Naciones Unidas A/60/95/Add.1

Asamblea General

Distr. general
21 de septiembre de 2005
Español
Original: inglés

Sexagésimo período de sesiones
Tema 86 del programa
Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Adición

Índice

05-51880 (S) 101005 101005

II. Respuestas recibidas de los Gobiernos

Brasil

[Original: inglés]
[24 de junio de 2005]

Al analizar las consecuencias de los avances en la tecnología de la información y las telecomunicaciones para la seguridad internacional, hay que empezar por reconocer que la relación entre las sociedades y el desarrollo tecnológico no puede describirse mediante interacciones sencillas y en una sola dirección; esa relación depende de una interacción compleja entre las necesidades, la creatividad, las iniciativas empresariales y la utilización colectiva de la tecnología. El siglo XXI es el alba de una nueva era, durante la cual se prevé que el auge de la "sociedad de la información" dará lugar a profundas transformaciones en todos los campos de la actividad humana, desde las interacciones individuales y sociales hasta las modalidades de producción económica y gobernanza del Estado.

La información ya se ha convertido en un elemento fundamental de la riqueza y prosperidad de las naciones, y se la considera hoy día, con razón, como uno de sus recursos más valiosos. Las empresas privadas, los bancos, las bolsas de valores y las organizaciones gubernamentales (incluidos los responsables de la defensa) están en todos los casos interconectados a través de las redes mundiales de información, que han pasado a ser elementos tan vitales para el progreso económico como la energía eléctrica y el abastecimiento de agua. Sin embargo, este elevado y creciente grado de conectividad crea también una nueva serie de posibles vulnerabilidades para los gobiernos y las economías, las cuales pueden aprovecharse para su utilización en conflictos militares y en actividades delictivas y terroristas.

En los últimos decenios, el empleo masivo de la tecnología y la automatización en la guerra ha creado condiciones propicias para que los conflictos entre los Estados se centren en mayor medida en objetivos militares y eviten los llamados daños colaterales. Al mismo tiempo, la creciente influencia de los medios de comunicación y de la sociedad civil organizada pone muchas limitaciones a la realización de las operaciones militares. Se supone que la guerra contemporánea es "limpia", e incluso "quirúrgica".

Esto está muy en consonancia con las posibilidades concretas que brinda la "guerra cibernética". Algunas fuerzas armadas ya están desplegando unidades militares especializadas, que están entrenadas y equipadas para hacer inutilizables, o incluso destruir, los elementos fundamentales de infraestructura por medio de la invasión y el sabotaje de las redes de información. Dependiendo del objetivo y de los medios empleados, los efectos de esos ataques pueden ir desde la "neutralización" del arma del enemigo hasta los sistemas de sensores para una perturbación cataclísmica de las redes de suministro de electricidad de todo un país. La eficiencia de esta forma de actividad bélica se ve incrementada por el hecho de que muchas de esas capacidades pueden establecerse con inversiones relativamente exiguas. Habida cuenta de esos factores, la guerra cibernética puede muy bien convertirse en un futuro próximo en la piedra angular de los conflictos militares entre Estados. Las mismas vulnerabilidades pueden también ser aprovechadas por organizaciones terroristas, con consecuencias negativas posiblemente mayores y menos previsibles.

Aunque en menor escala en función de la magnitud de los efectos, esos instrumentos ofensivos de la tecnología de la información ya están siendo ampliamente utilizados por los delincuentes: todos los años, los sistemas de tecnología de la información de numerosas instituciones financieras, empresas comerciales e instituciones gubernamentales son atacados e invadidos por personas o grupos que persiguen ilegalmente fines de lucro y/o información privilegiada.

Consciente de la importancia de esta cuestión para el mantenimiento de la paz y la seguridad internacionales, el Brasil sugiere que se aborde de dos formas diferentes. En primer lugar, la comunidad internacional debería tratar de crear instrumentos apropiados para hacer frente a las actividades delictivas y terroristas relacionadas con la tecnología de la información; en un enfoque separado pero complementario, debería examinar asimismo los efectos de la aparición de la guerra cibernética, y la posible necesidad de regímenes de desarme y no proliferación, así como de normas internacionales sobre la guerra a fin de tener en cuenta sus múltiples efectos.

Teniendo en cuenta la posibilidad de actividades terroristas y delictivas, sugerimos que las Naciones Unidas se pongan a la cabeza de los Estados Miembros para poner en marcha, en un régimen de cooperación, las medidas siguientes encaminadas a:

- Establecer redes alternativas y de emergencia para proteger la infraestructura fundamental
- Examinar su estructura de redes, analizando la interdependencia e identificando métodos eficaces de protección
- Promover la interacción entre los poderes públicos y el sector privado, a fin de lograr el grado deseado de seguridad de la información que se intercambian las organizaciones
- Establecer sistemas de protección para evitar los efectos de los ataques cibernéticos, o para reducirlos al mínimo
- Aplicar instrumentos y medidas para permitir a las autoridades detectar el origen de las agresiones informáticas
- Capacitar a las instituciones nacionales para que realicen ensayos y evaluaciones del nivel de seguridad de los sistemas de información
- Negociar y adoptar una convención internacional sobre los delitos cibernéticos.
- Promover y desarrollar tecnología relacionada con los medios y métodos para promover la seguridad de la información
- Garantizar a todo el público el acceso a la información y la tecnología de la información disponibles
- Evitar la creación de mecanismos que podrían impedir el acceso de los países a la alta tecnología en el campo de las telecomunicaciones y los sistemas de información
- Establecer procedimientos para la notificación mutua de las amenazas cibernéticas entre las autoridades nacionales competentes
- Educar a la población acerca de la importancia de la seguridad cibernética.

