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 third formal session of the Ad Hoc Committee

May 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 third formal session of the AHC or suggested provisions for the Convention. It also serves as INTERPOL's input for the second Intersessional consultation with multi-stakeholders scheduled between the second and third 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 Paper 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.

With reference to document A/AC.291/L.4/Add.4, INTERPOL's proposals are summarized below:

1. *Chapter 4. International cooperation*
    a) **Articles related to "Extradition":**
        i. Role of INTERPOL Red Notices in the transmission of requests for provisional arrest of fugitives pending extradition
        ii. Role of INTERPOL in the transmission of requests for extradition
    b) **Article related to "Mutual legal assistance"** – Role of INTERPOL in the transmission of requests for mutual legal assistance
    c) **Article related to "24/7 Cooperation"** – INTERPOL 24/7 Contact Points on Computer-related Crime

2. *Chapter 5. Technical assistance, including exchange of experience*
    a) **Article related to "Technical assistance"** – Role of INTERPOL in providing technical assistance and capabilities development as global law enforcement organization
    b) **Article related to "Collection, exchange and analysis of information"** – Role of INTERPOL in crime analysis
3. *Chapter 6. Preventive measures*
    a) **Article related to "Prevention" –** Role of INTERPOL in the exchange of information for the prevention of the offences set forth in the Convention

1. INTERPOL's proposals for Chapter 4. International Cooperation

1a(i). Article related to "Extradition" – Role of INTERPOL Red Notices in the transmission of requests for provisional arrest of fugitives pending extradition

- […] Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings. In case of urgency, the requesting State may transmit its request for the provisional arrest of the person through the International Criminal Police Organization-INTERPOL.

*(**References:** Art. 6(8) UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Art. 16(9) UN Convention against Transnational Organized Crime, Art. 44(10) UN Convention against Corruption; supplemented by Art. 9 "Provisional arrest" of the UN Model Treaty on Extradition adopted by UN General Assembly Resolutions A/RES/45/116 and A/RES/52/88; UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018) and A/RES/71/19 (2016))*

COMMENTARY

➢ ***Aim:** To strengthen provisional arrest mechanisms*

This first **article** on "Extradition" highlights the role of INTERPOL in the transmission of requests relating to the provisional arrest of fugitives. The extradition request itself is often preceded by a request for the provisional arrest of the person sought to prevent that person from taking advantage of the length of the extradition process to evade justice. Provisional arrest is a detention measure applied on a temporary basis, through the application of an extradition treaty and/or national legislation, prior to the submission of an extradition request. This is what is known as the pre-extradition procedure.

As a neutral interlocutor for its 195 member countries, INTERPOL is a communications hub regarding internationally-wanted fugitives. The international search for fugitives through INTERPOL's communication network plays a crucial role at the pre-extradition stage. Requests for provisional arrest may be sent through INTERPOL to one, several or all INTERPOL member countries.

The requests may be transmitted in two ways: either directly to one or several National Central Bureaus (NCB) through the I-24/7 network (through a diffusion or a message), or through a "red notice" issued by the General Secretariat of INTERPOL, at the request of the NCB of the requesting State, acting on the request of the judicial authority.

INTERPOL Red Notices are recognized by some member countries as having legal value to serve as a basis for provisional arrest with a view to extradition. Each member country decides the legal value it attaches to a Red Notice and the authority of their law enforcement officers to make arrests. Every Red Notice request is vetted by a specialized task force to ensure its compliance with INTERPOL's Constitution and Rules. Red Notices may be published only if the offence concerned is a serious ordinary-law crime.

IN THE FIELD

A Belgian national was convicted in 2016 in absentia by a Belgian court to 19 years in prison for distributing child sexual abuse materials online and for sexual abuse of minors. An INTERPOL Red Notice had been issued for the fugitive. He was subsequently arrested in Cambodia the same year and extradited back to Belgium to serve his sentence.

1a(ii). Article related to "Extradition" – Role of INTERPOL in the transmission of requests for extradition

- […] States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition. For that purpose, such agreements or arrangements shall consider transmitting requests for extradition and any communication related thereto through diplomatic channels directly between the ministries of justice or any other authorities designated by the Parties and, where the States Parties agree, through the International Criminal Police Organization-INTERPOL, if possible.

