Naciones Unidas A/69/112

Asamblea General

Distr. general
30 de junio de 2014
Español
Original: español/inglés

Sexagésimo noveno período de sesiones
Tema 92 de la lista preliminar*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

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

Informe del Secretario General

Índice

* A/69/50.

14-56479 (S) 220714 250714

I. Introducción

1. El 27 de diciembre de 2013 la Asamblea General aprobó la resolución 68/243 titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”. En el párrafo 3 de esa resolución, la Asamblea General invitó a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuraban en el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (A/68/98), siguieran comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

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

b) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y 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. Atendiendo a esa solicitud, el 19 de febrero de 2014, se envió una nota verbal a los Estados Miembros en la que se los invitaba a proporcionar información sobre el tema. En la sección II figuran las respuestas recibidas. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los Gobiernos

Alemania

[Original: inglés]
[30 de mayo de 2014]

Resumen

Las tecnologías de la información y las comunicaciones ofrecen oportunidades sin precedentes tanto para los países industrializados como para los países en desarrollo. Al mismo tiempo, existen vulnerabilidades y debilidades sistémicas.

Existe una tendencia hacia actividades difíciles de detectar, complejas y maliciosas, dirigidas a objetivos de gran valor. Pueden tener consecuencias graves. Un ataque cibernético contra infraestructuras esenciales puede causar más perturbación que un ataque físico aislado, a veces con consecuencias imprevisibles para otras entidades conectadas a la red.

A pesar de esos riesgos, una “ciberguerra” total parece poco realista por el momento. Más probable podría ser un uso limitado de las capacidades cibernéticas como parte de un esfuerzo de guerra más amplio. Por último, existe el peligro de que los incidentes cibernéticos puedan acabar en conflictos en la “vida real”.

En esta situación, es cada vez más importante aumentar la resiliencia cibernética, llegar a un acuerdo sobre leyes y normas que se apliquen a la utilización de las tecnologías de la información y las comunicaciones y participar en medidas de fomento de la confianza.

Se han producido avances positivos en 2013: el último informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional dejó claro que el derecho internacional se aplica al ciberespacio. El Grupo también concluyó que la soberanía del Estado y las normas y los principios internacionales que emanan de ella son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por parte de los Estados y a su jurisdicción sobre la infraestructura de tecnologías de la información y las comunicaciones dentro de su territorio. Alemania espera con interés comprobar cómo el nuevo Grupo de Expertos Gubernamentales ampliará esta cuestión.

En cuanto a las medidas de fomento de la confianza, la OSCE ha logrado importantes avances con la aprobación de un primer conjunto de medidas para aumentar la cooperación entre los Estados, la transparencia, la previsibilidad y la estabilidad con miras a reducir los riesgos de percepción errónea, escalada y conflictos que puedan derivarse del uso de tecnologías de la información y las comunicaciones. Este acuerdo de la OSCE podría ser útil como modelo para otras organizaciones regionales.

La Estrategia de Seguridad Cibernética de Alemania (2011) se basa en la afirmación de que la disponibilidad del ciberespacio y la integridad, la autenticidad y la confidencialidad de los datos en el ciberespacio han pasado a ser de vital importancia. Garantizar la seguridad cibernética se ha convertido en un desafío fundamental para el Estado, las empresas y la sociedad. Deben actuar juntos, a nivel nacional y en cooperación con los asociados internacionales. La Estrategia de Seguridad Cibernética de Alemania establece los siguientes objetivos y medidas:

- Protección de infraestructuras de información esenciales
- Seguridad de los sistemas de tecnología de la información
- Fortalecimiento de la seguridad de la tecnología de la información en la administración pública
- Funcionamiento de un centro nacional de ciberrespuesta
- Establecimiento de un Consejo de Seguridad Cibernética nacional
- Lucha efectiva contra la delincuencia en el ciberespacio
- Medidas eficaces coordinadas para garantizar la seguridad cibernética en Europa y en todo el mundo
- Utilización de tecnología de la información fiable y digna de confianza
- Desarrollo del personal entre autoridades federales
- Instrumentos para responder a los ataques cibernéticos.

Tras las elecciones generales de Alemania en septiembre de 2013 y de conformidad con el Acuerdo de Coalición, la seguridad cibernética figura en un lugar destacado en el programa del Gobierno. Aumentarán las normas de privacidad

de los datos. Los temas principales para los próximos cuatro años incluirán una mejor protección del consumidor; enmiendas a las leyes penales para proteger mejor a las personas; la aprobación de una ley de seguridad de la tecnología de la información con normas obligatorias de seguridad mínima para la infraestructura esencial de tecnología de la información; y la obligación de todas las autoridades federales de invertir el 10% de su presupuesto de tecnología de la información en mejorar la seguridad de sus sistemas.

Como consecuencia de las preocupaciones acerca de la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones, así como la recopilación ilícita o arbitraria de datos personales por terceros, el Gobierno de Alemania alienta encarecidamente a los proveedores de servicios de tecnología de la información a cifrar las telecomunicaciones y no transmitir datos de telecomunicaciones a servicios de inteligencia extranjeros.

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

Australia

[Original: inglés]
[30 de mayo de 2014]

En opinión de Australia, el derecho internacional vigente establece el marco para el comportamiento estatal en el ciberespacio y para responder adecuadamente a las actividades ilegales en línea realizadas por los Estados. Esto incluye, cuando procede, el derecho internacional humanitario, el derecho relativo al uso de la fuerza, el derecho internacional de los derechos humanos y el derecho internacional relativo a la responsabilidad del Estado. Toda norma nueva o complementaria para el comportamiento de los Estados en el ciberespacio se debe elaborar de conformidad con el derecho internacional.