En cuanto al empleo de las armas informáticas en los conflictos entre Estados, estimamos que las Naciones Unidas deberían evaluar la posibilidad de promover la aprobación de convenciones sobre los temas siguientes:

- Identificación, características y clasificación de la guerra de información
- Identificación y clasificación de las armas informáticas y los medios que pueden utilizarse como tales armas
- Prevención del empleo de armas o conocimientos militares cibernéticos por grupos terroristas
- Establecimiento de un código de conducta para la utilización de las armas informáticas
- Garantía de que todos los países tienen igual derecho a proteger su patria contra los ataques cibernéticos
- Creación de mecanismos internacionales para dar orientaciones acerca de la solución de los conflictos relacionados con las agresiones cibernéticas
- Preparación de un glosario de las Naciones Unidas que contenga definiciones de los principales términos relacionados con la seguridad de la información.

Canadá

[Original: inglés]
[4 de agosto de 2005]

La infraestructura de la información es un componente clave de la infraestructura fundamental del Canadá que incluye los siguientes sectores: energía y servicios públicos, comunicaciones y tecnología de la información, finanzas, atención de la salud, alimentación, agua, transporte, administración pública y actividades manufactureras. Los retos que plantea la acción para garantizar la seguridad de la infraestructura de la información son los mismos en todos los sectores; se estima que hasta el 90% de éstos son de propiedad privada y su funcionamiento está a cargo del sector privado. La importancia que reviste la infraestructura de información del Canadá para todos los canadienses ha inducido al Gobierno a actuar para mantener la seguridad, disponibilidad e integridad de sus sistemas, adoptar medidas para prevenir incidentes cibernéticos y responder rápidamente a toda perturbación que se comunique.

En diciembre de 2003, el Primer Ministro anunció la creación de un nuevo Departamento de Seguridad Pública y Protección Civil (PSEPC). Este nuevo departamento gubernamental aglutinó a la antigua Oficina de Protección de las Infraestructuras Esenciales y de la Protección Civil, la Real Policía Montada del Canadá y el Servicio Canadiense de Información de Seguridad (CSIS) —los tres principales organismos federales con mandatos en materia de seguridad cibernética— en un mismo Ministerio. El PSEPC se encarga de la vigilancia, el seguimiento y el análisis de las amenazas cibernéticas contra los sistemas gubernamentales, actuando como oficina central de notificación de los incidentes cibernéticos y alertando a los departamentos gubernamentales de las nuevas amenazas y vulnerabilidad. El CSIS se ocupa de investigar los incidentes que representen una amenaza para la seguridad nacional. La Real Policía Montada del Canadá se encarga de investigar cualesquiera

incidentes cibernéticos delictivos o potencialmente delictivos. Además, el Centro de la Seguridad de las Comunicaciones es la autoridad técnica encargada de la seguridad de la tecnología de la información que elabora las normas operacionales relativas a la certificación y acreditación de los sistemas, el análisis de riesgos y vulnerabilidad, la evaluación de productos, la seguridad de los sistemas y el análisis de la seguridad de las redes.

En abril de 2004, el Canadá dio a conocer su primera política nacional en materia de seguridad, que comporta una estrategia y un plan de acción integrados para hacer frente a las amenazas actuales y futuras. Este plan confirmaba específicamente que la seguridad cibernética era un problema en términos de seguridad pública y en él se proponía la creación de un Grupo de Acción nacional de alto nivel sobre la seguridad cibernética, con representación de los sectores público y privado, a fin de elaborar una estrategia nacional en la materia encaminada a abordar la cuestión. En la actualidad se está constituyendo el Grupo de Acción.

En febrero de 2005, el PSEPC creó el Centro Canadiense de Respuesta a los Incidentes Cibernéticos (CCIRC) para que sirviera como centro nacional de coordinación de la respuesta a esos incidentes y vigilara el entorno relacionado con las amenazas cibernéticas. El CCIRC actúa a partir del Centro de Operaciones del Gobierno, un servicio que funciona 24 horas al día y siete días a la semana como parte del Sistema Nacional de Intervención en Situaciones de Emergencia del Canadá.

Las provincias y territorios del Canadá están centrando la atención en la protección de sus propias infraestructuras esenciales, inclusive los sistemas y redes de los cuales depende su actividad. Está en curso la labor relacionada con iniciativas interprovinciales tales como la relativa a la capacidad de vigilancia y supervisión cibernéticas en régimen de colaboración.

El sector privado participa activamente en las iniciativas encaminadas a garantizar la seguridad cibernética. Las empresas de este sector protegen su propia infraestructura fundamental de tecnología de la información y, por conducto de las asociaciones industriales, colaboran en el intercambio de información sobre la vulnerabilidad, los incidentes y las soluciones cibernéticos en sus sectores. Las asociaciones industriales cooperan con el PSEPC en un foro que permite un amplio intercambio de información entre todos los sectores industriales.

El Canadá también ha participado en iniciativas multilaterales sobre la seguridad cibernética. Estas incluyen el Subgrupo sobre Delitos de Alta Tecnología del Grupo de los Ocho, que fue establecido en 1997 y adoptó 10 principios para la lucha contra el delito cibernético; la Convención del Consejo de Europa sobre el Delito Cibernético, cuya finalidad es armonizar las leyes nacionales que definen los delitos sustantivos, así como determinar los procedimientos de investigación y enjuiciamiento para abordar las redes mundiales y establecer un sistema rápido y eficaz de cooperación internacional, y la Organización de los Estados Americanos, cuyos miembros convinieron en “considerar la elaboración de los instrumentos jurídicos interamericanos pertinentes y de legislación modelo con el fin de fortalecer la cooperación hemisférica en el combate contra el delito cibernético, considerando normas relativas a la privacidad, la protección de la información, los aspectos procesales y la prevención del delito”.