INTERPOL

CYBERCRIME

Future-oriented policing projects

In keeping with its consistent support of international organisations to strengthen the global community, the United Arab Emirates – through the Interpol Foundation for a Safer World – is funding seven INTERPOL projects within seven crime areas, including Counter Terrorism, Cybercrime, Illicit Drug Trade, Illicit Goods and Global Health, Vehicle Crime, Vulnerable Communities and Protecting Cultural Heritage.

The INTERPOL Foundation for a Safer World is the rallying point for likeminded organizations to unite with INTERPOL to respond to today's crime challenges. It encourages an international commitment and partnership with the private sector to protect citizens, infrastructures, businesses and investments from the threats of terrorism, cybercrime and organized crime.

CYBERCRIME

THE ISSUE

CYBERCRIME

Sophisticated attacks, or high-tech crimes

For example, hacking, malware attacks, DDOS extortion

CYBER-ENABLED CRIME

'Traditional' crimes which are facilitated by technology

For example, theft, fraud, even terrorism

More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. These activities cause serious harm and pose very real threats to victims worldwide. In the past, cybercrime was committed mainly by individuals or small groups. Today, INTERPOL is seeing highly complex cybercriminal networks bringing together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organizations are turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. Advanced high-tech crimes such as hacking, malware attacks and DDoS extortion pose real threats to the security of governments, businesses and individuals and present challenges to law enforcement, as many countries do not yet have the technical knowledge or skills necessary to confront them. The increasing use of technology to facilitate crimes like theft, fraud and even terrorism adds a new dimension to these 'traditional' criminal activities.

Given the inherently transnational nature of cybercrime, it is highly likely that evidence will be located across various jurisdictions. Currently, many law enforcement agencies do not have the capability to conduct analysis on data that is necessary to further cybercrime investigations, nor do they have access to real-time threat information that may have a serious impact upon the safety of their citizens and infrastructure.

The elusive nature of cybercrime means that law enforcement bodies need to adopt new techniques in order to prevent cybercrimes, identify offences, patterns of crime and lines of enquiry that are robust enough to justify a criminal investigation.

INTERPOL'S ROLE

SUPPORT AND TRAIN OUR MEMBER COUNTRIES

INTERPOL carries out a variety of activities to support our member countries in the fight against cybercrime. We offer support to cybercrime investigations, work to develop innovative new technologies, assist countries in exploiting digital evidence, conduct training sessions, assist countries in reviewing their cybercrime-fighting capacities and develop actionable intelligence to help prevent and counter cybercrimes.

We help coordinate transnational cybercrime investigations and operations, either on-site or remotely from the INTERPOL Global Complex for Innovation (IGCI) in Singapore where the Organization's cybercrime fighting activities are based, through intelligence sharing and providing guidance on best practices in conducting cybercrime investigations.

We provide a range of training courses, targeted to the needs of participants, covering topics such as emerging trends in cybercrime, investigation techniques, digital forensics and more. Training events have focused on a range of areas including organized criminal activity on the Darknet; digital forensic tools and techniques; and malware analysis.

CYBER FUSION CENTRE

The Cyber Fusion Centre (CFC) brings together cyber experts from law enforcement and industry to gather and analyse all available information on criminal activities in cyberspace to provide countries with coherent, usable intelligence which can be transformed into operational action to both prevent crime and aid in the identification of criminals.

PRIVATE PARTNERSHIPS

As criminals are constantly evolving and adapting their tools and methods, INTERPOL works to develop new cutting-edge policing tools in consultation with partners in the cyber industry, and tests new private technologies with a view to their use by law enforcement.

DIGITAL FORENSICS LABORATORY

Through the Digital Forensics Laboratory, INTERPOL assists countries in enhancing their ability to detect and use digital evidence as part of their everyday police work, as the ability to extract evidence from computers, mobile phones and other devices is critical in supporting investigations and building strong cases against suspects. We help analyse malware, examine digital devices, test new digital forensic tools under development, train police in the latest digital forensic tools and techniques, and provide assistance during investigations.

LOOKING AHEAD

As cybercriminals are continually evolving and developing new tools and methods, so too is INTERPOL continually adapting its support to member countries to tackle cybercrime.

INFORMATION AND ANALYSIS PLATFORM

Responding to the emerging challenges faced by law enforcement in combating cybercrime requires a novel approach to the exchange of police information which can keep pace with the high-speed developments in cybercrime investigations and digital forensics.

While sharing police data globally is important, raw data alone is not enough to generate a clear picture of criminal developments, threats and trends. To support data analysis and the generation of usable intelligence, INTERPOL is developing a real-time information sharing and analytical platform.

This platform will go beyond the role of a data repository: INTERPOL and authorized users in member countries will be able to conduct research, analysis and connect with experts worldwide.

ASSESSING CYBER THREATS

INTERPOL is always working on new methods to ensure member countries are aware of, and equipped to confront, the latest cyber threats, such as encouraging countries to issue INTERPOL notices and diffusions to alert police worldwide to known threats.

Research will be conducted to provide strategic foresight into cybercrime trends, such as criminals selling their cybercrime tools to the highest bidder in ‘cybercrime as a service’, thus supporting member countries to develop their operational readiness. In parallel, INTERPOL is working to develop tools to counter these threats.

CONNECTING THE DIGITAL AND PHYSICAL

Electronic 'clues' which can lead to cybercrime perpetrators are usually held by private parties such as Internet service providers, which have specialized teams to manage security incidents. To bridge the gap between this privately held intelligence and law enforcement investigators, INTERPOL will conduct outreach to educate the private incident security community on the requirements of cyber investigations and develop positive relationships.

Linking digital information (IP addresses, mobile device identifiers) with physical information (biometrics, locations) in order to identify cybercrime suspects will be an important new area of focus; therefore INTERPOL is going to identify and test the most promising new investigative methods and technologies in collaboration with private industry and academia. These could include:

- **Facial recognition**
- **Image-based object recognition**
- **Text analysis**
- **Integrated analysis to link cybercrimes and criminals with the physical world**

11:08
cherry mobile

INTERPOL

www.interpol.int