Discurso Colombia en el Decimosexto Periodo Ordinario de Sesiones del CICTE.

Es indiscutible que las redes del crimen organizado han adquirido, lamentablemente, una especial pericia en el manejo de nuevas tecnologías, lo que ha potenciado y ampliado sus capacidades, facilitando su actuar y optimizando sus rendimientos. Es por esto que las estrategias de los Estados para crear un entorno digital seguro deben tener dentro de sus objetivos el entendimiento de fenómenos tales como el de ciberlavado de activos, el ciberterrorismo, o la ciberdelincuencia. Sin duda, entender la amenaza facilita su lucha.

De la misma manera, el uso de internet con fines terroristas supone un reto mayor para los Estados. Es evidente la imperante necesidad de fortalecer la cooperación internacional para contrarrestar la propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo); la financiación; el adiestramiento; la planificación (tanto por medio de comunicaciones secretas, como mediante la información de dominio público); la ejecución; y los ataques cibernéticos (5) en sí mismos.

Lo anterior supone un importante esfuerzo por parte de los Gobiernos, el sector privado y la academia, con el fin de hacer frente a los obstáculos en el intercambio de conocimiento, experiencias, investigación, desarrollo de nuevas tecnologías e información relacionada con los incidentes digitales.

Si bien no existen instrumentos internacionales globales sobre ciberdelincuencia o terrorismo que impongan a los Estados obligaciones específicas en materia de cooperación internacional, en el marco de diversos instrumentos bilaterales, regionales o multilaterales, se insta a los Estados a establecer políticas y marcos legislativos para facilitar la cooperación internacional eficaz en la investigación y persecución de los actos de terrorismo o los actos graves de delincuencia organizada.

De la misma manera, en caso de no haberse adoptado en las legislaciones nacionales medidas específicas para hacer frente al uso de las tecnologías de la información y las comunicaciones con fines delictivos o terroristas, el uso de la legislación general sobre ciberdelincuencia y legislación contra el terrorismo constituyen un marco conceptual útil para los encargados de diseñar políticas y los legisladores.

Colombia considera fundamentales los siguientes elementos:

Los organismos, instancias y entidades encargadas de análisis, identificación, prevención, investigación y persecución al crimen y la delincuencia en un entorno digital, debe contar con los recursos humanos, técnicos y financieros suficientes para enfrentar nuevos tipos de crimen y delincuencia, a nivel nacional y transnacional, con un enfoque de gestión de riesgos de seguridad digital.

Es fundamental fortalecer las capacidades de los fiscales y jueces en materia de ciberdefensa y ciberseguridad, así como el establecimiento de canales de cooperación interinstitucional y entre el sector público y el sector privado.

El Estado debe promover el intercambio de información entre las autoridades competentes de hacer frente a nuevas amenazas cibernéticas, tales como el Ciberterrorismo, el Ciberlavado, la Ciberdelincuencia y todas aquellas que afecten la defensa de la soberanía y la integridad territorial.

El lavado de activos es un delito transnacional cuya comisión, en el ámbito de la globalización y de la sociedad informática y de redes, hace uso del Ciberespacio y de las distintas tecnologías que hacen parte de éste. Las tipologías de lavado de activos continuamente deben incluir esas nuevas técnicas utilizadas por lavadores, con el fin de realizar una adecuada actividad de prevención, detección y consecuente represión. Dentro de estas - 4 - modalidades de Ciberlavado, es preciso tener en cuenta la creación de compañías de portafolios, transferencias inalámbricas entre corresponsales, ventas fraudulentas de bienes y utilización del mercado negro de cambio del peso, bancos fantasmas y monedas virtuales, principalmente.'

Para Colombia es prioritario lograr que las múltiples partes interesadas, hagan un uso responsable de un entorno digital, a través del fortalecimiento de sus capacidades para identificar, gestionar y mitigar los riesgos de las actividades digitales, contribuyendo al crecimiento de la economía digital nacional, y maximizando de esta manera los beneficios obtenidos de una mayor prosperidad económica, política y social del país.

Finalmente, quisiera reiterar la invitación al “Segundo Simposio Internacional de Ciberseguridad para equipos de respuesta de seguridad cibernética”, que tendrá lugar en la ciudad de Bogotá en octubre de 2016, organizado por el Gobierno de Colombia de manera conjunta con el CICTE. El principal objetivo del evento es estrechar los lazos de cooperación y fomentar la mutua transferencia de conocimiento en materia de Ciberseguridad y Ciberdefensa