27 de julio de 2020
Español
Original: inglés

Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético
Viena, 27 a 29 de julio de 2020

Proyecto de informe

Adición

II. Lista de recomendaciones y conclusiones preliminares (*continuación*)

B. Prevención

1. De conformidad con el plan de trabajo del Grupo de Expertos, el presente párrafo contiene una recopilación de las sugerencias formuladas en la reunión por los Estados Miembros en relación con el tema 3 del programa, “Prevención”. Estas recomendaciones y conclusiones preliminares fueron formuladas por los Estados Miembros y su inclusión en este documento no supone que el Grupo de Expertos las haya hecho suyas; tampoco están presentadas en orden de importancia:

1) Debe reconocerse que la prevención no es solo responsabilidad de los gobiernos, sino que requiere la participación de todos los interesados pertinentes, incluidos los organismos encargados de hacer cumplir la ley, el sector privado, especialmente los proveedores de servicios de Internet, las organizaciones no gubernamentales, las escuelas y los círculos académicos, además del público en general.

2) Se recomendó que el público tuviera fácil acceso a instrumentos de prevención como plataformas en línea, archivos de audio e infografías en lenguaje sencillo, así como a plataformas para presentar denuncias.

3) Se consideró necesario elaborar una serie de políticas públicas de largo plazo en materia de prevención, que deberían incluir el desarrollo de campañas de sensibilización sobre el uso seguro de Internet.

4) La sensibilización sobre la ciberseguridad debería incluirse como asignatura en la enseñanza primaria, secundaria y terciaria, tanto para los estudiantes como para los docentes. Lo ideal sería que esto formara parte de una estrategia nacional de ciberseguridad. Los Estados también deberían transmitir experiencias sobre la forma de utilizar las estrategias de ciberseguridad para prevenir el delito cibernético. Además, los Estados deberían prestar especial atención a las medidas de prevención dirigidas a los jóvenes, incluidos los que cometen delitos por primera vez, a fin de evitar la reincidencia.

V.20-04123 (S) 290720 290720

5) Al prevenir y combatir el delito cibernético, los Estados deberían prestar especial atención a las cuestiones de la prevención y la erradicación de la violencia de género, la violencia contra las mujeres y las niñas y los delitos motivados por el odio.

6) Las actividades de prevención deben ser proactivas, periódicas y continuas, como también adecuadas para los grupos vulnerables.

7) La intersección y la colaboración entre los sectores público y privado con conjuntos o centros de macrodatos pueden representar un ámbito muy vulnerable, en particular, pero no exclusivamente, en el sector de la salud, en vista de la pandemia actual. Los Estados deberían prestar especial atención a la reglamentación del acceso legal a esos datos y a su protección contra los ataques de los ciberdelincuentes.

8) En cuanto a las medidas de prevención, los proveedores de servicios de Internet deberían asumir una mayor responsabilidad en cuanto a las precauciones de seguridad ("por defecto") y la prevención del delito cibernético, y deberían elaborarse normas internacionales sobre el contenido y la duración de los registros que deben conservar dichos proveedores de servicios de Internet. Además, deberían definirse claramente las responsabilidades de los proveedores de servicios de Internet en lo que respecta a la detección, prevención y desbaratamiento del delito cibernético.

9) Se necesitan alianzas público-privadas para prevenir y combatir el delito cibernético, incluida la cooperación con las partes interesadas en la ciberseguridad y las grandes empresas de tecnología en lo que respecta al intercambio de información.

10) Los Estados deberían impartir capacitación a magistrados y jueces especializados que se ocupan de los casos de delito cibernético y proporcionar a los órganos de investigación instrumentos de alto rendimiento para rastrear las criptomonedas y hacer frente a su utilización con fines delictivos.

11) Los Estados deberían intensificar las estrategias para combatir el uso por parte de los grupos delictivos tradicionales de los instrumentos cibernéticos utilizados para ocultar sus comunicaciones y actividades.

12) Deberían elaborarse soluciones para la cooperación directa de las autoridades nacionales con los proveedores de servicios de Internet, respetando al mismo tiempo el estado de derecho y los derechos humanos, incluidos los requisitos de protección de datos.

13) Los Estados deben garantizar la libertad de prensa al elaborar medidas para prevenir el delito cibernético.

14) Se recomendó fomentar las capacidades colectivas de las instituciones competentes y cambiar la cultura de prevención de una reactiva a una proactiva. También se recomendó establecer un mecanismo sólido para estimular y facilitar el intercambio de información de inteligencia sobre los posibles *modus operandi* delictivos.

15) Se alienta a los Estados Miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético; la realización de campañas relativas específicamente a los *modus operandi*, como el *phishing* o los programas maliciosos ("programas secuestradores"), y dirigidas a diferentes grupos, como los jóvenes o las personas de edad; la probabilidad de enjuiciamiento y castigo de los delincuentes y los esfuerzos por prevenir el delito mediante la detección y el desbaratamiento de las actividades ilícitas en línea en curso. El departamento de policía y la fiscalía deben invertir en detectar y señalizar las amenazas de los delitos cibernéticos y reaccionar a ellas. Es importante indicar que también en este caso es indispensable la colaboración entre el sector público y el privado. Estas actividades de prevención no requieren leyes o reglamentos adicionales.

16) Debido a la existencia de una “brecha digital”, algunos países en desarrollo carecen de capacidad para prevenir, detectar y combatir el delito cibernético, y son más vulnerables ante los desafíos que este plantea.

17) Se alentó encarecidamente a la UNODC a que siguiera prestando asistencia técnica, previa solicitud, para prevenir y combatir el delito cibernético.