*(**References**: Art. 6(11), 7(8) UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, Art. 16(17), 18(13) UN Convention against Transnational Organized Crime, Art. 44(18), 46(13) UN Convention against Corruption; supplemented by Art. 5 "Channels of communication and required documents" of the UN Model Treaty on Extradition adopted by UN General Assembly Resolutions A/RES/45/116 and A/RES/52/8; and INTERPOL General Assembly Resolutions AG-2013-RES-09 and AG-2014-RES-20 on the INTERPOL e-Extradition Initiative).*

COMMENTARY

- ***Aim:** To enhance extradition processes and make them fit to today's digitalized societies.*

This second **article** on "Extradition" reaffirms the need for enhanced extradition processes. As such, for the implementation of the future Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes, States Parties are encouraged to make use of INTERPOL's secure communication channels in order to exchange real time information regarding extradition processes, but also to send their requests for extradition.

While criminals use the internet, messaging services and electronic encryption to carry out their transnational illicit activities, the sending of extradition materials often still follows a path of the pre-digital era which can lead to challenges such as long processing times due to the requirement to send and receive physical documents. At the same time, INTERPOL provides for one of the world's most reliable secure communication networks connecting 195 member countries in real time. The potential of the network is such that competent authorities could use it to formally certify the documents, place electronic seals and create a complete chain of electronic custody from the requesting to the requested country.

This article mirrors the rationale for **INTERPOL's e-Extradition Initiative**, which is outlined in Resolution AG-2013-RES-09 approved by the INTERPOL General Assembly. The e-Extradition initiative aims to provide INTERPOL member countries with the opportunity to transmit extradition requests in an electronic format via a state-of-the-art communications tool and with due respect for current legislative and institutional norms. With further financial support, the INTERPOL's e-Extradition initiative will be ready to be implemented.

1b. Article related to "Mutual legal assistance" – Role of INTERPOL in the transmission of requests for mutual legal assistance

- […] Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, where the States Parties agree, through the International Criminal Police Organization-INTERPOL, if possible.

*(**References**: Art. 7(8) UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Art. 18(13) UN Convention against Transnational Organized Crime, Art. 46(13) UN Convention against Corruption)*

COMMENTARY

➢ ***Aim:** To enable the secure electronic transmission of MLA exchanges.*

This **article** on "Mutual legal assistance" uses language from UNCAC (Art. 46, par 13) and UNTOC (Art. 18 par 13). These conventions both recognize the role of INTERPOL as a possible channel for mutual legal assistance requests.

With cybercrime on the rise, transnational investigations are more and more frequent, and require increased and timely cooperation between law enforcement and judicial authorities from different jurisdictions. Yet, the traditional MLA process is long and resource intensive. This is especially the case with cybercrime where evidence needs to be secured in a timely fashion before it is no longer available.

INTERPOL's secure communication network I-24/7 is an effective tool at the disposal of all 195 member countries allowing the **real-time and secure transmission** of Mutual Legal Assistance (MLA) requests. Yet, I-24/7 was not designed for the specifics of Mutual Legal Assistance as electronic MLA requests are frequently considered as advance copies of the formal documents demanded in hard copy and sent through traditional means.

In order to speed up and streamline the transmission process of official requests for MLA and bridge the gap between the current means of communication, INTERPOL has designed the **"e-MLA Initiative"** (electronic transmission of MLA exchanges). **The INTERPOL e-MLA** Initiative has been designed to allow for the swift, secure, and streamlined electronic transfer of requests for mutual legal assistance in criminal matters between INTERPOL member countries with due respect for current legislative and institutional norms.

The initiative was endorsed by the INTERPOL General Assembly through Resolution GA-2018-87-RES-04. With further financial support, the INTERPOL's e-MLA initiative will be ready to be implemented.

1c. Article related to "24/7 Cooperation" – INTERPOL 24/7 Contact Points on Computer-related Crime

- States Parties shall make full use of and strengthen existing networks of points of contact, including the 24/7 Contact Points for Computer-related Crime of the International Criminal Police Organization-INTERPOL, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning the offences set forth in this Convention, or for the collection of electronic evidence of a criminal offence.

