



Organization of
American States



COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)

DUODÉCIMO PERÍODO ORDINARIO DE SESIONES
7 de marzo de 2012
Washington, D.C.

OEA/Ser.L/X.2.12
CICTE/INF.1/12
7 marzo 2012
Original: inglés

DISCURSO DEL SECRETARIO GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS EXCELENTÍSIMO SEÑOR JOSÉ MIGUEL INSULZA

(Pronunciado en la Ceremonia Inaugural, celebrada el 7 de marzo de 2012)

DISCURSO DEL SECRETARIO GENERAL
DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS
EXCELENTÍSIMO SEÑOR JOSÉ MIGUEL INSULZA

(Pronunciado en la Ceremonia Inaugural, celebrada el 7 de marzo de 2012)

Distinguida Presidenta del Comité Interamericano contra el Terrorismo,
Excelentísimo Vicepresidente del Comité Interamericano contra el Terrorismo,
Embajador Jorge Skinner-Klée
Señoras y Sres. Delegados de las Representaciones Permanentes de los Estados Miembros ante la
OEA,
Sr. Secretario de Seguridad Multidimensional,
Embajador Adam Blackwell
Sr. Secretario del Comité Interamericano contra el Terrorismo,
Gordon Duguid
Señoras y Señores

Nos encontramos hoy nuevamente reunidos en el ámbito de decisión del Comité Inter-Americano contra el Terrorismo (CICTE) para retomar el tratamiento de temas de gran importancia para la Organización y sus Estados Miembros. En esta oportunidad el Comité discutirá el tema del “Fortalecimiento de la Seguridad Cibernética en las Américas, y adoptará una Declaración en ese sentido, que representa un componente invaluable del renovado compromiso de los Estados Miembros en la lucha colectiva del hemisferio contra el terrorismo.

La Declaración tiene mucha importancia ya que al aprobarla contaremos con un documento consensuado que orientará y dará pautas definidas sobre el trabajo que debemos realizar y una serie de principios que debemos seguir para enfrentar las amenazas a la seguridad cibernética.

La región siempre ha estado en la vanguardia en la lucha contra el terrorismo. Ya en la primera Cumbre de las Américas, en 1994, los presidentes del hemisferio hicieron un llamado para convocar una conferencia especial de la OEA sobre la prevención del terrorismo. Nuestros países crearon el CICTE con el objetivo principal de promover la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el flagelo del terrorismo

El tema central del Duodécimo Período Ordinario de Sesiones del Comité Interamericano contra el Terrorismo, la seguridad cibernética, es de la mayor importancia para todos nuestros Estados y sus ciudadanos. Las nuevas tecnologías y los progresos en las telecomunicaciones han permitido extraordinarios resultados y, delineado lo que hasta hace poco eran nuevos e inimaginables horizontes. Sin embargo, los avances en esta era moderna, desafortunadamente han abierto la puerta a crecientes amenazas cibernéticas que plantean nuevos y desafiantes problemas. Para su comisión no existen ni importan las aduanas ni otros controles de fronteras terrestres, puertos o aeropuertos. No se requiere pasaporte ni visa, ni identidad alguna. De hecho, no se necesita que los autores materiales o intelectuales se encuentren en el país donde se cometen.

Cada día que pasa todos y cada uno de nuestros ciudadanos y los gobiernos que los representan dependen aún más de las redes, sistemas de información y tecnologías relacionadas e integradas en el ciberespacio. Individuos, familias, empresas y gobiernos utilizan la red global de Internet,

computadoras, programas, teléfonos celulares, correos electrónicos; una infraestructura física y virtual para la información y las comunicaciones, crítica tanto para la seguridad nacional, regional e individual, como para la seguridad económica, calidad de vida y prosperidad de nuestra gente.

Es que la libre circulación de la información y comunicación y su correspondiente privacidad son esenciales para el funcionamiento y objetivos de dichas redes y la innovación necesaria para el crecimiento económico y el desarrollo social en una economía globalizada.

Los incidentes cibernéticos pueden tener infinidad de formas y acarrear las más serias consecuencias. Gobiernos y estados pueden ser virtualmente paralizados. Compañías y negocios; en suma los niveles de empleo y la prosperidad económica de un país pueden verse afectados por el robo de información confidencial y propiedad intelectual. Individuos pueden sufrir estafas, el robo de su información personal, médica u otra, o convertirse en víctimas de infinidad de delitos contra la persona y su propiedad.

Terroristas, delincuentes y organizaciones criminales explotan tanto las vulnerabilidades como las ventajas de las tecnologías de la información y las comunicaciones para llevar a cabo actividades ilegales que varían significativamente de país a país, e incluso entre regiones dentro de un mismo Estado: el tráfico de drogas y armas ilícitas; la trata de personas; el contrabando; el secuestro; el uso de la Red de Internet con fines terroristas, la incitación al terrorismo; la extorsión; los delitos contra la propiedad; la corrupción y el lavado de activos relacionado con estas y otras formas de crimen organizado nacional e internacional.

Nuestra capacidad de respuesta ante estas amenazas todavía presenta debilidades.

Necesitamos incrementar la concientización sobre la importancia de la ciber seguridad en todos los niveles, pero particularmente en el nivel de la toma de decisiones políticas, a fin de promover la adopción de prácticas y estrategias nacionales de seguridad cibernética, que permitan promover de manera efectiva y acertada la implementación de las medidas necesarias para el mejor y honesto uso y aprovechamiento de las tecnologías de la información y la comunicación.