El informe de consenso del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (A/68/98) hizo una contribución significativa a la orientación de los Estados al afirmar que el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable a la utilización del ciberespacio por los Estados y es fundamental para mantener la paz y la estabilidad. Australia considera que esta conclusión es de fundamental importancia. Australia cree que los Estados, de manera individual y colectiva, deben reiterar públicamente su entendimiento de que el derecho internacional se aplica a la conducta de los Estados en el ciberespacio y su compromiso de actuar en el ciberespacio de conformidad con su comprensión del derecho internacional.

El informe reconoció la necesidad de seguir debatiendo y definiendo la manera en que el derecho internacional se aplica al uso del ciberespacio por los Estados y recomendó un estudio más a fondo en esa esfera. Señaló que se podrían elaborar normas adicionales con el tiempo. Australia considera que la explicación de la manera en que el derecho internacional se aplica al comportamiento de los Estados en el ciberespacio, en situaciones de conflicto y de no conflicto, aun reconociendo la complejidad que supone, es una tarea prioritaria para la comunidad internacional.

El informe también formuló recomendaciones innovadoras sobre medidas de fomento de la confianza en el ciberespacio. Australia reconoce que la explicación de la manera en que el derecho internacional se aplica a la utilización del ciberespacio por los Estados es una tarea a largo plazo. A corto plazo, es necesario adoptar medidas prácticas para abordar y prevenir problemas entre los Estados en el ciberespacio que podrían deberse a percepciones erróneas y causar conflictos por errores de cálculo y aumento de los problemas. Las organizaciones de seguridad regionales están especialmente bien situadas para examinar, elaborar y poner en práctica medidas de fomento de la confianza en el ciberespacio. Australia está dirigiendo los trabajos en el seno del Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN) para avanzar en esta importante agenda, que, en vista de diversas capacidades entre los miembros, debería incluir objetivos de aumento de la capacidad.

Austria

[Original: inglés]
[19 de mayo de 2014]

La Estrategia sobre Seguridad Cibernética de Austria, aprobada en marzo de 2013, proporciona un concepto integral y proactivo para proteger el ciberespacio y a las personas en un espacio virtual, garantizando al mismo tiempo los derechos humanos. Mejora la seguridad y la resiliencia de las infraestructuras y los servicios de Austria en el ciberespacio. Lo que es más importante, sirve para aumentar la conciencia y la confianza de la sociedad austríaca.

El establecimiento de redes mundiales y la cooperación internacional son elementos esenciales de la Estrategia sobre Seguridad Cibernética de Austria. La seguridad en el ciberespacio se procura lograr mediante una combinación de políticas coordinadas a nivel nacional e internacional. Austria participará en una "ciberpolítica exterior" en el marco de las alianzas de la Unión Europea, las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Consejo de Europa, la Organización de Cooperación y Desarrollo Económicos (OCDE) y la Organización del Tratado del Atlántico Norte (OTAN) sobre la base de un enfoque coordinado y con objetivos precisos.

Austria contribuirá de manera sustancial a la aplicación de la Estrategia de Ciberseguridad de la Unión Europea, participando plenamente en la labor estratégica y operacional de la Unión Europea. Los ministerios competentes adoptarán las medidas necesarias para aplicar y aprovechar plenamente el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Austria aboga por un acceso gratuito a Internet a nivel internacional. El libre ejercicio de todos los derechos humanos debe estar garantizado en el espacio virtual; en particular, el derecho a la libertad de expresión y la información no debe restringirse indebidamente en Internet.

Austria mantendrá su cooperación bilateral en el marco de su alianza con la OTAN y apoyará activamente la preparación de una lista de medidas de fomento de la confianza y la seguridad en la OSCE. Austria participa activamente en la planificación y ejecución de ejercicios cibernéticos transnacionales. La experiencia adquirida se integrará directamente en la planificación y seguirá desarrollando la cooperación operacional. El Ministerio de Relaciones Exteriores coordina las medidas de política

exterior pertinentes para la seguridad cibernética. Cuando proceda, se tendrá en cuenta la concertación de acuerdos bilaterales o internacionales.

A nivel nacional, un grupo directivo está elaborando un plan de aplicación para aplicar las medidas horizontales establecidas en la Estrategia sobre Seguridad Cibernética de Austria. Los órganos competentes se encargan de aplicar esas medidas en el marco de sus respectivos mandatos, con la coordinación del grupo directivo. Sobre la base de la Estrategia sobre Seguridad Cibernética de Austria, desarrollarán subestrategias para su ámbito de responsabilidad. Los ministerios representados en el grupo directivo se encargan de presentar un plan de ejecución al Gobierno Federal cada dos años. La preparación del plan irá acompañada de un examen de la Estrategia sobre Seguridad Cibernética de Austria, que se revisará y actualizará de ser necesario.

Colombia

[Original: español]
[23 de mayo de 2014]

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

Durante los últimos años se ha presentado un progreso significativo en el desarrollo y aplicación de las tecnologías de la información y las comunicaciones, lo que ha generado importantes cambios y beneficios que han contribuido considerablemente al desarrollo de los países y, ha favorecido la expansión de la cooperación internacional con el objetivo de optimizar la difusión de la información.

No obstante, y de manera simultánea, el avance de estas tecnologías pone de manifiesto una profunda preocupación entorno a la posibilidad de que estos desarrollos sean utilizados con el propósito de quebrantar la estabilidad y seguridad internacional, y de afectar la integridad de la infraestructura de los Estados, afectando a su vez, la seguridad en los ámbitos civil y militar de los mismos.

Bajo este marco, para Colombia el uso de las nuevas tecnologías para generar amenazas informáticas, y la amenaza que actualmente genera la criminalidad en el ciberespacio, es un asunto de la mayor preocupación e interés nacional.

