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.5/12
14 marzo 2012
Original: español

PALABRAS DEL PRESIDENTE DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO 2012-2013

(Pronunciado por el Excelentísimo Señor Embajador Jorge Skinner-Klee, Representante Permanente de Guatemala ante la OEA, en la Primera Sesión Plenaria, celebrada el 7 de marzo de 2012)

PALABRAS DEL PRESIDENTE DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO 2012-2013

(Pronunciado por el Excelentísimo Señor Embajador Jorge Skinner-Klee, Representante Permanente de Guatemala ante la OEA, en la Primera Sesión Plenaria, celebrada el 7 de marzo de 2012)

Distinguida Presidenta del Comité Interamericano contra el Terrorismo;
Excelentísima Embajadora Gillian Bristol, Representante Permanente de Grenada;
Señoras y Sres. Delegados de las Representaciones Permanentes de los Estados Miembros ante la OEA;
Señores Representantes de las Misiones Observadores ante la OEA;
Sr. Secretario del Comité Interamericano contra el Terrorismo, Gordon Duguid;
Señoras y Señores e Invitados Especiales.

Tengo el orgullo y el privilegio personal de aceptar, en nombre de la República de Guatemala, la presidencia del Comité Interamericano contra el Terrorismo. La propuesta de nuestra candidatura hecha por las distinguidas delegaciones de México y Grenada, y con el respaldo unánime de todos los Estados miembros, significa para nosotros un gran honor y una clara indicación de la confianza depositada en nuestro país para dirigir este foro hemisférico único. Deseo asegurarles que asumimos este cargo con toda la voluntad de cumplir con lo que se espera de nosotros y que responderemos activamente con los compromisos adquiridos, lo haremos colaborando estrechamente con todos y cada uno de los Estados miembros, con la Vicepresidencia que será ejercida sin duda en forma más que destacada por la República de Colombia, y con la Secretaría.

Este día es para nosotros un punto de llegada y, al mismo tiempo, un punto de partida. En primer lugar, quiero reiterarles a todas las delegaciones un cordial saludo de bienvenida y los mejores votos por una sesion que logre concretar las expectativas que deseamos alcanzar. Ante nosotros se abre una oportunidad única para forjar un mundo mejor. En segundo lugar, deseo agradecer al gobierno de Grenada por el liderazgo ejercido en este Comité durante el pasado año, con particular enfoque en el desarrollo de la cooperación entre los Estados miembros para prevenir y combatir el flagelo del terrorismo. Quisiera reconocer

particularmente el trabajo de la Embajadora de ese país ante la OEA, Gillian Bristol, quien condujo con ahínco y éxito el proceso preparatorio de este Duodécimo Período de Sesiones Ordinario del CICTE.

Por otra parte, quiero recordar que desde su creación, el Comité Interamericano contra el Terrorismo ha sido un modelo de cooperación internacional eficaz, solidaria y oportuna, en la lucha contra un antiguo fenómeno que ha adquirido una nueva magnitud y desborda las fronteras nacionales, convirtiéndose en una de las mas inusitadas amenazas para la paz y la seguridad internacional, como para los ciudadanos en particular.

Por ello, ratificamos el mas firme compromiso de mi país con todos los países miembros de la OEA, para realizar nuestro mejor esfuerzo para contribuir a la conducción de los trabajos de este Comité, a fin de facilitar la búsqueda de los acuerdos que permitan reflejar el interés hemisférico en el combate a las diversas amenazas que enfrentamos juntos.

Guatemala tuvo el honor de proponer el tema principal que nos convoca este día, el "Fortalecimiento de la Seguridad Cibernética en las Américas", el cual ya no es más un tema de un futuro distante, sino que está enquistado en nuestro acuciante presente, hoy y ahora.

El uso de las tecnologías de la información y la comunicación trae consigo cambios y retos permanentes y por tanto constituye uno de los pilares del desarrollo en una economía cada vez más global. Dichas tecnologías son críticas para el desarrollo de toda actividad económica pues facilitan enormemente el comercio, la prestación de bienes y servicios, la asistencia humanitaria, la investigación, la innovación y el emprendimiento; y de otra parte, estas tecnologías son las que permiten y fomentan el libre flujo de información entre individuos, organizaciones y gobiernos. En efecto, la información y comunicación del mundo actual proveen la plataforma para el gobierno electrónico, promueven el desarrollo económico, habilitan las estructuras críticas de los servicios públicos y, por sobretodo, permiten que los ciudadanos tengan acceso y compartan la información oportunamente, todo lo cual se traduce en un ciudadano informado, en mayor seguridad pública, en

infraestructuras de servicios más efectivas, en una seguridad nacional más activa y confiable y, en general, en un mundo más interconectado y democrático y por lo tanto más accesible, transparente y operacional.

