OBSERVACIONES AL DOCUMENTO "ESTUDIO EXHAUSTIVO DEL PROBLEMA DEL DELITO CIBERNÉTICO" DE LA UNODC

ANTECEDENTES.-

El Subsecretario de Gabinete, mediante Memorando No. MDN-GAB-2016-0132-ME, del 07-MAR-2016, pone a conocimiento de esta Subsecretaría que, mediante Oficio No. MREMH-DDCS-2016-0021-O de 04-MAR-2016, se pone a conocimiento que la Secretaría de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) informa que un grupo intergubernamental de expertos se reunirá con antelación al 20° periodo de sesiones de la Comisión, para realizar un estudio exhaustivo del problema cibernético y las repuestas de los estados miembros, la comunidad internacional y el sector privado ante este fenómeno. Por lo dispuesto en la Resolución 22/7 de la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), se invita a los estados miembros a formular observaciones sobre el documento "Estudio Exhaustivo del Problema del Delito Cibernético".

Ante lo cual, este despacho, solicitó al Comando Conjunto de FF.AA. mediante Oficio No. MDN-SUF-2016-0195-OF del 08-MAR-2016, se remitan observaciones al documento "Estudio Exhaustivo del Problema del Delito Cibernético", quien a su vez responde con el Oficio No 16-COCIBER-42 de fecha 22-MAR-2016, en el que adjunta el informe solicitado.

RESUMEN DEL INFORME.-

El informe resume el documento del estudio, el cual examina el problema del delito cibernético y su afectación a nivel de gobierno, sector privado, academia y organizaciones internacionales. Se divide en ocho capítulos que tratan el ámbito de la conectividad y el delito cibernético, la perspectiva global sobre los delitos de ésta índole, la legislación y tipificación de los delitos, la aplicabilidad de las leyes en las diferentes regiones del mundo, la evidencia electrónica y su permanencia y manejo dentro de la justicia penal, y finalmente los medios cooperación internacional existentes y la prevención del delito en el ámbito público y privado.

El enfoque del estudio se limita a los aspectos del delito y de la justicia penal de la prevención y el combate del delito cibernético. Se habla sobre datos del crecimiento del delito cibernético, las tasas de victimización, estadísticas sobre capacidades policiales, herramientas informáticas delictivas, contenidos prohibidos o sancionados en internet, y violación de derechos de autor. Analiza las medidas jurídicas y su rol en la prevención y lucha contra el delito cibernético; además, se pone a conocimiento que menos de la mitad de los países encuestados perciben que sus normativas sean suficientes. Se detallan 14 actos comúnmente incluidos en el concepto de delito cibernético y la tipificación de los mismos en los países encuestados. Se mencionan los resultados de las encuestas en cuanto a aplicación de la ley y denuncias de delitos cibernéticos; los cuales se denuncian localmente pero tienen un alcance global por su naturaleza transnacional. Se habla de la cooperación internacional existente y sus limitaciones. Finalmente se trata la prevención del delito cibernético como estrategias de seguridad informática y campañas de concienciación.

El análisis realizado basa sus resultados en las encuestas realizadas a 69 estados, 11 de África, 13 de América, 19 de Asia, 24 de Europa y 2 de Oceanía; además, de información de 40 organizaciones del sector privado, 16 organizaciones académicas y 11 organizaciones intergubernamentales, realizadas en el año 2012.

ANÁLISIS.-

El Ministerio de Defensa ejerce la rectoría de la Ciberdefensa, que se define en el Acuerdo Ministerial No. 281, del 12-SEP-2014, como: "el conjunto de políticas e instrumentos articulados a la protección y defensa de la infraestructura crítica e información estratégica del Estado". Por lo antes mencionado, y por la relación existente entre las ciberamenazas y la tipificación de algunos delitos cibernéticos, el informe revisado tiene pertinencia para el sector.

En este sentido, el capítulo correspondiente a la "Tipificación del delito", en el que se identifican 14 actos contra la confidencialidad, integridad y la disponibilidad de datos o sistemas informáticos, es de interés porque se enlistan situaciones que se relacionan en la aplicación de la ley dada la ocurrencia de una ciberamenaza. Las acciones tienen que ver directamente con el acceso ilegal a sistemas informáticos, la violación de medidas de protección de datos, el acceso ilegal e intercepción de datos informáticos, y actos informáticos en respaldo de delitos de terrorismo. Para mayor provecho del contenido de este documento para el sector defensa, se podría recomendar que se incluya mayor información en lo correspondiente a tendencias sobre vulneraciones o intentos de penetrar redes de información de sectores estratégicos de los estados.

OBSERVACIÓN.-

1. El documento "Estudio Exhaustivo del Problema del Delito Cibernético", podría profundizar en lo correspondiente a tendencias sobre vulneraciones o intentos de penetrar redes de información de sectores estratégicos de los estados.

Quito, 07 de abril del 2016.