Por lo anterior, para Colombia resulta imperativo definir políticas y estrategias con el fin de impedir que las tecnologías de la información sean utilizadas con objetivos terroristas o delictivos.

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional

Respuestas normativas e institucionales

En el año 2005, Colombia elaboró la norma ISO-27001, concebida como un sistema de gestión que establecía unos estándares de calidad de seguridad de la

información en las entidades nacionales, y propendía por la preservación de las características de confidencialidad, integridad y disponibilidad de la información [1].

Cuatro años después, el Congreso de la República de Colombia promulgó la Ley 1273 de 2009, por medio de la cual se modificó el Código Penal creando un nuevo bien jurídico tutelado, denominado “De la protección de la información y de los datos”. Modificación que permitió la creación de un marco jurídico nacional que permitiría a las entidades competentes perseguir y judicializar los delitos asociados al uso de las tecnologías de la información.

En este marco, Colombia penalizó entre otras cuestiones, el acceso ilícito; la interceptación ilícita; los ataques a la integridad de datos; los ataques a la integridad de sistemas; el abuso de dispositivos; la falsificación informática; el fraude informático; la pornografía infantil; y los delitos contra la propiedad intelectual y derechos afines.

En el año 2011, a través del documento CONPES 3701, Colombia puso en marcha una política y estrategia nacional en materia de ciberseguridad y ciberdefensa basada en tres pilares esenciales:

a) La adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten;

b) El desarrollo de programas de capacitación y formación especializada en seguridad de la información;

c) El fortalecimiento de la legislación nacional en estas materias, así como el fortalecimiento de la cooperación internacional, y en este marco, adelantar la adhesión de Colombia a los diferentes instrumentos internacionales, es decir, a la Convención de Budapest.

Con el objetivo de desarrollar de manera integral las precitadas líneas estratégicas, Colombia diseñó y puso en marcha cuatro instancias:

1. La Comisión Intersectorial, encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica, información pública y ciberseguridad y ciberdefensa;

2. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), ente coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa;

3. El Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), que tiene la función de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales;

4. Finalmente se implementó el Centro Cibernético Policial (CCP), encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos.

[1] Confidencialidad: evitar que la información sea utilizada por individuos o procesos no autorizados. Integridad: proteger la precisión y completitud de cualquier cosa que posee valor para una organización. Disponibilidad: información accesible y utilizable bajo petición de las entidades autorizadas.

Igualmente, Colombia cuenta con un marco jurídico en materia de protección de datos personales, establecido por la Ley 1581 de 2012 y el Decreto 1377 de 2013, por el cual se reglamenta parcialmente esta Ley. Adicionalmente, en la Superintendencia de Industria y Comercio se creó una Delegatura para la Protección de Datos Personales.

Por otra parte, el Ministerio de Tecnologías de la Información y las Comunicaciones diseñó e implementó la estrategia del Gobierno en línea, en la que se incorporan los requerimientos de las entidades en la adopción de sistemas de gestión de seguridad de la información. Igualmente, desde el año 2008, este Ministerio ha capacitado cerca de 6.300 funcionarios en procesos asociados a gestión de las tecnologías de la información.

Finalmente, es importante mencionar que en materia de capacidades se está avanzando en la identificación de la infraestructura crítica nacional (aquella que en caso de ser afectada tiene el potencial de generar pérdidas de vidas humanas, económicas o de gobernabilidad en el país) con miras a mantener la seguridad en materia cibernética de estos lugares.

Cooperación internacional

En el año 2013, Colombia solicitó formalmente la adhesión del país al Convenio Europeo sobre la Ciberdelincuencia, el cual establece los principios del acuerdo internacional sobre seguridad cibernética y la sanción de los delitos de esta naturaleza, y cuyo principal objetivo radica en proteger a la sociedad de la ciberdelincuencia a través del establecimiento de una legislación oportuna y de la cooperación internacional.

Adicionalmente, en el año 2012 Colombia se unió a un convenio multilateral con el Foro Económico Mundial, denominado “Alianza para la Resiliencia Cibernética”, dirigido a identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, cada vez mayor, entre las personas, los procesos y los objetos.

Por otro lado, la secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos, ha establecido un enfoque integral en la construcción de capacidades en materia de ciberseguridad entre los Estados miembros. El principal logro de la secretaría ha sido el establecimiento de grupos nacionales de “alerta, vigilancia y prevención”, también conocidos como Equipos de Respuesta a Incidentes, que cuentan con el mandato y la capacidad de responder ante crisis, incidentes y amenazas a la seguridad cibernética.

Bajo este marco y gracias a la cooperación del CICTE, Colombia ha desarrollado grupos nacionales de “alerta, vigilancia y prevención” que contribuyen al desarrollo de estrategias nacionales sobre ciberseguridad. Igualmente, ha participado en talleres, cursos y congresos sobre el manejo de incidentes relacionados con la seguridad de la información y el delito cibernético.

Finalmente, cabe mencionar que el país ha suscrito acuerdos con empresas y organizaciones internacionales pertenecientes a la industria de la información y las comunicaciones, dentro de los cuales se destacan el acuerdo con Microsoft en función de acceder a instancias como el “Cybercrime Center” y a otros programas de ciberseguridad; y el acuerdo con la organización “Antipishing Working Group” con el fin de hacer parte de la coalición de autoridades legales, empresas de la

industria y entidades de gobierno a nivel mundial que trabajan para contar con mecanismos de alarma y respuesta a incidentes cibernéticos más eficientes.

Medidas internacionales para fortalecer la seguridad de la información

La ciberseguridad no es un problema exclusivo del Gobierno, ni puede resolverlo solo, se requiere el concurso de otros actores —la academia, la industria y la sociedad civil— para afrontar de manera efectiva los riesgos asociados al uso cada vez más intensivo de las tecnologías de la información y las comunicaciones en todos los ámbitos.

