INTERPOL

CYBERCRIMINALITÉ

Des projets de police tournés vers l'avenir

En écho au soutien constant qu'ils apportent aux organisations internationales pour renforcer la communauté mondiale, les Émirats arabes unis financent, par l'intermédiaire de la Fondation INTERPOL pour un monde plus sûr, sept projets INTERPOL visant des types de criminalité différents, à savoir la lutte contre le terrorisme, la cybercriminalité, le trafic de drogues, le trafic de biens illicites et la santé mondiale, la criminalité liée aux véhicules, les communautés vulnérables et la protection du patrimoine culturel.

La Fondation INTERPOL pour un monde plus sûr rassemble des organisations qui partagent la même vision et s'unissent à INTERPOL pour faire face aux défis actuels en matière de criminalité. Elle œuvre pour un engagement à l'international et des partenariats avec le secteur privé pour protéger les citoyens, les infrastructures, les entreprises et les investissements face aux menaces que représentent le terrorisme, la cybercriminalité et la criminalité organisée.

CYBERCRIMINALITÉ

LA PROBLÉMATIQUE

CYBERCRIMINALITÉ

Criminalité sophistiquée ou de très haute technologie

Ex. Piratage, logiciels malveillants, extortion DDOS

CRIMINALITÉ FACILITÉE PAR INTERNET

Activités criminelles "Traditionelles" facilitées par la technologie

Ex. les vols, la fraude, et même le terrorisme

Un nombre croissant de malfaiteurs tirent parti de la vitesse, de la facilité d'utilisation, et de l'anonymat d'Internet pour se livrer à diverses activités criminelles que ne limite aucune frontière, physique ou virtuelle. Ces activités sont particulièrement préjudiciables et représentent une menace bien réelle pour les personnes qui en sont victimes dans le monde. Jusqu'à présent, la cybercriminalité était principalement le fait d'individus ou de petits groupes. Aujourd'hui, INTERPOL constate l'apparition de réseaux de cybercriminalité d'une grande complexité qui réunissent, en temps réel, des individus de tous pays pour perpétrer des infractions d'une ampleur sans précédent.

Les organisations criminelles privilégient de plus en plus Internet pour faciliter leurs activités et réaliser des bénéfices maximum en un minimum de temps. La criminalité de très haute technologie comme le piratage informatique, les attaques par logiciel malveillant, et l'extorsion DDoS, représente une menace réelle pour la sécurité des gouvernements, des entreprises, et des particuliers. Elle présente, en outre, d'importants défis pour les services chargés de l'application de la loi, car de nombreux pays ne disposent pas encore de la connaissance ou des compétences techniques nécessaires pour y faire face. L'utilisation accrue de la technologie pour commettre les infractions comme les vols, la fraude et même le terrorisme ajoute une nouvelle dimension à ces activités criminelles « traditionnelles ».

Au regard de la nature intrinsèquement transnationale de la cybercriminalité, les éléments de preuve relèveront très probablement de plusieurs juridictions. Actuellement, la plupart des services chargés de l'application de la loi ne sont pas en mesure d'analyser les données requises pour approfondir les enquêtes sur la cybercriminalité. En outre, ils n'ont pas accès aux informations en temps réel sur les menaces susceptibles de nuire gravement à la sécurité des citoyens et des infrastructures.

En raison de la nature mouvante de la cybercriminalité, les services chargés de l'application de la loi doivent adopter de nouvelles techniques afin de prévenir la cybercriminalité, et mettre en évidence des infractions, des schémas criminels, ainsi que des pistes d'enquête suffisamment solides pour justifier l'ouverture d'une enquête criminelle.

LE RÔLE D'INTERPOL

AIDER ET FORMER LES PAYS MEMBRES

INTERPOL a mis en place plusieurs dispositifs pour aider les pays membres à lutter contre la cybercriminalité. Nous apportons notre soutien lors des enquêtes sur la cybercriminalité, proposons de nouvelles technologies innovantes, fournissons une assistance aux pays dans le cadre du traitement des éléments de preuve numériques, réalisons des formations, aidons les pays à passer en revue leurs capacités de lutte contre la cybercriminalité, et communiquons des renseignements exploitables pour contribuer à la prévention et la lutte contre la cybercriminalité.

Nous facilitons la coordination des enquêtes et des opérations sur la cybercriminalité transnationale, que ce soit sur site ou à distance depuis le Complexe mondial INTERPOL pour l'innovation (CMII) à Singapour qui regroupe les activités de lutte contre la cybercriminalité de l'Organisation, en partageant des renseignements et en recommandant des meilleures pratiques à mettre en œuvre dans le cadre des enquêtes sur la cybercriminalité.

Nous proposons un programme complet de formations adaptées aux besoins des participants qui portent, par exemple, sur les nouvelles tendances de la cybercriminalité, les techniques d'enquête, l'informatique légale, etc. Nous avons déjà organisé des sessions sur de nombreux domaines, notamment la criminalité organisée sur le Darknet ; les outils et techniques de l'informatique légale ; et l'analyse des logiciels malveillants.