*(**References**: INTERPOL General Assembly Resolutions GA-2008-RES-07 and GA-2012-RES-08)*

COMMENTARY

➢ ***Aim:** To foster international cooperation and optimize the use of existing global mechanisms.*

This article reaffirms the need for effective international communication in the fight against the inherently transnational use of ICTs for criminal purposes, through INTERPOL's channels. This **article** is based on a final recommendation by the Intergovernmental Expert Group (IEG) on cybercrime as adopted at its 7th session (April 2021), which states that: "Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and INTERPOL channels for prompt police-to-police cooperation".

INTERPOL maintains a list of **24/7 Contact Points for Computer-related Crime** to ensure that the information exchanged through the appropriate INTERPOL channels reaches the national cybercrime units with the least possible delay. These Contact Points are also essential for coordinating global law enforcement responses to large-scale major cyber incidents. By having direct contacts with the responsible cybercrime units, information can be acted on quickly. This is also complemented by INTERPOL's secure communication network where information can subsequently can be exchanged and INTERPOL is also able to connect with and utilize its network of private partners. Because the INTERPOL's 24/7 Contact Points for Computer-related Crime is a list that includes INTERPOL's 195 member countries, this can ensure that gaps are bridged with other 24/7 networks of contact points that have a more limited membership. INTERPOL's 24/7 Contact Points for Computer-related Crime thus complements other networks or bilateral means of communications.

2. INTERPOL's proposals for Chapter 5. Technical assistance, including exchange of experience

2a. Article related to "Technical assistance" – Role of INTERPOL in providing technical assistance and capabilities development as global law enforcement organization

- […] Countries shall strengthen, to the extent necessary, efforts to maximize operational and training activities for law enforcement within international and regional organizations, including the International Criminal Police Organization-INTERPOL, and within other relevant bilateral and multilateral agreements or arrangements.

*(**References**: Art. 29(4) UN Convention against Transnational Organized Crime, UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018) and A/RES/71/19 (2016), INTERPOL General Assembly Resolutions GA-2021-89-RES-11)*

COMMENTARY

- ***Aim:** To enhance the provision of technical assistance and other capabilities development support to beneficiary countries*

The **article** on "Technical assistance" reflects similar articles in other UN instruments such as UNTOC, covering training and technical assistance especially concerning law enforcement personnel. INTERPOL plays an important role in supporting law enforcement through its training and capacity-building programmes which seek to enhance national cyber skills, knowledge and technical capabilities – in line with INTERPOL standards.

States Parties can also map their capacity-building efforts at the national, regional and global levels to counter cybercrime made in collaboration with international organizations such as INTERPOL. Having a coherent big picture can help to avoid duplication and create synergies in the best interests of practitioners and stakeholders.

IN THE FIELD

INTERPOL currently has several capacity-building and training projects. These include the Cyber Capabilities & Capacity Development Project (**C3DP**) funded by United States Department of State, Global Action on Cybercrime Extended Project (**GLACY+**) funded by Council of Europe, and INTERPOL Support Programme for the African Union in relation to AFRIPOL (**ISPA**) funded by German Federal Foreign Office.

Aside from conducting regular trainings and online courses, INTERPOL developed guidebooks and toolkits to help member countries build long-term capabilities. For instance, the C3DP Project published a *National Cybercrime Strategy Guidebook* to support member countries in developing or updating their national Cybercrime Strategies. The GLACY+ project also developed the *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* to assist member countries in developing cybercrime statistics and measuring the impact of cybercrime. INTERPOL also focuses on the management of digital forensic and electronic evidence (see *Guidelines for Digital Forensics First Responders*, and *Global Guidelines for Digital Forensics Laboratories*).

2b. Article related to "Collection, exchange and analysis of information" – Role of INTERPOL in crime analysis

- […] States Parties shall consider developing and sharing with each other and through international and regional organizations, statistics, information and analytical expertise concerning the use of information and communications technologies for criminal purposes with a view to developing, insofar as possible, potential criminal modi operandi, guidelines to assist law enforcement agencies in their investigations and cooperation with the private sector as well as information on best practices for the prevention and investigation of the offences set forth in this Convention. For that purpose, States Parties may exchange information and share international alerts through the International Criminal Police Organization-INTERPOL.