Bajo este marco, para Colombia, con miras a fortalecer la seguridad de la información internacional a escala mundial, es importante que la comunidad internacional:

- Busque mecanismos para crear una mayor conciencia en la sociedad, en los mandatarios y en las entidades de cada Estado, sobre la necesidad de generar una cultura de seguridad de la información y la importancia de la cooperación internacional en la lucha contra el delito cibernético.
- Promueva la obligación de los Estados de generar estrategias encaminadas a fortalecer las capacidades nacionales en materia de ciberseguridad y ciberdefensa.
- Exhorte a los Estados a identificar sus infraestructuras críticas y establecer un programa específico para mejorar su seguridad y resiliencia.
- Incentive la adecuación de los marcos normativos nacionales a los instrumentos internacionales existentes en materia de ciberseguridad. Una mayor armonización normativa entre los países facilita el establecimiento de canales de cooperación en materia de prevención, investigación, y judicialización del delito cibernético entre los Estados.

Esta labor de armonización debe contemplar el fomento de la tipificación de los delitos asociados al uso de las tecnologías, así como el establecimiento de reglas claras sobre jurisdicción y competencia para el enjuiciamiento.

- Promueva el establecimiento de obligaciones para los Estados y las entidades nacionales, públicas y privadas, respecto a la preservación de los registros de naturaleza informática, con el fin de que estos puedan ser utilizados durante un proceso de investigación y judicialización.
- Elabore un glosario de términos informáticos inherentes a la ciberdelincuencia, que por lo general, son desconocidos por los operadores del sistema de justicia penal, para asegurar la confidencialidad e integridad de los sistemas, redes y datos informáticos.
- Promueva el intercambio de experiencias y buenas prácticas en materia de ciberdefensa y ciberseguridad, así como el establecimiento de redes de formación especializada en esta materia.
- Exhorte a los Estados a ser partes de las redes de alerta sobre incidentes cibernéticos.

Cuba

[Original: español]
[27 de mayo de 2014]

Cuba comparte plenamente la preocupación que se expresa en la resolución 68/243 respecto al empleo de las tecnologías y medios de información con propósitos que pueden afectar la estabilidad y la seguridad internacionales, la integridad de los Estados y en detrimento de su seguridad en las esferas civil y militar. Igualmente, esa resolución hace adecuado énfasis en la necesidad de impedir la utilización de los recursos y las tecnologías de la información con fines delictivos o terroristas.

En este contexto, Cuba 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. Algunos gobiernos han expresado, incluso, la posibilidad de responder a esos ataques con armas convencionales. El único camino para prevenir y enfrentar estas novedosas amenazas es la cooperación mancomunada entre todos los Estados, al igual que para evitar que el ciberespacio se convierta en un teatro de operaciones militares.

El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales.

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

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

Estas transmisiones contra Cuba violan las normas internacionales vigentes de la constitución de la Unión Internacional de Telecomunicaciones, cuyo preámbulo reconoce la importancia creciente de las telecomunicaciones para la salvaguardia de la paz y el desarrollo económico y social de todos los Estados, y tiene como fin facilitar las relaciones pacíficas, la cooperación internacional entre los pueblos y el desarrollo económico y social por medio del buen funcionamiento de las telecomunicaciones.

El Gobierno de los Estados Unidos de América continúa realizando transmisiones de radiodifusión sonora por la banda comercial de ondas medias diariamente y durante las 24 horas del día. Esta banda de frecuencias no está establecida para dar servicio a otros países. Otras emisoras comerciales brindan

servicios a organizaciones anticubanas para realizar transmisiones, con el propósito de subvertir el orden interno y desinformar a la población cubana.

Iguales transmisiones se realizan, por varias de estas organizaciones, con la total anuencia del Gobierno de los Estados Unidos, a través de las bandas de ondas cortas.

En el período de abril de 2013 a abril de 2014, la cifra promedio dedicada a la transmisión de contenidos subversivos contra nuestro país semanalmente osciló entre 1.909 horas y 2.070 horas utilizando unas 27 frecuencias. En los meses de septiembre y octubre de 2013 dos estaciones estadounidenses que transmiten para el sur de la Florida y cuyas señales se reciben en la zona occidental y central de nuestro país, comenzaron a transmitir programaciones de corte contrarrevolucionario.

Las transmisiones contra Cuba de la radio y televisión Martí por sistemas satelitales internacionales y domésticos estadounidenses también continuaron.

Por otro lado, este año fue revelado públicamente el caso de "ZunZuneo", un complejo plan del Gobierno de los Estados Unidos, al que dedicaron sumas millonarias, para promover la subversión en Cuba a través de un servicio de mensajería en las redes sociales.

Mediante ese programa ilegal, que estuvo activo hasta 2012, se reunieron datos privados de usuarios cubanos, sin su consentimiento, que les permitió procesar perfiles por sexos, edades, gustos y filiaciones de diversa índole, para ser utilizados con fines políticos.

ZunZuneo, al igual que otras operaciones subversivas, infringen leyes cubanas y leyes estadounidenses, como la Ley de Control de Pornografía y Publicidad Comercial No Solicitadas de 2003 (Ley pública 108-187), aprobada por el Congreso estadounidense en diciembre de 2003, que prohíbe enviar mensajes comerciales o de otro tipo sin que el destinatario exprese su consentimiento.

Una vez más, se violó la Constitución de la Unión Internacional de Telecomunicaciones, toda vez que tales usos de las nuevas tecnologías, y en particular de las redes sociales, resultan claramente contrarias a relaciones pacíficas y la cooperación internacional por medio del buen funcionamiento de las telecomunicaciones.

