de la coherencia de los sistemas de información.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[29 de mayo de 2015]

El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con satisfacción la oportunidad de responder a la resolución 69/28 de la Asamblea General, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional” y en la presente comunicación abunda en la respuesta que dio en 2013 a la resolución 68/243. En la presente respuesta, el Reino Unido prefiere y emplea el término “ciberseguridad” y los conceptos conexos, a fin de evitar confusiones debido a 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 esencial nacional e internacional y constituye la base indispensable de la actividad económica y social en línea. Las amenazas reales y presuntas que plantean las actividades en el ciberespacio suscitan gran preocupación. En nuestra respuesta se detallan los enfoques nacionales e internacionales que se han adoptado o se adoptarán para fortalecer la seguridad y promover la cooperación en esta esfera. Esos enfoques se sustentan en la Estrategia Nacional de Ciberseguridad del Reino Unido, publicada en noviembre de 2011.

El Reino Unido sigue teniendo un papel destacado en el debate internacional sobre la ciberseguridad. Hemos proporcionado expertos a los cuatro Grupos de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y consideramos que el informe de consenso del último Grupo demuestra que se han hecho valiosos avances en lo que respecta a lograr un entendimiento común sobre las normas de comportamiento de los Estados en el ciberespacio y afirmar la aplicabilidad del derecho internacional al ciberespacio. Esperamos con interés los resultados de las deliberaciones celebradas por el Grupo actual en junio de 2015. El Reino Unido acoge complacido que se sigan examinando en la Organización para la Seguridad y la Cooperación en Europa posibles medidas de fomento de la confianza en el ciberespacio para complementar las que se negociaron con éxito en 2013, así como los trabajos similares que se vienen realizando en otras organizaciones regionales.

La respuesta del Reino Unido esboza la labor que realiza el país para apoyar y mejorar la ciberseguridad y compartir las mejores prácticas, tanto a nivel nacional como en todo el mundo, incluso colaborando con asociados internacionales para enfrentar la ciberdelincuencia y los incidentes de mayor importancia y crear capacidad cibernética. El Reino Unido espera con interés que se siga avanzando en todas esas esferas. Asimismo, se complace en participar activamente en el examen de esas importantes cuestiones y espera seguir contribuyendo a fortalecer la capacidad y la cooperación internacional en materia de ciberseguridad.

El texto completo de la presentación del Reino Unido puede consultarse en www.un.org/disarmament/topics/informationsecurity/.

República de Corea

[Original: inglés]
[11 de junio de 2015]

En la actualidad, el ciberespacio constituye un nuevo horizonte que ofrece infinitas posibilidades y beneficios económicos y sociales sin precedentes. Sin embargo, por su carácter abierto y anónimo, sin fronteras, las amenazas en el ciberespacio están pasando a ser un problema grave para la seguridad internacional.

La República de Corea ha venido sufriendo una serie de ciberataques, incluidos los ataques lanzados en 2014 contra la empresa que opera sus plantas de energía nuclear. Para responder a los ciberataques con más eficacia, la República de Corea estableció en marzo de 2015 planes amplios de mejora de la ciberseguridad y creó el puesto de Secretario de la Presidencia para los Asuntos de Ciberseguridad. La República de Corea tiene la firme convicción de que es importante llegar a un acuerdo sobre un conjunto de normas internacionales aplicables al ciberespacio y poner en práctica medidas de fomento de la confianza y la capacidad cibernética.

A ese respecto, la República de Corea acoge complacida los resultados presentados por el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en su informe de 2013, en el que se reconoció la posibilidad de aplicar el derecho internacional al comportamiento de los Estados en el ciberespacio, y espera que se siga examinando la manera de aplicar los principios convenidos al comportamiento de los Estados en el ciberespacio. La República de Corea acogió en 2014 el seminario regional de Asia y el Pacífico sobre el derecho internacional y el comportamiento de los Estados en el ciberespacio, organizado junto con el Instituto de las Naciones Unidas de Investigación sobre el Desarme. El seminario dio a los países de la región la oportunidad de examinar cuestiones relacionadas con la ciberseguridad.

El Gobierno de la República de Corea también ha procurado fortalecer la cooperación bilateral y trilateral con determinados países y participa activamente en foros regionales e internacionales sobre cuestiones cibernéticas, como el Foro Regional de la Asociación de Naciones del Asia Sudoriental y el Grupo de Expertos Gubernamentales de las Naciones Unidas. En su calidad de anfitrión de la Conferencia de Seúl sobre el Ciberespacio celebrada en 2013, la República de Corea colaboró estrechamente con los Países Bajos en los preparativos de la Conferencia

Mundial sobre el Ciberespacio celebrada en La Haya en 2015, y seguirá haciendo contribuciones a las conferencias del proceso de Londres.

El texto completo de la presentación de la República de Corea puede consultarse en www.un.org/disarmament/topics/informationsecurity/.