INTERPOL

INTERPOL's Proposals for the Comprehensive International Convention on Countering the Use of Information Communications Technologies for Criminal Purposes

Proposals related to chapters to be examined at the second formal session of the Ad Hoc Committee

MARCH 2022

Introduction

As part of the work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC), INTERPOL would like to propose relevant provisions that highlight the needs and perspective of global law enforcement, and the areas in which INTERPOL can support its 195 member countries.

This document may serve as a reference for Member States in formulating their contributions to the second formal session of the AHC or suggested provisions for the Convention. It also serves as INTERPOL's input for the first Intersessional consultation with multi-stakeholders scheduled between the first and second formal sessions of the AHC.

These provisions are based upon INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, submitted on 8 November 2021 to the AHC. This initial contribution details four Strategic Priorities which, in INTERPOL's view, are key for this new international legal instrument to become an effective and practical tool to counter the criminal use of Information and Communications Technologies. The four strategic priorities are:

1. Enhance international law enforcement cooperation for a timely and effective global response to cybercrime
2. Reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime
3. Close gaps and bridge divides in capabilities, capacity and information sharing across the globe to overcome the challenges of investigating cybercrime
4. Maximize prevention efforts through Public-Private Partnerships for proactive disruption of cyber threats and their ecosystem

With reference to document A/AC.291/L.4/Add.4, INTERPOL will focus on Chapter 3 of the proposed structure of the Convention entitled "Procedural measures and Law Enforcement", which is most relevant to the mandate of our Organization. INTERPOL's proposals are summarized below:

Article related to "Law enforcement cooperation" – Role of INTERPOL for the secure and rapid exchange of information between law enforcement authorities *within* and *between* countries.

Article related to the "Cooperation between national authorities and the private sector" – Role of INTERPOL in the exchange of information between law enforcement and the private sector.

INTERPOL's proposals for the "Procedural measures and Law Enforcement" chapter of the Convention

Article related to "Law enforcement cooperation" – Role of INTERPOL for the secure and rapid exchange of information between law enforcement authorities *within* and *between* countries

- […] States Parties shall, in particular, take effective measures:

  (a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services, including through the International Criminal Police Organization (INTERPOL), in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

  (b) To cooperate with other States Parties in conducting inquiries and exchanging information with respect to offences covered by this Convention, including through the International Criminal Police Organization (INTERPOL), concerning:

    (i) the identity, whereabouts and activities of persons suspected of involvement in such offences, the computer data and systems in these persons' possession or control, or the location of other persons concerned; […]
    (ii) the identity of the victims of such offences, and the type of data copied, transmitted, viewed, altered, tampered, interfered with, stolen or used, by persons suspected of involvement in such offences;

  (c) To exchange information with other States Parties on specific means and methods used to commit offences covered by this Convention, including through the International Criminal Police Organization (INTERPOL). […]

*(**References**: Art. 27 UN Convention against Transnational Organized Crime, Art. 48 UN Convention against Corruption, Art. 9 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018), and A/RES/71/19 (2016))*

COMMENTARY

- ***Aim:** Highlight and promote the use of existing, proven communication channels and mechanisms to effectively support law enforcement in the fight against transnational crime.*

This article entitled **"Law enforcement cooperation"** reaffirms the need for strong and efficient cooperation between law enforcement to prevent, investigate, disrupt, and effectively prosecute the use of information and communications technologies (hereafter known as ICTs) for criminal purposes. Fostering law enforcement cooperation is at the heart of the mandate given to INTERPOL by its 195 member countries.

Paragraph (a) encourages States Parties to use INTERPOL's communication infrastructure in order for the relevant authorities, and in particular, for law enforcement agencies within States Parties to share information on the criminal use of ICTs.