(***References**: Art. 28 UN Convention against Transnational Organized Crime, Art. 18 International Convention for the Suppression of the Financing of Terrorism, Art. 61 UN Convention against Corruption, UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018) and A/RES/71/19 (2016), INTERPOL General Assembly Resolutions GA-2021-89-RES-11)*

COMMENTARY

- ***Aim:** To enhance exchange of information, analysis and knowledge about the nature of cybercrime*

The **article** entitled "Collection, exchange and analysis of information" stresses the importance of States proactively engaging in the exchange of information, knowledge and best practices regarding the use of ICTs for criminal purposes, supported by the UN General Assembly resolutions which provide the framework for the cooperation between the United Nations and INTERPOL[1].

INTERPOL conducts strategic intelligence analysis of specific crime threats and trends, and develops global and regional assessments on cybercrime. These assessments are produced based on member country surveys and data from private partners. They help prioritize and devise strategic and operational measures in anticipation of the development of threat landscapes and crime trends.

INTERPOL has also developed tools designed to enhance INTERPOL's cybercrime analytical capabilities. In addition to this, INTERPOL offers its member countries a Cybercrime Knowledge Exchange platform for exchange of knowledge and best practice. In 2020, INTERPOL published together with the Council of Europe and the EU a *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* to enhance countries' understanding of the scale, types and impact of crime in cyberspace.

IN THE FIELD

To enable a better understanding of the regional dimension of cybercrime, INTERPOL has published regional cybercrime threat assessments for the ASEAN region and for Africa respectively. The assessments profile the most prominent cyber threats for the regions. INTERPOL also produces Cyber Activity Reports on more specific aspects of cyber threat actors that are shared with member countries.

In 2020, INTERPOL published the COVID-19 Cybercrime Analysis Report that assessed the effect of the global pandemic on the cybercrime threat landscape.

3. INTERPOL's proposals for Chapter 6. Preventive measures

3a. Article related to "Prevention" – Role of INTERPOL in the exchange of information for the prevention of the offences set forth in the Convention

- States Parties shall cooperate in the prevention of the offences set forth in this Convention by exchanging accurate and verified information in accordance with their domestic law, and where the States Parties agree, conduct such exchanges through the International Criminal Police Organization-INTERPOL.

[1] *UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018) and A/RES/71/19 (2016)*

(***References:*** *Art. 18 International Convention for the Suppression of the Financing of Terrorism, UN General Assembly Resolutions A/RES/75/10 (2020), A/RES/73/11 (2018) and A/RES/71/19 (2016), INTERPOL General Assembly Resolution GA-2021-89-RES-11)*

COMMENTARY

- ***Aim:*** *To maximize prevention efforts for proactive disruption of cyber threats and their ecosystem.*

The **article** related to "Prevention" reasserts the need for proactive and pre-emptive action against cybercrime, such as raising awareness and sharing knowledge about the threats and dangers present on the cyberspace.

To this end, the modi operandi of contemporary cybercriminals should be carefully studied through intelligence analysis and criminological research, especially with the use of INTERPOL's analytical capabilities. INTERPOL produces regional and global threat assessment reports on cybercrime. This allows identification of vulnerabilities, prioritization and deployment existing resources more effectively.

Information on cybercriminal groups can be shared among member countries through INTERPOL Notices, particularly through:

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

The prevention of cybercrime requires the cooperation of a wide variety of stakeholders. In line with the *United Nations Guidelines for the Prevention of Crime* that highlights the importance of public education and awareness, INTERPOL focuses on cybercrime prevention by raising public awareness through a series of global awareness campaigns in collaboration with public and private partners. Another example is INTERPOL's partnership with the World Economic Forum to build the Partnership Against Cybercrime alliance, which gathers law enforcement, private sector and civil society organizations.

IN THE FIELD

In March 2022, INTERPOL issued a Purple Notice on the Conti Ransomware deployment against critical infrastructure and organizations globally, in collaboration with the Irish police An Garda Síochána. The criminal activities and modi operandi outlined in the Purple Notice served as an alert for all member countries to deploy necessary mitigation and prevention techniques in order to safeguard their critical infrastructure.

Every year, INTERPOL also conducts a global awareness campaign to highlight to the general public the different aspects of cybercrime threat. The campaign in 2021, named #JustOneClick, was supported by over 80 member countries and reached more than four million people online. It provided cyber hygiene advice to ensure that individuals and businesses are equipped with the knowledge of how to protect their systems and data.