TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

CANCILLERÍA

COMENTARIOS GOBIERNO DE COLOMBIA

Estudio Exhaustivo del delito de cibernético

Ministerio de Relaciones Exteriores– República de Colombia

El presente documento reúne los comentarios realizados por el Gobierno Nacional, frente al Estudio Exhaustivo del delito cibernético (2013), presentado por el Grupo Intergubernamental de Expertos establecido por la Comisión de Prevención del delito y justicia penal, de acuerdo con la resolución 65/230 de la Asamblea General de las Naciones Unidas.

Se resalta la identificación del fortalecimiento de la asistencia técnica como elemento fundamental para hacer frente a los retos que plantea el tema actualmente, sin perjuicio de los debates que se adelantan sobre los eventuales instrumentos internacionales aplicables.

A continuación, las observaciones realizadas, divididas en cinco secciones: prevención del delito, respuestas legales, justicia penal, cooperación internacional y desarrollo de capacidades y asistencia técnica.

1. PREVENCIÓN DEL CIBERDELITO

El documento aborda las estrategias de prevención en dos ítems, los cuales están enfocados únicamente a la ciberseguridad (estrategias de ciberseguridad y estrategias contra el ciberdelito); no obstante, es necesaria la inclusión de un tercer ítem enfocado a la ciberdefensa clasificando y generando los alcances y nacionalidad de cada agencia y sus involucrados. Adicionalmente, el término de ciberseguridad está siendo abordado de manera reducida, cuando este podría ser evaluado de manera independiente en el documento como un elemento estratégico.

No se hace claridad frente a las obligaciones de los estados miembros para generar y regular las estrategias tendientes a prevenir los incidentes que involucren la seguridad digital y que sean producto de errores del factor humano o vulnerabilidades desconocidas.

Es de anotar que no se está incluyendo el término ciberdefensa, el cual sería la definición más apropiada para los ataques de índole internacional (entre Estados) que tienen un contexto de afectación a la soberanía digital de cada Gobierno. Sería preciso que se puntualizara en la ausencia de normatividad frente a la existencia del delito de contenido y las facultades de los Estados miembros para solicitar ante las diferentes plataformas de internet la eliminación de estos.

Cabe destacar que muchas veces, el sistema informático solamente es el medio para la comisión del delito, por lo cual hay ciertas conductas punibles que, aunque se realizan a través de medios informáticos, no pueden perder su enfoque y confundirse con ciberdelito, cuando el sistema informático solamente es el medio para un fin, que no genera una afectación sobre la disponibilidad, integridad y confidencialidad de los sistemas de información y los datos.

2. RESPUESTAS LEGALES

Resulta de gran relevancia evidenciar el apoyo que debe realizarse para labores de concienciación a nivel de denuncia, enfocándose en la creación de mecanismos legales a partir de la diferencia dimensional con los delitos comunes, al igual que las políticas trasnacionales con tiempos de respuesta inmediato. Adicionalmente, los esfuerzos deben orientarse hacia:

1. Fortalecimiento de los mecanismos legales procesales para que las denuncias individuales adquieran un contexto global y no local por la naturaleza de los ciberdelitos (ataque simultáneo y en tiempo real desde una ciudad a dos ciudades diferentes).

2. Generación de enfoques proactivos legales trasnacionales que permitan trasladar al campo cibernético las actuaciones de tipo investigativo y de inteligencia policial, para un adecuado control del tráfico en internet como una medida a favor para la implementación de acciones preventivas sin que ello vulnere la privacidad.

3. Garantizar la integración efectiva de los proveedores de servicios de internet (ISP) y entes tecnológicos (administradores de hosting) mediante la generación de normatividades locales y trasnacionales (acuerdos, tratados, convenios) vinculantes en el desarrollo de las acciones ejecutadas por las agencias de ley en la lucha contra el ciberdelito trasnacional.

4. Creación de mecanismos obligatorios de educación ciudadana por parte de los entes educativos para prevenir el cibercrimen y motivar la actividad de denuncia, así como para generar una mayor percepción de importancia simétrica a los delitos tradicionales, creando conciencia de la profesionalización de los entes judiciales de investigación y la reserva de la información.

5. Generación de apoyo estructural y legislativo nacional y trasnacional para una mayor efectividad en la preservación de los datos informáticos (naturaleza volátil de la evidencia electrónica), y recopilación de datos en tiempo real, con uso de herramientas forenses remotas a datos informáticos extraterritoriales.

3. JUSTICIA PENAL

Se evidencia la problemática de la carencia de un marco legal homogéneo entre los Estados, que establezca tipos penales y procedimientos en materia de cibercrimen; por lo tanto, es fundamental que los países se comprometan a legislar y establecer en sus ordenamientos jurídicos instrumentos legales para la lucha y prevención contra el cibercrimen.

Teniendo en cuenta la carencia de comunicación en doble vía entre las procuradurías y/o Fiscalías en los Estados, se considera conveniente el establecimiento de modelos de justico penal transnacional como los establecidos en la Unión Europea "EUROJUST".

Con respecto al establecimiento de convenios y/o instrumentos de cooperación internacional, resaltamos que estos deben tener un carácter más expedito y que permita coadyuvar al intercambio eficaz de información entre las agencias de ley, permitiendo dar respuesta a las necesidades de investigación judicial.

Elevar a los máximos niveles de responsabilidad y toma de decisiones los temas referentes a lucha contra el cibercrimen, se requiere una posición política más activa e incluyente en estos temas que afectan en gran medida la ciudadanía en general y el uso de las TIC para el desarrollo económico de los Estados.

4. COOPERACIÓN INTERNACIONAL

Es relevante mencionar en el documento la garantía de comunicación que debe haber entre las agencias de Ley, mediante las instituciones que han sido establecidas para tal fin y en el marco de asistencia judicial internacional (Interpol, Europol, Ameripol, entre otras).

Es importante proponer que los Estados miembros generen espacios de innovación y desarrollo frente a las últimas amenazas informáticas que se presenten a nivel global, como por ejemplo, deep web, bullet pro hosting, monedas virtuales, ransomware, malware a la medida, cibercrimen como servicio y crimen organizado virtual.

Se manifiesta un interés por privilegiar el fortalecimiento de la asistencia técnica como elemento fundamental para hacer frente a los retos que plantea el tema actualmente, sin perjuicio de los debates que se adelantan sobre los eventuales instrumentos internacionales aplicables.

5. DESARROLLO DE CAPACIDADES Y ASISTENCIA TÉCNICA

Se resalta la asistencia técnica como el pilar para el trabajo mancomunado entre los países con el fin de unir y retroalimentar las diferentes modalidades del delito cibernético, procesamiento y análisis de la evidencia digital, con un sostenimiento a largo plazo, que permita establecer

canales activos y eficientes para dar una acertada orientación y trazabilidad de los objetivos planteados.

Los organismos del estado deben propender por expandir y desarrollar aún más las capacidades existentes, con el fin de soportar los requerimientos de las instituciones menos adelantadas frente al delito cibernético, generando canales que permitan la actualización continua y un respaldo efectivo.

Se considera relevante la implementación de un Centro mundial de asistencia técnica que permita reunir a los líderes de cada país en el tema, con el fin de generar escalas de capacitación y generación de doctrina que tenga una constancia en el tiempo para atender asertivamente los incidentes presentados.

***