Las prácticas nocivas de correos no deseados (spam) han sido objeto de más de diez recomendaciones de la Oficina de Normalización de las Telecomunicaciones y constituye una violación del numeral 37 de la Declaración de Principios aprobada en la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Ginebra en 2003.

El Gobierno de los Estados Unidos debe respetar el derecho internacional y los propósitos y principios de la Carta de las Naciones Unidas; y por tanto, cesar en sus acciones ilegales y encubiertas contra Cuba, que son rechazadas por el pueblo cubano y la opinión pública internacional.

Al respecto, la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) aprobó el 29 de abril un comunicado enfatizando que el uso ilícito de las nuevas tecnologías de la información y las comunicaciones tiene un impacto negativo para las naciones y sus ciudadanos.

En dicho comunicado, la CELAC expresó su 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. Subrayó 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. Reiteró su compromiso de intensificar los esfuerzos internacionales dirigidos a salvaguardar el ciberespacio y promover su exclusivo uso con fines pacíficos y como vehículo para contribuir al desarrollo económico y social.

Cuba apoyó la resolución 68/243 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]
[26 de mayo de 2014]

La Fuerza Armada de El Salvador, en el marco de la seguridad de la información y las telecomunicaciones, ha implementado una red de telecomunicaciones de voz, vídeo y datos independientes de la red pública, con el fin de proteger toda la información de cualquier agente externo que pretenda infiltrarse, así como de ataques cibernéticos.

Georgia

[Original: inglés]
[30 de mayo de 2014]

Resumen

La guerra cibernética realizada contra Georgia en 2008 colocó la protección de la infraestructura crítica en el programa del Gobierno de Georgia. La creciente dependencia de la infraestructura esencial y los servicios gubernamentales de tecnología de la información aumenta la vulnerabilidad a incidentes relacionados con delitos cibernéticos. En consecuencia, una de las prioridades del Gobierno de Georgia es la adecuada protección de la infraestructura crítica de las amenazas cibernéticas.

Los primeros blancos de los ataques cibernéticos de 2008 fueron sitios web del Gobierno y de noticias de los medios de comunicación. Más tarde, los ataques se ampliaron e incluyeron muchos más sitios web del Gobierno, instituciones financieras, asociaciones empresariales, instituciones educativas, más sitios web de noticias y un foro de piratería informática de Georgia. Esos ataques cibernéticos tenían por objeto interrumpir las operaciones normales. Aparte de dos grandes bancos, las empresas objeto de ataques eran principalmente organizaciones que podrían haberse utilizado para comunicarse y coordinar respuestas entre diferentes empresas.

Esa experiencia demuestra que los ataques cibernéticos contra la infraestructura esencial de Georgia por agentes estatales y privados pueden causar graves daños físicos, así como importantes daños financieros a los sectores público y privado. Por tanto, el Gobierno de Georgia considera que la seguridad cibernética forma parte de la política general de seguridad del país, especialmente habida cuenta de su mayor dependencia de la tecnología de la información como vehículo para la prestación de servicios públicos.

Expresando esas preocupaciones, el Consejo Nacional de Seguridad y un grupo de trabajo especial integrado por diferentes organismos públicos elaboró la Estrategia Nacional de Seguridad Cibernética de Georgia a lo largo de 2011, como parte del examen de la seguridad nacional. La Estrategia de Seguridad Cibernética y el plan de acción para su aplicación se presentaron al público para su examen en marzo de 2012 y, fueron aprobados en enero de 2013.

Un nuevo paso fue la creación en 2010 del Organismo de Intercambio de Datos del Ministerio de Justicia de Georgia como entidad gubernamental central responsable de la elaboración y aplicación de políticas y soluciones de gobernanza electrónica. Una parte importante del mandato del Organismo es la seguridad de la información para el sector público y las entidades privadas como se indica a continuación:

- Adoptar y aplicar políticas y normas de seguridad de la información en el sector público y la infraestructura esencial
- Prestar servicios de consultoría en la esfera de la seguridad de la información y la realización de auditorías de seguridad de la información
- Realizar actividades de sensibilización sobre cuestiones de seguridad de la información entre la población, así como el sector civil
- Mandato de seguridad cibernética mediante el equipo nacional de respuesta a emergencias cibernéticas.

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

Portugal

[Original: inglés]
[20 de mayo de 2014]

La resolución 68/243 de la Asamblea General sobre este tema recuerda el importante papel de la ciencia y la tecnología en el contexto de la seguridad internacional, reconociendo que los avances en esas esferas pueden tener aplicaciones civiles y militares y reconociendo también que se deben mantener y fomentar los progresos. Los progresos en la esfera de la información y las telecomunicaciones suponen aumentar las oportunidades para el desarrollo de la civilización; la cooperación entre los Estados; la promoción de la creatividad humana; y la difusión de información en la comunidad en su conjunto.

Sin embargo, esos medios y tecnologías podrían utilizarse con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad

internacionales y podrían afectar negativamente a la seguridad de los Estados en las esferas civil y militar.

La resolución 68/243 de la Asamblea General requiere la contribución de los Estados Miembros en cuatro esferas, recordando el informe del Grupo de Expertos Gubernamentales (A/68/98):

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

2. Medidas a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito;

3. Contenido de los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones;

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

El informe presentó algunas recomendaciones sobre las siguientes esferas: normas, reglas y principios de comportamiento responsable de los Estados; medidas de fomento de la confianza y el intercambio de información; y medidas de creación de capacidad.