Paragraph (b) highlights the use of the INTERPOL Information System for State Parties to exchange information between themselves. This includes information on the identity and whereabouts of threat actors, the digital and online infrastructure they use, the type of data copied, transmitted, viewed, altered, tampered, interfered with, stolen or used, and the victims targeted by these threat actors.

Through INTERPOL's Notices and diffusions, States Parties are also able to send requests for cooperation and share critical information.

Red Notices are requests to law enforcement worldwide to locate and provisionally arrest a person pending extradition, surrender, or similar legal action. It contains information to identify the wanted person, as well as information related to the crime they are wanted for.

Blue Notices are requests to law enforcement worldwide to collect additional information about a person's identity, location or activities in relation to a crime. This information is centralized by INTERPOL, and made available to each of the Organization's member countries.

INTERPOL's Global Communication System, called I-24/7, securely connects each of the Organization's 195 member countries through their National Central Bureau. It enables authorized users to share sensitive and urgent police information with their counterparts around the globe for the primary purpose of assisting in the prevention, detection and investigation of crime, in accordance with the INTERPOL mandate. UN General Assembly resolution A/RES/75/10 (2020) encourages increased cooperation between the United Nations and INTERPOL to assist Member States in effectively using INTERPOL's global secure communications system (article 13).

Article 14 of the same UNGA resolution (A/RES/75/10) acknowledges the importance for National Central Bureaus to expand further INTERPOL's global secure communications system to other national law enforcement entities at strategic locations with a view to increasing the security of their borders. Extending real-time access to I-24/7 allows, for example, a frontline officer to verify in real time whether a passport has been stolen, or a firearms specialist from an anti-crime unit to verify a ballistic profile. INTERPOL's global communication system can also be made available to non-police entities upon NCB's authorization.

IN THE FIELD

In 2021 alone, law enforcement across the world exchanged above 26 million messages via the INTERPOL global communication system, I-24/7. This system allowed law enforcement to conduct approximately 4 billion searches in INTERPOL's 19 databases, containing over 120 million records. Among these databases, the INTERPOL's International Child Sexual Exploitation (ICSE) database allows specialized investigators to share data on cases of child sexual abuse. On average, the ICSE database helps identify seven child abuse victims every day. In total ICSE has assisted in the identification of more than 26,000 victims worldwide, and more than 12,000 offenders.

Further, with the aim of supporting police in obtaining, exchanging and disseminating actionable criminal intelligence on cybercrime, INTERPOL has created the **Cybercrime Knowledge Exchange** for general sharing of good practices, and **Cybercrime Collaborative Platform** for operational purpose. These platforms allow law enforcement to keep pace with cyber-criminal threats and techniques by exchanging knowledge and information securely and rapidly between member countries.

IN THE FIELD

In November 2021, the cooperation between INTERPOL and the law enforcement authorities of the Republic of Korea, Ukraine, and the United States, with support from private partners, resulted in one of global law enforcement's first online criminal gang arrests. In the operation, codenamed Operation Cyclone, INTERPOL's Cyber Fusion Centre in Singapore – with its established collaboration with private partners – was able to analyze threat data and information from multiple sources, and produce relevant actionable intelligence reports to member countries, helping to prevent further cyberattacks. In addition to the arrest in Ukraine of six members of a ransomware family (June 2021), two Red Notices were circulated to INTERPOL's 195 member countries upon the request of the Republic of Korea. As such, Operation Cyclone continues to supply evidence that feeds into further cybercrime investigations. This operation also highlights the importance of the exchange of information between public-private partners and law enforcement, which was made possible through INTERPOL's platforms and expertise.

Paragraph (c) encourages States Parties to use INTERPOL channels to share information on cybercriminals' modus operandi. This type of information is specifically circulated within INTERPOL's Purple Notices.

Purple Notices are requests to law enforcement worldwide to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals. As with Blue Notices, this information is then centralized by INTERPOL, and made available to member countries.