Sin embargo, advertimos que entre más aumenta el uso y la dependencia de las tecnologías de información y comunicación, también aumentan los riesgos asociados con ellas, tanto los provenientes de la naturaleza como los causados por el hombre. Estas amenazas se ciernen sobre la confiabilidad de las infraestructuras críticas que habilitan el uso de información, la red global y la integridad misma de la información que es usada o almacenada en tales infraestructuras. Las circunstancias y las motivaciones que amenazan estas tecnologías varían en naturaleza, desde el simple delito del hurto de información o dinero, o el entorpecimiento a la libre competencia, hasta actos de sabotaje y formas cibernéticas de agresión en el ciberespacio.

Hemos conocido así, ataques contra personas y su identidad, contra empresas y consorcios comerciales, contra infraestructuras municipales, nacionales o internacionales críticas e incluso contra países enteros, todo lo cual tiene graves consecuencias para el bienestar de los ciudadanos y la seguridad de las naciones, afectando negativamente el interés común y el bienestar de la comunidad internacional. Por eso, los Estados miembros de la OEA estamos llamados a encarar el reto de mantener y auspiciar una atmósfera que promueva la libertad de sus ciudadanos, respete sus derechos y libertades fundamentales, fomente el libre flujo de información y proteja la libertad de expresión y en consecuencia debemos aunar esfuerzos para mejorar la integridad y la seguridad de las tecnologías informáticas y avanza en la cooperación internacional para apoyar las acciones orientadas a evitar o disminuir los ataques a las redes informáticas y proteger a sus usuarios.

Este esfuerzo impostergable debe incluir la gestión de incidentes, la respuesta y la mitigación de ataques cibernéticos, incluso la investigación y el enjuiciamiento de los crímenes transnacionales de esta naturaleza, así como la logística para proteger la infraestructura cibernética crítica, esencial en la vida contemporánea.

El Internet es global, no distingue región o subregión, ni países importantes o menores, ni tampoco un ámbito o áreas específicas o individuales, sino que lo contiene todo. En el ciberespacio, los ciudadanos, las empresas, las organizaciones y los Estados son usuarios con el mismo derecho y las mismas necesidades. El crimen organizado transnacional utiliza, lucra y negocia ilícitamente a través del espacio cibernético, razón por la cual los Estados estamos obligados a defender a los ciudadanos de las actividades ilícitas, de las intromisiones en su vida privada y de las disrupciones de los servicios que la vida cotidiana demanda. Los ataques cibernéticos van desde la intromisión al vandalismo, comenzando por la estafa y el hurto de información personal o la sustracción de planes comerciales o de megaproyectos industriales; pero también incluyen la interrupción de comunicaciones a servicios críticos, como el agua, la red eléctrica, las plantas químicas o los controladores aéreos, entre otros. Estos gravísimos hechos reclaman la acción concertada y en legítima defensa para impedir, degradar, destruir, entorpecer o retrasar los efectos de tales ataques criminales. En suma, es necesario como impostergable resguardar la infraestructura crítica de cada país para evitar la ruptura, interrupción o sabotaje de las comunicaciones, como para asegurar que el Internet y su ciberespacio sea un lugar seguro donde las libertades fundamentales de la persona sean resguardadas junto a la confidencialidad de la información así como su emisión y difusión. Por ello, la colaboración para articular una mejor seguridad cibernética en las Américas nos permitirá promover pautas internacionales, proteger la propiedad intelectual y la seguridad del ciberespacio, al igual que avanzar en la libertad y la democracia para el más fluido intercambio de ideas y el comercio en la era digital.

Por tanto, resulta ineludible como necesario continuar avanzando en el desarrollo de la cooperación necesaria para fortalecer las capacidades nacionales y regionales en materia de manejo de incidentes de seguridad cibernética, incluyendo aquellas capacidades necesarias para prepararse para prevenir, detectar, responder, mitigar, recuperar y resistir incidentes contra la seguridad cibernética, a la vez de proteger y asegurar la infraestructura de información crítica y sistemas de redes.

