INTERPOL

CIBERDELINCUENCIA

Proyectos policiales que miran al futuro

En concordancia con su ayuda constante a las organizaciones internacionales con el fin de fortalecer la comunidad mundial, los Emiratos Árabes Unidos – a través de la Fundación INTERPOL para un mundo más Seguro – está financiando siete proyectos de INTERPOL en siete áreas delictivas diferentes, incluyendo Contraterrorismo, Ciberdelincuencia, Tráfico ilícito de estupefacientes, Productos ilícitos y salud mundial, Delincuencia relacionada con vehículos, Comunidades vulnerables y Protección del patrimonio cultural.

La Fundación INTERPOL para un Mundo más Seguro es el punto de encuentro donde organizaciones afines se unen a INTERPOL a fin de responder a los desafíos actuales planteados por la delincuencia. Alienta el compromiso internacional y la colaboración con el sector privado con miras a proteger a los ciudadanos, las infraestructuras, los negocios y las inversiones de las amenazas del terrorismo, la ciberdelincuencia y la delincuencia organizada.

CIBERDELINCUENCIA

ASUNTO

CIBERDELINCUENCIA

Ataques sofisticades o delitos tecnológicos

Por ejamplo : piratería, ataques con códigos maliciosos o ataques DDoS

CRIMINALIDAD FACILITADOS POR INTERNET

Delictivas 'tradicionales' facilitados por la technologia

Por ejamplo : obo, fraude e incluso terrorismo

Un número creciente de delincuentes está aprovechando la rapidez, conveniencia y anonimato de Internet para perpetrar una serie de actividades delictivas que no conoce fronteras, ni físicas ni virtuales. Estas actividades causan un grave daño y plantean amenazas muy reales para las víctimas en todo el mundo. En el pasado, la ciberdelincuencia era cometida principalmente por individuos o por pequeños grupos. Actualmente, INTERPOL constata la existencia de redes de ciberdelincuencia muy complejas que reúnen a individuos de todo el planeta en tiempo real para cometer delitos a una escala sin precedentes.

Las organizaciones delictivas utilizan cada vez más Internet para facilitar sus actividades y optimizar sus beneficios en el menor espacio de tiempo. Los delitos tecnológicos más avanzados como piratería, ataques con códigos maliciosos o ataques DDoS constituyen amenazas a la seguridad de los gobiernos, negocios e individuos, y suponen un desafío para los organismos encargados de la aplicación de la ley, pues muchos países todavía no cuentan con las capacidades o conocimientos técnicos necesarios para combatirlos. El creciente uso de la tecnología para facilitar los delitos como robo, fraude e incluso terrorismo agrega una nueva dimensión a estas actividades delictivas 'tradicionales'.

Dada la naturaleza transnacional inherente a la ciberdelincuencia, es muy probable que las pruebas estén localizadas en diferentes jurisdicciones. En la actualidad, muchos organismos encargados de la aplicación de la ley no cuentan con la capacidad de realizar los análisis de datos necesarios para avanzar en las investigaciones sobre ciberdelincuencia, ni tienen acceso en tiempo real a información sobre amenazas que pueden influir de forma importante en la seguridad de sus ciudadanos e infraestructura.

La naturaleza elusiva de la ciberdelincuencia implica que los organismos encargados de la aplicación de la ley necesitan adoptar nuevas técnicas a fin de prevenir la ciberdelincuencia, así como identificar los delitos, los modelos de delincuencia y las líneas de investigación que sean lo suficientemente sólidas como para justificar una investigación policial.

EL PAPEL DE INTERPOL

APOYO Y FORMACIÓN DE NUESTROS PAÍSES MIEMBROS

INTERPOL lleva a cabo una serie de actividades para apoyar a sus países miembros en la lucha contra la ciberdelincuencia. Ofrece su ayuda a investigaciones sobre ciberdelincuencia, trabaja para desarrollar nuevas tecnologías innovadoras, ayuda a los países a utilizar las pruebas digitales, realiza sesiones de formación, asiste a los países en la revisión de sus capacidades de lucha contra la ciberdelincuencia y elabora información policial operativa para ayudar a prevenir y contrarrestar la ciberdelincuencia.

Asimismo, ayuda a coordinar investigaciones y operaciones transnacionales sobre ciberdelincuencia, tanto in situ como de forma remota desde el Complejo Mundial de INTERPOL para la Innovación (IGCI) en Singapur, donde se ubican las actividades de lucha contra la ciberdelincuencia de la Organización, mediante el intercambio de información policial y la orientación en cuanto a las buenas prácticas en las investigaciones sobre ciberdelincuencia.

Ofrece asimismo una serie de cursos de formación enfocados en las necesidades de los participantes, que abordan temas como tendencias emergentes en ciberdelincuencia, técnicas de investigación, análisis forense digital y otros. Las sesiones de formación se han centrado en varios campos, entre otros: actividad delictiva organizada en la red oscura; herramientas y técnicas forenses digitales; y análisis de códigos maliciosos.