Necesitamos profundizar la capacitación de personal altamente calificado, requerido para responder adecuadamente a esas amenazas -de naturaleza multidimensional- a las redes y sistemas críticos de información, para poder prevenir y responder a incidentes de seguridad cibernética, así como para poder detectar, investigar y someter a la justicia a los responsables de esos delitos.

Para combatir a una red se necesita una red. Para combatir tanto a las amenazas a la ciber seguridad, tanto al terrorismo como a las redes del crimen organizado transnacional, se necesitan redes transnacionales de actores públicos y privados dispuestos y preparados para cooperar a fin de prevenir la acción criminal y hacer respetar las leyes.

La OEA ha hecho avances significativos en este terreno. En 2004 los Estados Miembros de la OEA adoptaron la Estrategia Interamericana de Combate a las Amenazas a la Seguridad Cibernética. En el marco de esa estrategia, el Grupo de Expertos Gubernamentales en materia de Ciber delito de la Reunión de Ministros de Justicia y Fiscales Generales de las Américas se ha concentrado en el desarrollo de los instrumentos legales necesarios para proteger a los usuarios de Internet y de redes de información, así como en asistir a los Estados Miembros en el desarrollo de las capacidades de investigación y persecución legal correspondientes.

Por su parte, la Comisión Interamericana de Telecomunicaciones se ha dedicado a la promoción de una cultura de la seguridad cibernética y a trabajar, con gobiernos y empresas privadas, en el desarrollo e implementación de estándares y regulaciones en la materia.

Finalmente, la Secretaría del CICTE ha asistido a los Estados Miembros para el desarrollo de sus capacidades permanentes de vigilancia, alerta y respuesta a las amenazas a la seguridad cibernética. Esta asistencia se ha traducido en la creación de Equipos nacionales de Respuesta a Incidentes de Seguridad de Informática (CSIRTs, por su sigla en inglés), que ya suman dieciséis. También ha venido desarrollando una Red Hemisférica (de CSIRTs) y actores en Seguridad Cibernética, la cual cuenta con 100 usuarios que representan a 19 Estados Miembros. De la misma forma ha venido promoviendo el desarrollo de políticas y estrategias de Seguridad Cibernética y, reconociendo la importancia de la sociedad civil y el sector privado, ha estado trabajando con dichos actores en diferentes actividades con el propósito de promover la cooperación, y el intercambio de información y buenas prácticas.

A lo largo de los últimos años hemos procurado tender puentes entre los países y sus capacidades, promoviendo la cooperación para enfrentar estas amenazas transnacionales y multidimensionales. Nuestro esfuerzo ha estado orientado, principalmente, a contribuir al fortalecimiento de las capacidades técnicas de nuestros Estados Miembros; a contribuir al desarrollo de una conciencia de seguridad cibernética; a fortalecer las capacidades legales e institucionales; y a fortalecer los vínculos y sistemas de cooperación entre nuestros países ante un ataque cibernético.

Este año el CICTE centrará sus trabajos en reforzar la cooperación internacional para, juntos enfrentar estas amenazas. En este contexto, la acción de los países cobra mayor relevancia. La OEA, a través de la Secretaría de CICTE, se propone, entre otros objetivos, apoyar a los Estados Miembros que todavía no han instalado sus Centros Nacionales de Respuesta a Incidentes de Informática (CSIRTs); mejorar las capacidades técnicas del personal en CSIRTs nacionales ya establecidos; promover el desarrollo de marcos o estrategias nacionales de ciber seguridad; aumentar y consolidar la cooperación regional e internacional existentes, así como con el sector privado, en temas relacionados con la seguridad cibernética y especialmente con la protección de la infraestructura de información crítica.

El desarrollo de una visión moderna de cooperación entre el sector público y el privado -que es propietario y operador de la mayor parte de las infraestructuras de información de las que dependen los países y entre los gobiernos de la región, es una imperiosa necesidad para mejorar la seguridad y capacidad de prevención, respuesta y recuperación de la infraestructura crítica de información y comunicaciones ante las amenazas cibernéticas.

Finalmente, quisiera destacar esa cooperación que estamos promoviendo con el sector privado, el cual es un actor fundamental para cualquier estrategia de seguridad cibernética que aspire a tener alguna probabilidad de éxito. En este sentido, quisiera expresar nuestro reconocimiento a la Sra. Cheri Maguire, Vicepresidente de Asuntos Gubernamentales y Políticas Globales de Seguridad Cibernética de *Symantec Corporation*, quien va a participar y contribuir a las deliberaciones de este Comité.

La OEA, como órgano político que reúne a todos los Estados Miembros soberanos del Continente, les ofrece un espacio político y jurídico para que autoridades nacionales de las Américas en materia

de ciber seguridad puedan intercambiar información, coordinar acciones y en definitiva desarrollar la cooperación necesaria para la construcción y consolidación de esas redes imprescindibles para enfrentar las amenazas antes mencionadas.

Esperamos sinceramente que de este esfuerzo surja una voluntad fortalecida para que entre todos contribuyamos al fortalecimiento de las capacidades nacionales y regionales para enfrentar los delitos cibernéticos y el crimen organizado o el ciber terrorismo que de aquél se valen, en búsqueda de nuestro fin común que no es otro que el bienestar y prosperidad de nuestros ciudadanos.

Para concluir, deseo expresar mi agradecimiento a la Presidencia de Grenada y Vicepresidencia de Guatemala del CICTE, por su destacado liderazgo durante todo el pasado año, a los Estados Miembros y Observadores Permanentes por su apoyo y activa participación en las labores del Comité, y a la Secretaría por su dedicado trabajo.

Muchas gracias.