INTERPOL

Supporting digital crime investigations

The rapid development of the Internet and technology has shaped and improved the world around us. But the transition to a digital age also offers new opportunities for criminals, consequently presenting new challenges for police worldwide.

Criminals are increasingly exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of crimes that know no borders, either physical or virtual. It is therefore essential for police to adapt their responses to effectively confront this new and evolving type of crime.

INTERPOL is committed to becoming a global coordination body for the detection and prevention of digital crimes through its INTERPOL Global Complex for Innovation (IGCI), which houses INTERPOL's Global Cybercrime Programme. INTERPOL seeks to facilitate transnational digital crime investigations and provide operational support to police across its 190 member countries.

As a guiding principle we focus on making cyberspace more secure, while at the same time preserving its openness. In consultation with our member countries, we have designed a model for international law enforcement cooperation against cyber criminals.

ACTIVITIES TO SUPPORT DIGITAL CRIME INVESTIGATIONS

DIGITAL CRIME INVESTIGATIVE SUPPORT

INTERPOL assists member countries in coordinating and facilitating transnational cybercrime investigations and operations. We can provide support either remotely or on-site. Remote support may include facilitating sharing of information or intelligence via tele-meetings or providing guidance and advice in terms of best practices in cybercrime investigations. Depending on the requirements of the member country officers may travel to the location of the incident to provide on-site support in coordinating expertise.

We also bring together relevant law enforcement agencies of member countries, as well as the private sector and academia where necessary to facilitate joint investigative work.

These activities mainly focus on cybercrime related to botnets, malware and high end cybercrime-enablers such as bulletproof hosting services, professional remittance services, DDoS services, etc.

SUPPORTING DIGITAL CRIME INVESTIGATIONS

CYBER FUSION CENTRE

The Cyber Fusion Centre (CFC) is a multi-stakeholder environment bringing together law enforcement specialists and industry experts. The CFC uses innovative techniques to make full use of all information available to generate actionable intelligence capable of impacting upon criminal cyber activity in member countries.

The CFC supplies the expertise and infrastructure to manage and facilitate support to dynamic cyber operational activity. CFC functions in collaboration with the DIS unit and member countries to coordinate and deliver operational activity.

Actionable intelligence

The CFC is the single point of entry for global cyber-related information and intelligence. It provides a gateway to receive, analyze and securely store all cyber-related information and intelligence The CFC also develops and disseminates actionable intelligence products to relevant member countries for action and can assist member countries check if a new request has been made or new information has already been shared or acted upon, to avoid duplication of effort.

Live operations

The fusion centre is the hub where INTERPOL supports live cyber operations, such as regional anti-cybercrime campaigns including the ASEAN and Americas operational surges in 2017.

24/7 CONTACT NETWORK

INTERPOL manages a list of specialized National Reference Points for the exchange of police information on cybercrime. These dedicated points of contact are from the cybercrime units of INTERPOL's member countries who provide an avenue for rapidly exchanging information on cybercrime and facilitating transnational law enforcement cooperation.

REGIONAL WORKING GROUPS ON CYBERCRIME FOR HEADS OF UNIT

Cybercrime working groups have been created to better assess regional crime trends and to formulate action plans and transnational operations.

The annual working group meetings for each of the regions – Africa, Americas, Eurasia (Europe and Asia/South Pacific) and Middle East and North Africa - provide an invaluable platform to discuss the latest cybercrime trends and other issues, and act as a springboard for formulating regional action plans and operations to fight cybercrime. To ensure that the police keep pace with technological developments and have the required expertise and skills to deal with evolving digital crime at the national and international levels, DIS has also been organizing regional Train-the-Trainer for Cybercrime Investigation courses to enhance the capacity of member countries in cybercrime investigation.

REGIONAL BUREAU DIGITAL CRIME OFFICERS

Digital Crime Officers (DCO) will be recruited in each of INTERPOL's Regional Bureaus and will serve as the liaison point with the IGCI in relation to operational support and capacity building at the regional level.

INTERPOL

- **CONTACT INFORMATION:**
  Global Complex for Innovation
  18 Napier Road
  Singapore 258510

  Tel: +65 6550 3535
  Email: IGCI@interpol.int

- **Twitter: @INTERPOL_HQ**
- **YouTube: INTERPOLHQ**
- **WWW.INTERPOL.INT**