Siguiendo esas recomendaciones, podemos describir nuestro contexto nacional:

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

1. Portugal considera que la seguridad de información de la red es importante y ha ido aumentando;

2. Debemos resaltar los esfuerzos en la aplicación de leyes sobre la seguridad e integridad de la red mediante la adopción de métodos en materia de riesgo, que exigen la adopción de medidas de seguridad adecuadas, a nivel técnico y de organización, y el requisito de comunicar las violaciones de la seguridad o la pérdida de integridad, que tienen importantes repercusiones en el funcionamiento de los servicios. También son importantes los procedimientos de auditoría en el ámbito de la seguridad, llevados a cabo por el Centro Nacional de Notificación de Violaciones de la Seguridad o Pérdida de Integridad;

3. En cuanto a la protección de los datos personales y la privacidad, es importante destacar los cambios que se han producido, por ejemplo, en la notificación obligatoria de violaciones de los datos personales;

4. En el nivel de conceptos, es importante reforzar la idea de que la regulación debería derivarse de las normas internacionales;

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

II) Medidas para fortalecer la confianza y el intercambio de información

1. Es fundamental promover el intercambio de información, teniendo en cuenta la globalización más amplia;

2. A nivel nacional, nuestros esfuerzos se han centrado en la realización de ejercicios conjuntos en que participan entidades públicas y privadas, la promoción de la normalización técnica y la organización de conferencias y seminarios, algunos de ellos con la participación de oradores internacionales.

III) Medidas de desarrollo de la capacidad

1. Es importante elaborar 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;

2. Es necesario facilitar el acceso a los conocimientos;

3. La jerarquía de nivel superior no es suficientemente consciente de su propia responsabilidad en estos asuntos.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[29 de mayo de 2014]

Resumen

El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con satisfacción la oportunidad de responder a la resolución 68/243 de la Asamblea General, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, que se basa en su respuesta a la resolución 67/27 en 2013. El Reino Unido utiliza su terminología preferida de “seguridad cibernética” y conceptos conexos en toda su respuesta a fin de evitar confusiones, teniendo en cuenta las diferentes interpretaciones de la expresión “seguridad de la información” en este contexto.

El Reino Unido reconoce que el ciberespacio es un elemento fundamental de la infraestructura nacional e internacional esencial y una base crucial para la actividad económica y social en línea. Las amenazas reales y potenciales que plantean las actividades en el ciberespacio son motivo de gran preocupación. Nuestra respuesta detalla enfoques nacionales e internacionales que se han adoptado y se adoptarán a fin de fortalecer la seguridad y promover la cooperación en este ámbito. Esos enfoques han sido respaldados por la Estrategia Nacional de Seguridad Cibernética del Reino Unido, publicada en noviembre de 2011.

El Reino Unido ha participado activa y constructivamente en el debate internacional sobre la seguridad cibernética. Hemos proporcionado expertos a los tres Grupos de Expertos Gubernamentales y acogemos con beneplácito el informe de consenso del último Grupo, que ha hecho valiosos avances en el logro de un entendimiento común sobre las normas del comportamiento de los Estados en el ciberespacio y ha afirmado la aplicabilidad del derecho internacional al ciberespacio. El Reino Unido también acoge con beneplácito la aprobación de la primera serie de medidas regionales de fomento de la confianza sobre el

ciberespacio que se negoció con éxito en la OSCE. La respuesta describe la labor del Reino Unido sobre el intercambio de mejores prácticas en todo el mundo, tanto mediante la colaboración con los asociados internacionales para abordar la ciberdelincuencia e incidentes de gravedad como por su compromiso con la construcción de cibercapacidad y ciberaptitudes.

El Reino Unido espera con interés que se siga avanzando en todas esas esferas. Esto incluye el próximo Grupo de Expertos Gubernamentales, la aplicación de las medidas de fomento de la confianza en la OSCE y la elaboración de nuevas medidas de fomento de la confianza en ella y en otros grupos regionales, el establecimiento de equipos de respuesta para emergencias informáticas y el aumento de la cooperación entre ellos, el fortalecimiento de la cooperación en la aplicación de la ley sobre ciberdelincuencia y, la promoción de un enfoque de múltiples interesados.

El Reino Unido se complace en participar activamente en esas importantes cuestiones y espera con interés seguir participando en el fortalecimiento de la capacidad y la cooperación internacional en materia de seguridad cibernética.

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

Serbia

[Original: inglés]
[28 de mayo de 2014]

Teniendo en cuenta la gran importancia que se da a la seguridad de la información a nivel mundial y nacional, la República de Serbia ha adoptado una serie de actividades a fin de proporcionar políticas nacionales y mecanismos de seguridad eficaces. En la Estrategia para el Desarrollo de la Sociedad de la Información en la República de Serbia hasta 2020, aprobada por el Gobierno de la República de Serbia en 2010, se declara que la seguridad de la información es una de seis esferas prioritarias. Serbia no tiene una estrategia nacional dedicada exclusivamente a la seguridad de la información, pero el tema se trata en varios otros documentos. En octubre de 2013 se formó un grupo de trabajo especial y se le encomendó la tarea de redactar una ley de seguridad de la información. La ley se ha armonizado con las normas internacionales pertinentes y los marcos jurídicos de la Unión Europea y determina lo siguiente: el marco institucional de seguridad de la información; las medidas necesarias para proporcionar mayor seguridad a los sistemas de tecnología de la información y las comunicaciones en la República de Serbia, incluidos los sistemas de tecnología de la información y las comunicaciones de los organismos públicos y las empresas; las normas para coordinar la prevención de los riesgos de seguridad en los sistemas de tecnología de la información y las comunicaciones; la creación de un equipo nacional de respuesta a emergencias cibernéticas; las medidas específicas de seguridad y las condiciones previas que se han de aplicar en los sistemas de información de los organismos estatales; la seguridad de la información clasificada en los sistemas de tecnología de la información y las comunicaciones; la criptoseguridad y la protección de emanaciones electromagnéticas comprometedoras.