Ante tales retos, nuestra capacidad de respuesta ante estas amenazas todavía presenta debilidades y es insuficiente.

Como Estados socios, necesitamos también incrementar la concientización sobre la importancia de la ciber-seguridad como complemento de la seguridad nacional y regional, y como parte de la prevención y el combate al ciber-delito en todos los niveles, a fin de promover la adopción de prácticas óptimas y seguras para el uso de las tecnologías de la información y las comunicaciones.

Debemos pues, continuar y acrecentar la cooperación internacional prestando nuestro apoyo a los Estados Miembros que todavía no han instalado un Centro Nacional de Respuesta a Incidentes de Informática (CSIRTs), para que los puedan concretar; paralelamente, debemos mejorar las capacidades técnicas del personal en CSIRTs nacionales ya establecidos. También tenemos que promover el desarrollo de marcos o estrategias nacionales de ciber-seguridad; y aumentar, fortalecer y consolidar la cooperación regional e internacional existentes, así como con el sector privado, en el cambo de la ciber seguridad relacionada con la protección de la infraestructura crítica de información y comunicaciones.

El desarrollo de una visión moderna y ágil de cooperación entre el sector público y el privado, 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 imprescindible tarea si queremos mejorar la seguridad y la capacidad de recuperación de la infraestructura crítica de información y comunicaciones ante las ciber amenazas y los ataques cibernéticos, con especial énfasis en las instituciones gubernamentales críticas, así como en los sectores esenciales para la seguridad nacional, incluyendo los sistemas de servicios públicos como energía, agua, servicios financieros, transporte y telecomunicaciones, entre otros.

En consecuencia es menester, proteger esa variada y endeble infraestructura crítica de la información y comunicaciones, incluyendo la implementación de programas de desarrollo

de capacidades que fortalezcan todos los componentes críticos de las cadenas de suministro global.

Subrayamos la necesidad de profundizar la capacitación de personal altamente calificado, requerido para responder adecuadamente a esas amenazas, que son de naturaleza multidimensional como multinacional y ciertamente no convencional a las redes y sistema críticos de información, para poder prevenir y responder a incidentes de ciber-seguridad, así como detectar, investigar y someter a la justicia a los responsables de ciber delitos.

Por eso pensamos que para combatir a una red se necesita una respuesta recíproca, como bien lo indico nuestro Secretario General, es decir otra red. Para combatir tanto a las amenazas a la ciber-seguridad como a las redes del crimen organizado transnacional se requiere de redes transnacionales de actores públicos y privados dispuestos y preparados para cooperar a fin de prevenir la acción criminal y hacer respetar el uso legítimo y libre de las tecnologías informáticas en favor del progreso económico y desarrollo social. Es un reto que todos podemos afrontar y que no podemos diferir, por lo que se impone tender puentes de nuestro entendimiento para articular avenidas de cooperación útil y prontas para el tratamiento de un fenómeno por demás pernicioso, como complejo.

El tema que nos convoca se inscribe en la búsqueda de un fin común que no es otro que el bienestar y la prosperidad de esos nuestros ciudadanos y la defensa de sus derechos humanos, libertades, propiedad y privacidad, todos esenciales a la defensa de los valores democráticos en el mundo digital. Nuestra obligación es protegerlos y es una prioridad de este Comité.

En ese marco y contexto, esperamos y deseamos la activa participación de los Estados miembros de la OEA en los programas del CICTE, particularmente en las áreas relacionadas con la protección de la infraestructura crítica y la seguridad cibernética, donde tenemos experiencias positivas que debemos compartir y diseminar.

Es necesario continuar nuestro progreso, con la implementación del Plan de Trabajo aprobado para el período que hoy comienza mediante el cual aspiramos alcanzar, conjuntamente con todos y cada uno de los Estados miembros, los mejores resultados posibles en aras de los principios y objetivos antes seante señalados. El debate y análisis inter-estatal, con participación de otros actores relevantes, es el instrumento a nuestra disposición para ello.

Permítaseme finalmente reiterar nuestro agradecimiento a los distinguidos y Representantes de los Estados miembros de la OEA por la confianza depositada en nuestro país para asumir este honroso cargo, y reafirmar el compromiso de contribuir al fortalecimiento del CICTE como una valiosa herramienta hemisférica para enfrentar de manera decidida este flagelo, en plena observancia de los instrumentos internacionales universales y regionales suscritos por los Estados parte.

Muchas gracias