CYBER FUSION CENTRE

Le CFC (Cyber Fusion Centre) d'INTERPOL réunit des experts en cybercriminalité des services chargés de l'application de la loi et du secteur privé afin de recueillir et analyser toutes les informations disponibles sur les activités criminelles dans le cyberespace et de fournir aux pays des renseignements cohérents et exploitables susceptibles de donner lieu à une action opérationnelle en vue d'empêcher les infractions et de faciliter l'identification des malfaiteurs.

PARTENARIATS PRIVÉS

Face à l'évolution et à l'adaptation permanentes des outils et des méthodes des malfaiteurs, INTERPOL s'attache à développer de nouveaux outils policiers de pointe en consultation avec ses partenaires de l'industrie cybernétique et teste de nouvelles technologies privées en vue de leur utilisation par les services chargés de l'application de la loi.

LABORATOIRE D'INFORMATIQUE LÉGALE

Par le biais de son Laboratoire d'informatique légale, INTERPOL aide les pays à renforcer leurs capacités de détection et d'exploitation des éléments de preuve numériques dans le cadre du travail quotidien de la police, car il est fondamental de pouvoir extraire les éléments de preuve des ordinateurs, des téléphones mobiles, et d'autres périphériques pour étayer les enquêtes et constituer des dossiers solides contre les suspects. Nous facilitons l'analyse des logiciels malveillants, l'examen des périphériques numériques, les essais sur les nouveaux outils d'informatique légale en développement, la formation des officiers de police aux outils et techniques les plus récents de l'informatique légale, et nous fournissons un soutien au cours des enquêtes.

LES PERSPECTIVES

Les cybermalfaiteurs n'ayant de cesse de faire évoluer et d'élaborer de nouveaux outils et méthodes, INTERPOL doit s'attacher à adapter en permanence le soutien fourni à ses pays membres dans le cadre de la lutte contre la cybercriminalité.

PLATEFORME D'INFORMATION ET D'ANALYSE

Pour répondre aux nouveaux enjeux de la lutte contre la cybercriminalité, les services chargés de l'application de la loi doivent adopter une nouvelle approche en matière d'échange d'informations de police, capable de soutenir le rythme rapide des développements des enquêtes sur la cybercriminalité et de l'informatique légale.

Si le partage mondial des données de police est important, les données brutes ne suffisent pas à elles seules à produire une image claire des évolutions, des menaces et des tendances de la criminalité. Pour soutenir l'analyse des données et la production de renseignements exploitables, INTERPOL développe une plateforme de partage et d'analyse en temps réel de l'information.

Cette plateforme sera plus qu'un simple référentiel de données : INTERPOL et les utilisateurs autorisés des pays membres pourront effectuer des requêtes, réaliser des analyses, et échanger avec des experts du monde entier.

ÉVALUATION DES CYBERMENACES

INTERPOL mène un travail constant pour élaborer de nouvelles méthodes afin que ses pays membres soient sensibilisés aux cybermenaces les plus récentes, et qu'ils acquièrent les outils nécessaires pour les combattre. Aussi sont-ils encouragés à publier les notices et diffusions INTERPOL pour alerter toutes les polices du monde sur les menaces connues.

Des recherches vont être menées pour établir une prospective stratégique sur les tendances de la cybercriminalité, par exemple la vente par les malfaiteurs de leurs outils de cybercriminalité au soumissionnaire le plus offrant dans le cadre d'une « prestation de criminalité », ce qui aidera les pays membres à mieux se préparer au plan opérationnel. En parallèle, INTERPOL travaille au développement d'outils pour lutter contre ces menaces.

RELIER LES MONDES NUMÉRIQUE ET PHYSIQUE

Les « indices » électroniques susceptibles d'identifier les auteurs d'actes de cybercriminalité sont souvent détenus par des entités privées comme les fournisseurs d'accès à Internet, qui disposent d'équipes spécialisées pour gérer les incidents de sécurité. INTERPOL va s'engager dans un effort de sensibilisation dans le but de former la communauté privée de la sécurité aux exigences des enquêtes dans le cyberespace et d'établir des relations constructives afin que les enquêteurs des services chargés de l'application de la loi puissent avoir accès aux renseignements détenus par le secteur privé.

La capacité à mettre en corrélation les informations numériques (adresses IP, identifiants des périphériques mobiles) et les informations physiques (données biométriques, localisations) afin d'identifier les suspects d'actes de cybercriminalité va constituer un nouveau domaine d'intervention de la plus haute importance ; de ce fait, INTERPOL va identifier et tester les méthodes et les technologies d'enquête récentes les plus prometteuses en collaboration avec le secteur privé et le monde universitaire. Elles peuvent porter sur :

- **la reconnaissance faciale**
- **la reconnaissance d'objets sur la base d'images**
- **l'analyse de texte**
- **l'analyse intégrée pour lier la cybercriminalité et les cybercriminels au monde physique**

INTERPOL

www.interpol.int