El Departamento de Tecnología de la Información y las Comunicaciones de la Administración de Servicios Conjuntos de los órganos de la República realiza las actividades relacionadas con la protección de la seguridad de la información, la protección de los datos y la aplicación de las normas de seguridad establecidas para los sistemas de información de los órganos estatales. En el informe anual de la Administración se señaló que en el marco de su mandato de proteger los sistemas estatales de tecnología de la información y las comunicaciones, el Departamento proporciona protección contra los ataques cibernéticos a diario, ya que la red sufre ataques diarios.

La Red Académica de la República de Serbia realiza las actividades de respuesta a incidentes de seguridad informática para instituciones de educación e investigación científica en la República de Serbia. En el informe anual de 2013 de la Red Académica se declaró que hubo un número cada vez mayor de incidentes en comparación con 2012. En el informe se afirmó que los equipos antiguos eran una de las razones del número cada vez mayor de ataques.

Solo una cultura nacional de seguridad de la información bien establecida adoptada a todos los niveles de la sociedad puede ser eficaz para reforzar a nivel local la seguridad de los sistemas nacionales de información y telecomunicaciones. Del mismo modo, solo sistemas nacionales de seguridad de la información bien establecidos pueden ser parte de la aplicación de conceptos internacionales de seguridad de la información para fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

La Oficina del Consejo Nacional de Seguridad y Protección de la Información Clasificada (en lo sucesivo, la Oficina del Consejo Nacional de Seguridad) es el servicio del Gobierno de Serbia responsable de coordinar la aplicación de las políticas de seguridad nacionales y de la Unión Europea a nivel nacional (Dirección Nacional de Seguridad). Un segmento específico de sus actividades se refleja en la adopción de medidas de garantía de la información y la coordinación de la aplicación de esas medidas en los órganos gubernamentales y otras instituciones con el fin de proteger la información clasificada. En este contexto, en 2011 se aprobó el Decreto sobre medidas especiales para la protección de información reservada en los sistemas de telecomunicaciones (Gaceta Oficial RS, núm. 53/2011). A nivel internacional, desde 2011 la Oficina del Consejo Nacional de Seguridad ha participado activamente en el Foro de directores de las Autoridades Nacionales de Seguridad de Europa Sudoriental. Uno de los principales objetivos del Foro es aumentar la garantía de la información y la protección de la información clasificada en los países de la región, de conformidad con las normas internacionales. La Oficina del Consejo Nacional de Seguridad actúa como coordinador principal para elaborar un concepto de ciberdefensa regional en el marco de las Autoridades Nacionales de Seguridad de Europa Sudoriental.

La Oficina del Consejo Nacional de Seguridad ha preparado y enviado a otros miembros del grupo de trabajo temático una serie de propuestas para su examen, armonización y aprobación. Esas propuestas se han estructurado por medio de los siguientes documentos de trabajo: 1) los objetivos del programa de ciberdefensa; y 2) el cuestionario sobre ciberdefensa de las Autoridades Nacionales de Seguridad de Europa Sudoriental.

El Ministerio de Defensa de la República de Serbia está participando en la aplicación de la resolución 68/243 de la Asamblea General. Departamentos del Ministerio de Defensa participan activamente en el grupo de trabajo encargado de redactar la ley de seguridad de la información.

Además, el Ministerio de Defensa está formando diferentes departamentos que trabajarán en la esfera de la seguridad de la información y la ciberdefensa.

Suiza

[Original: inglés]
[29 de mayo de 2014]

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

Las tecnologías de la información y las comunicaciones se han convertido en un factor indispensable de las actividades sociales, económicas y políticas. Suiza está comprometida a aprovechar las oportunidades que genera la utilización de las tecnologías de la información y las comunicaciones. Suiza tiene en cuenta los nuevos acontecimientos y dificultades en relación con las tecnologías de la información y las comunicaciones y participa activamente en la configuración de la sociedad de la información por medio de la Estrategia del Consejo Federal de Suiza para una Sociedad de la Información en Suiza.

Sin embargo, la utilización de tecnologías de la información y las comunicaciones ha expuesto a la infraestructura de la información y las comunicaciones a un uso indebido o deterioro funcional por delincuentes, servicios de inteligencia, agentes político-militares o terroristas. Las alteraciones, manipulación y ataques concretos llevados a cabo a través de redes electrónicas son los riesgos que entraña una sociedad de la información. En ese contexto, los Estados se han dedicado cada vez más a entablar una serie de discusiones sobre políticas regionales e internacionales y debates sobre la seguridad cibernética. Esta participación es generada por un sentimiento creciente de inseguridad sobre las vulnerabilidades en los sistemas informáticos y tecnologías conexas y la forma en que pueden ser explotados con fines maliciosos.

Aunque se han registrado vulnerabilidades y amenazas en este entorno desde el decenio de 1980, no fue sino hasta los últimos siete años que las amenazas y vulnerabilidades derivadas de la utilización de las tecnología de la información y las comunicaciones se han incluido en los programas de seguridad nacional. Como resultado, el Gobierno Federal de Suiza estableció un grupo de expertos en 2010 con el fin de investigar los riesgos y aumentar la capacidad nacional para responder a esas amenazas y vulnerabilidades.