CYBER FUSION CENTRE

El Cyber Fusion Centre (CFC), reúne a expertos procedentes de organismos encargados de la aplicación de la ley y de la industria para recopilar y analizar toda la información disponible sobre actividades delictivas en el ciberespacio. Su objetivo es proporcionar a los países información policial útil y coherente que pueda transformarse en acciones operativas de prevención de delitos e identificación de delincuentes.

ASOCIACIONES PRIVADAS

Dado que los delincuentes constantemente evolucionan y adaptan sus herramientas y métodos, INTERPOL desarrolla nuevas herramientas policiales punteras consultando a socios de la industria cibernética, y prueba nuevas tecnologías privadas para ser utilizadas por los organismos encargados de la aplicación de la ley.

LABORATORIO FORENSE DIGITAL

A través del Laboratorio Forense Digital, INTERPOL ayuda a los países a mejorar su capacidad de detectar y utilizar pruebas digitales como parte de su trabajo diario, pues la capacidad de extraer pruebas de ordenadores, teléfonos móviles y otros dispositivos es fundamental para apoyar las investigaciones y construir casos sólidos contra los sospechosos. Asiste también analizando códigos maliciosos, examinando dispositivos digitales, probando nuevas herramientas forenses digitales en desarrollo, formando a los policías en el uso de las últimas herramientas y técnicas forenses digitales, y proporcionando asistencia durante las investigaciones.

EL FUTURO

Dado que los delincuentes cibernéticos constantemente evolucionan y adaptan sus herramientas y métodos, INTERPOL también actualiza continuamente su apoyo a los países miembros a fin de abordar la ciberdelincuencia.

PLATAFORMA DE INFORMACIÓN Y ANÁLISIS

Responder a los nuevos desafíos a los que se enfrentan los organismos encargados de la aplicación de la ley en su lucha contra la ciberdelincuencia requiere un nuevo planteamiento sobre el intercambio de información policial, a fin de mantener el paso de los rápidos cambios en las investigaciones sobre ciberdelincuencia y en el análisis forense digital.

Si bien es importante el intercambio de datos policiales a nivel internacional, los datos sin procesar por sí solos no son suficientes para generar una imagen clara de los cambios, amenazas y tendencias en el ámbito de la delincuencia. Para apoyar el análisis de datos y la producción de información policial utilizable, INTERPOL está creando una plataforma en tiempo real para el intercambio de información y el análisis.

Esta plataforma será más que un repositorio de datos: INTERPOL y usuarios autorizados en países miembros podrán realizar investigaciones y análisis, y conectar con expertos de todo el mundo.

EVALUACIÓN DE AMENAZAS CIBERNÉTICAS

INTERPOL trabaja siempre sobre nuevos métodos para garantizar que los países miembros estén equipados y al día para enfrentarse a las últimas amenazas cibernéticas, y alienta a los países a publicar notificaciones y difusiones de INTERPOL con el fin de alertar a las fuerzas policiales de todo el mundo sobre amenazas conocidas.

Se realizarán estudios con el fin de aportar previsión estratégica en cuanto a las tendencias de la ciberdelincuencia, como la venta por parte de los delincuentes de sus herramientas de ciberdelincuencia al mayor postor en la 'ciberdelincuencia como un servicio', apoyando así a los países miembros a desarrollar su disposición operativa. De forma paralela, INTERPOL desarrolla herramientas para contrarrestar estas amenazas.

CONEXIÓN DE LO DIGITAL Y LO FÍSICO

Las pistas electrónicas que pueden conducir a los ciberdelincuentes están normalmente en posesión de entidades privadas, como los proveedores de servicios de Internet, que cuentan con equipos especializados de gestión de incidentes de seguridad. Con el fin de crear puentes entre esta información policial en manos privadas y los investigadores de organismos encargados de la aplicación de la ley, INTERPOL realizará actividades de comunicación dirigidas a la comunidad de gestión de incidentes de seguridad del sector privado, para transmitir los requisitos de las investigaciones en materia de ciberdelincuencia y establecer relaciones positivas con el sector.

Vincular la información digital (direcciones IP, identificadores de dispositivos móviles) con la información física (biometría, ubicaciones) con el fin de identificar sospechosos de ciberdelincuencia será un nuevo ámbito de trabajo. Para ello, INTERPOL va a identificar y probar las tecnologías y los métodos de investigación más prometedores y novedosos en colaboración con la industria privada y el sector académico. Podría incluir:

- **Reconocimiento facial**
- **Reconocimiento de objetos basado en imágenes**
- **Análisis de textos**
- **Análisis integrado para vincular los delitos cibernéticos y los delincuentes con el mundo físico**

INTERPOL

www.interpol.int