IN THE FIELD

During the global pandemic, INTERPOL actively supported member countries in countering increased attempts of ransomware attacks, especially those targeting institutions at the forefront of the fight against the COVID-19 outbreak, such as hospitals and medical services. In 2020, INTERPOL issued a Purple Notice alerting police in all its member countries of the heightened ransomware threat designed to lock organizations out of their critical systems in an attempt to extort payments. The Notice included relevant information on ransomware with the aim to ultimately assist law enforcement in ensuring that vital healthcare systems remained untouched and the criminals targeting them held accountable.

Article related to Private sector – Role of INTERPOL in the exchange of information between law enforcement and the private sector

- States Parties shall take such measures as may be necessary to encourage, in accordance with their domestic laws, to facilitate the secure and rapid exchange of information between law enforcement agencies and relevant private entities, including through the International Criminal Police Organization (INTERPOL), for the prevention and investigation of the offences set forth in this Convention.

*(**References:** Art. 39 UN Convention Against Corruption, GGE report 2021 A/76/135 (para. 30, 35), INTERPOL General Assembly Resolutions GA-2019-88-RES-11 and GA-2021-89-RES-11)*

COMMENTARY

➢ ***Aim:** Reinforce the cooperation and knowledge exchange between law enforcement and the private sector through INTERPOL's dedicated framework*

The prevention of cybercrime requires participation of various stakeholders, including governments, law enforcement authorities, the private sector, international organizations and civil society organizations. It is to that aim that the INTERPOL General Assembly endorsed **the "Gateway" initiative**, which enables the Organization to exchange information with private sector companies with which it has signed legal arrangements.

Through this unique partnership, INTERPOL is able to receive and analyze data from private sector entities using its secure cybercrime database and analytical platforms, and produce various cyber intelligence products for member countries. This enables member countries to carry out follow-up preventive action or disruption, including but not limited to investigations, arrests, searches and seizures. This is also made possible by INTERPOL's Rules for Processing Data (RPD), and in particular Article 28, which regulates the exchange and processing of data with and by private entities under agreements concluded with INTERPOL. As such, INTERPOL is well placed to act as an interlocutor between law enforcement and the private sector, enabling crucial information flow.

Since cooperation with the private sector is key, this paragraph encourages States Parties to use INTERPOL's "Gateway" to facilitate the secure and rapid exchange of information between law enforcement agencies and relevant private entities for the prevention and disruption of the cybercrime. The use of INTERPOL channels enables the safe and secure transmission of sensitive data between public and private entities.

IN THE FIELD

In May 2021, the Irish Heath Service Executive was hit by a large-scale Conti ransomware attack. At the request of Ireland, INTERPOL provided assistance in the investigation, deploying expertise and sharing information. With the support of its Gateway private partners, INTERPOL was able to facilitate the identification and takeover of the attacker's command and control server, and supported the post-event disruption activities on criminal infrastructure led by Ireland.

This **paragraph** also allows States Parties to benefit from **INTERPOL's WHOIS Portal**, which will enable vetted law enforcement entities to access non-public domain registration data. For many years, the general public could access the registration data through a simple query to the Internet Corporation for Assigned Names and Numbers (ICANN). However, following the EU General Data Protection Regulation's entry into force in May 2018, domain registration data is no longer publically available through WHOIS. Law enforcement officials must now make individual requests to obtain this data. To facilitate the global law enforcement community's access to WHOIS data for lawful purposes, INTERPOL initiated the WHOIS Project in September 2018 to create the INTERPOL Registration Portal, through which accredited law enforcement officials from INTERPOL member countries can access domain registration information.

Further, INTERPOL, with its institutional legitimacy, policing infrastructure, and 195-member country network, is seeking to develop a global system that enables law enforcement officers to certify their identity to non-police actors – such as Internet security providers – through dedicated INTERPOL portals. INTERPOL also aims to ensure that the access to digital frontline policing tools is secure and restricted to law enforcement authorities only, to facilitate their investigations.