El funcionamiento de Suiza como sistema holístico depende de un número cada vez mayor de servicios de información y comunicación interconectados en red (computadoras y redes). Esa infraestructura es vulnerable. Las perturbaciones y ataques en todo el país o de larga duración podrían tener graves efectos adversos en el desempeño técnico, económico y administrativo de Suiza. Esos ataques podrían realizarlos diversos autores y tener varios motivos: autores individuales, activistas políticos, organizaciones delictivas con la intención de cometer fraudes o extorsión,

y terroristas o espías estatales que quieran perturbar y desestabilizar el Estado y la sociedad. Las tecnologías de la información y las comunicaciones son un blanco particularmente atractivo, no solo porque ofrecen muchas posibilidades de que se produzcan abusos, manipulación y daños, sino también porque pueden utilizarse de forma anónima y con poco esfuerzo. El interés nacional de Suiza es proteger la infraestructura de la información y las comunicaciones de esas perturbaciones y ataques. En este sentido, acogemos con beneplácito la conclusión del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de que el derecho internacional es aplicable a las tecnologías de la información y las comunicaciones.

B. Medidas a nivel nacional para fortalecer la seguridad de la información y promover la colaboración internacional en ese ámbito

El 27 de junio de 2012 el Gobierno Federal de Suiza aprobó la estrategia nacional para la protección de Suiza contra los riesgos cibernéticos, sentando así las bases para un enfoque amplio, integrado y holístico para abordar los riesgos cibernéticos. La estrategia tiene por objeto mejorar la detección temprana de riesgos cibernéticos y las amenazas emergentes, hacer que la infraestructura suiza sea más resistente a los ataques cibernéticos, y en general, reducir los riesgos cibernéticos. Las actividades se centran principalmente en la ciberdelincuencia, el espionaje y el sabotaje. El fundamento racional de la estrategia es la necesidad de una cultura de seguridad cibernética, responsabilidad compartida y un enfoque basado en los riesgos. Aboga por una mayor coordinación en el plano gubernamental y fomenta la asociación entre el sector público y el privado y una mayor cooperación en el ámbito internacional.

La estrategia comprende un conjunto de 16 medidas, que deben ponerse en práctica a más tardar en 2017. A fin de garantizar la aplicación eficaz y oportuna de esas medidas, el 15 de mayo de 2013 el Gobierno de Suiza adoptó un plan detallado para la aplicación de la estrategia. También estableció un comité directivo, en el que está representado el principal organismo responsable de la aplicación de una medida específica. El comité directivo tiene el mandato de asegurar la aplicación coordinada y decidida de esta estrategia. Sus funciones y responsabilidades incluyen garantizar la coordinación entre los departamentos federales[2] suizos pertinentes y los organismos pertinentes a nivel local. A nivel operacional, el Gobierno ha establecido una dependencia de coordinación para apoyar la labor del comité directivo.

El conjunto de medidas incluyen el análisis del riesgo y la vulnerabilidad, el análisis del panorama de las amenazas, las medidas de continuidad y gestión de crisis y de aumento de la competencia para la cooperación e iniciativas internacionales.

Las 16 medidas pueden dividirse en cuatro esferas principales:

– Prevención (por ejemplo, análisis del riesgo y la vulnerabilidad y del panorama de las amenazas);

– Reacción (es decir, manejo de los incidentes, medidas activas e imposición de la ley);

[2] Equivalente a un Ministerio.

– Continuidad (es decir, continuidad y gestión de las crisis);

– Apoyo a los procesos (es decir, cooperación internacional, educación e investigación, fundamentos jurídicos, etc.).

C. Contenido de los conceptos mencionados en el párrafo 2 de la resolución 68/243 de la Asamblea General

La cooperación internacional es uno de los ámbitos de acción que debe fortalecerse mediante la ciberestrategia nacional de Suiza. Así, Suiza está decidida a cooperar a nivel de políticas de seguridad internacionales a fin de abordar las amenazas en el ciberespacio junto con otros países y organizaciones internacionales. Suiza está decidida a vigilar y dar forma a las novedades respectivas a nivel diplomático y promover intercambios políticos en el marco de conferencias internacionales y otras iniciativas diplomáticas.

En ese contexto, Suiza participa en diferentes procesos internacionales encaminados a elaborar mecanismos mundiales. La OSCE ha adoptado medidas de fomento de la confianza en la esfera de la seguridad cibernética. Suiza considera que este proceso es fundamental. Así pues, mediante la aplicación de una “doble vía”, Suiza se centrará en la aplicación del primer conjunto de medidas de fomento de la confianza, así como en la formulación de nuevas medidas. Además, el Programa de Londres constituye otro importante proceso en el que participa Suiza. Por último, al no ser miembro del Grupo de Expertos Gubernamentales, Suiza está interesada en los informes publicados por ese Grupo. En este sentido, apoyamos en particular la petición de que se siga estudiando, entre otras cosas, la manera en que el derecho internacional, incluida la Carta de las Naciones Unidas y el derecho de los derechos humanos y el derecho internacional humanitario, se aplican a la utilización de las tecnologías de la información y las comunicaciones.

A nivel bilateral, Suiza celebra periódicamente consultas políticas con los países sobre cuestiones relacionadas con la cibernética.

Suiza es un país signatario del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que entró en vigor el 1 de enero de 2012.

D. Posibles medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial

Es necesario centrar la atención en iniciativas y medidas destinadas a aumentar la confianza y fomentar una mejor comprensión y confianza entre los Estados. A nivel bilateral, los diálogos de nivel 1, 1.5 y 2 entre los Estados y otras partes interesadas pertinentes en materia de seguridad cibernética han demostrado ser fructíferos. Es necesario seguir desarrollando y mejorando los diálogos sobre seguridad cibernética.

Se podría reforzar la seguridad de la información a nivel mundial mediante el establecimiento de mecanismos conjuntos para evitar la intensificación hacia conflictos armados. Por tanto, podrían establecerse líneas de comunicación directa a nivel técnico y normativo. Se puede mejorar la seguridad en el ciberespacio manteniendo contactos periódicos al más alto nivel.