INTERPOL

RESUMEN

ESTRATEGIA MUNDIAL CONTRA LA CIBERDELINCUENCIA

INTRODUCCIÓN

La ciberdelincuencia es uno de los delitos transnacionales de más rápido crecimiento a los que se enfrentan los países miembros de INTERPOL. Aunque la rápida evolución de Internet y la tecnología informática han permitido el crecimiento económico y social, una mayor dependencia de Internet ha generado más riesgos y vulnerabilidades, y ha abierto nuevas posibilidades para las actividades delictivas.

La naturaleza "sin fronteras" de la ciberdelincuencia implica que los organismos encargados de la aplicación de la ley tienen problemas para responder eficazmente, a causa de los límites en las investigaciones transfronterizas, problemas de tipo jurídico y la diversidad de capacidades en el mundo.

A diferencia de otras investigaciones, en muchos casos de ciberdelincuencia las pruebas digitales se encuentran principalmente en el sector privado, que opera y mantiene muchas partes de la infraestructura de Internet. Por ello, es fundamental colaborar entre las distintas partes interesadas a fin de abordar las nuevas amenazas cibernéticas.

ALCANCE

La *Estrategia contra la Ciberdelincuencia* describe el plan de INTERPOL para apoyar los esfuerzos de los países miembros en su lucha contra la ciberdelincuencia, mediante la coordinación y facilitación de capacidades policiales especializadas de 2016 a 2020. Se revisará periódicamente para garantizar que mantiene su relevancia, continúa respondiendo a nuevas amenazas en el dinámico entorno en el que opera, y responde a las expectativas de los países miembros.

El principal ámbito de acción del Programa de INTERPOL sobre Ciberdelincuencia es abordar la "ciberdelincuencia pura", delitos contra ordenadores y sistemas de información en los que el objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo (típicamente mediante el uso de software malicioso).

No obstante, INTERPOL reconoce la importancia de la lucha contra los delitos cibernéticos en los que el uso de ordenadores y sistemas de información amplifican el delito, como el fraude financiero y el uso terrorista de los medios sociales. Además, existe una creciente demanda de especialistas forenses informáticos para apoyar la lucha contra muchos tipos de delitos.

HACER EL CIBERESPACIO MÁS SEGURO PARA TODOS, AYUDANDO A LOS PAÍSES A IDENTIFICAR ATAQUES CIBERNÉTICOS Y SUS PERPETRADORES.

LÍNEAS DE ACCIÓN

La estrategia comprende cinco líneas de acción, con el objetivo común de ayudar a los países miembros a identificar ataques cibernéticos y sus perpetradores:

1. Evaluación y análisis de amenazas, seguimiento de las tendencias
Detectar e identificar positivamente la ciberdelincuencia, ciberdelincuentes y grupos de ciberdelincuencia, mediante evaluación de amenazas, análisis y seguimiento de las tendencias.

2. Acceso a, y explotación de, datos digitales brutos
Facilitar el acceso a datos relacionados con ataques cibernéticos, y a las herramientas y socios pertinentes, para consolidar la recopilación de datos y mejorar su explotación.

3. Proceso de gestión de pruebas digitales
Gestión de pruebas digitales encaminada a la investigación y el enjuiciamiento: recopilación legal de pistas informáticas, conservación de pruebas y hacer que éstas sean inteligibles y aceptables para el sistema judicial.

4. Correlación de información digital y física
Establecer puentes entre las huellas informáticas y la identificación física, a fin de identificar la ubicación de los posibles perpetradores.

5. Armonización e interoperabilidad
Mejorar la interoperabilidad en las operaciones y la coordinación mundial, y alentar la armonización legislativa.

CAPACIDADES Y APLICACIÓN

El Programa sobre Ciberdelincuencia está dirigido desde el Complejo Mundial de INTERPOL para la Innovación en Singapur, donde se encuentra el centro Cyber Fusion, que reúne a varias partes interesadas, un laboratorio forense digital y un centro de innovación.

Estas líneas de acción se aplicarán haciendo uso de las capacidades policiales de INTERPOL, y se ajustan a los otros dos programas mundiales de la Organización (Contraterrorismo, Delincuencia organizada y nuevas tendencias delictivas), a fin de garantizar un planteamiento coherente y eficaz en la lucha contra todas las formas de delitos transnacionales.

MODELO OPERATIVO DE INTERPOL

Los delitos actuales son cada vez más complejos. Están interconectados y se cometen a escala mundial, tanto en un ámbito físico como virtual. La cooperación policial multilateral es más necesaria que nunca para hacer frente a los problemas de seguridad que afectan a las sociedades.

Con sus 190 países miembros, INTERPOL está en una situación idónea para trabajar con las fuerzas del orden de todo el planeta a fin de reforzar su capacidad para prevenir la delincuencia e identificar y detener a los delincuentes. Las alianzas con otras organizaciones regionales e internacionales intensifican el enfoque combinado para afrontar los problemas comunes.

Las actividades de INTERPOL giran en torno a tres programas sobre delincuencia a escala internacional –lucha contra el terrorismo, delincuencia organizada y nuevas tendencias delictivas, y ciberdelincuencia–, para cada uno de los cuales se ha desarrollado una estrategia que abarca el periodo 2016-2020. Estas estrategias, y las iniciativas que engloban, irán evolucionando para adecuarse a la naturaleza dinámica del entorno operativo.

Los mencionados programas cuentan con el apoyo de un conjunto de capacidades policiales que la Organización proporciona a los países miembros, a saber: gestión de datos policiales, análisis de información criminal, apoyo en materia forense, apoyo a las investigaciones sobre prófugos, Centro de Mando y Coordinación, capacitación y formación, innovación y proyectos especiales.

Secretaría General de INTERPOL - 200, quai Charles de Gaulle - 69006 Lyon - Francia - www.interpol.int

Febrero de 2017