INTERNATIONAL CRIMINAL POLICE ORGANIZATION
ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL
ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE
المنظمة الدولية للشرطة الجنائية

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

Proposal related to the Consolidated Negotiation Document and the chapters to be examined at the fifth formal session of the Ad Hoc Committee

February 2023

Introduction

As discussions continue to evolve around 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 provide its recommendations on some of the chapters of the Consolidated Negotiating Document (CND) to be discussed at the fifth formal session of the AHC.

These recommendations highlight how existing international cooperation mechanisms can support Member States in implementing the commitments and obligations arising from this new Convention – noting that a text which is reflective of the realities of global law enforcement cooperation is more likely to be successfully operationalized.

These recommendations are in line with 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, and subsequent contributions to the formal sessions and intersessional consultations. This document may serve as reference for member countries in formulating their contributions and negotiations around the fifth session of the AHC.

With reference to the CND, as per A/AC.291/19, INTERPOL's recommendations in this submission focus on the following two chapters:

- **Chapter IV International cooperation**
  - Cluster 2
    - Art 58 (10) and (20) **Extradition**
  - Cluster 4
    - Art 61 (12) General principles and **procedures relating to mutual legal assistance**
    - Art 64 (1) **Spontaneous information**
    - Art 66 (8) **Emergency mutual legal assistance**
    - Art 67 (6) and (1) **24/7 Networks**
  - Cluster 6
    - Art 75 (2) **Law Enforcement cooperation**

- **Chapter V Technical assistance, including information exchange**
  - Art 87 (9) **Training and technical assistance**
  - Art 88 (2) **Exchange of information**

1. INTERPOL's proposals for Chapter IV on International Cooperation

INTERPOL welcomes the inclusion of a chapter on international cooperation and the strong congruence between INTERPOL's strategy against cybercrime and this chapter's General Principles [**Art 56(1) CND**]. Indeed, enhanced international cooperation on criminal matters is at the core of INTERPOL's mission to prevent, detect, investigate, and disrupt cybercrime. In that regard, it is suggested to consider a broader reference to the use of INTERPOL's policing capabilities and the possible use of INTERPOL's channels for additional purposes beyond the exchange of emergency MLA requests.

In this context, INTERPOL would like to make the following proposals on provisions in Clusters 2, 4, and 6 of Chapter IV:

a) Cluster 2: Provisions related to Extradition

i) Role of INTERPOL Red Notices in the transmission of request for provisional arrest of fugitives pending extradition.

Art 58 (10) CND

- […] 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))*

As proposed in previous submissions, INTERPOL suggests this additional language **to strengthen provisional arrest mechanisms in the future convention.**

This addition would reflect INTERPOL's role 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 undue delays that are the result of transmission via diplomatic channels. 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 intergovernmental organization with 195 member countries, INTERPOL provides an international mechanism for its member countries to locate and arrest internationally wanted individuals and fugitives. The international search for fugitives through INTERPOL's channels plays a crucial role at

the pre-extradition stage. Requests for location and arrest of wanted individuals may be sent through INTERPOL's communication network 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. Every Red Notice request is vetted by a specialized task force to ensure its compliance with INTERPOL's Constitution, Rules and legal framework. Red Notices may be published only if the offence concerned is a serious ordinary-law crime.

Other types of INTERPOL Notices can also prove highly relevant in the fights against cybercrime. For instance, the "Blue Notice" provides relevant, investigation-specific information, such as location or identity details, and can be used in parallel to MLA requests, or for information sharing in lieu of such request, depending on the national laws of the requesting and requested state. Further, if countries wish to alert other countries about cybercriminal activity, they can do so via the "Green Notice", the "Orange Notice" (for imminent threats) or "Purple Notice" (for modus operandi).

***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.

ii) Role of INTERPOL in the transmission of requests for extradition

Art 58 (20) CND

- […] 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 may include transmission of 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, whenever possible, through the International Criminal Police Organization-INTERPOL.*

*(**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 AG2014-RES-20 on the INTERPOL e-Extradition Initiative).*

As proposed in previous submissions, INTERPOL suggests this additional language **to enhance extradition processes and make them fit for today's digitalized societies.**

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.

b) Cluster 4: Articles related to Mutual Legal Assistance (MLA)

i) Spontaneous information: use of existing Police-to-police cooperation channels

In the Conclusions and recommendations agreed upon by the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (6-8 April 2021), the Expert Group made the following recommendation[1]:

> *"23. 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, as well as networking with strategically aligned partners, with a view to sharing data on cybercrime matters and enabling rapid responses and minimizing loss of critical evidence. The use of police-to-police cooperation and **other methods of informal cooperation** before using mutual legal assistance channels was also recommended;" (emphasis not in original)*

Relatedly, in **Art 64 CND** on "Spontaneous Information" reference is made to information sharing. INTERPOL is entrusted by its 195 member countries as one of the main channels for these types of communications where police-to-police cooperation plays a key role for investigative and intelligence purposes. Accordingly, INTERPOL recommends the addition of the following language to **Art 64 (3) CND**:

Art 64 (3) CND

- […] The transmission of information pursuant to this article shall be without prejudice to inquiries and criminal proceedings in the State Party providing the information**.** *A State Party may transmit spontaneous information to the relevant competent authorities of another State Party, either directly or through the 24/7 network established in accordance with article 67 of this Convention or through the channels of the International Criminal Police Organization.*

[1] https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf

ii) Role of INTERPOL in the transmission of MLA requests

INTERPOL welcomes the direct reference made to its channels in **Art 66 (8) CND** concerning emergency mutual legal assistance in line with UNTOC (Art 18(13)) and UNCAC (Art 46(13)).

Art 66 (8) CND

- In the event of an emergency, requests may be made directly by the competent authorities of the requesting State Party to the relevant competent authorities of the requested State Party or through the 24/7 network established in accordance with article 67 of this Convention, or **channels of the International Criminal Police Organization […].**

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 MLA requests. In fact, member countries have already been utilizing INTERPOL channels to send MLA requests, **also in non-emergency scenarios.** This is especially the case in the absence of an MLA treaty or other pre-existing bilateral channels between States Parties.

***IN THE FIELD*:** In 2022, two Red Notice fugitives wanted by Korea for suspected involvement in a global Ponzi scheme were arrested in Greece and Italy after embezzling EUR 28 million from 2,000 Korean victims. The arrests followed coordination between INTERPOL and the National Central Bureaus (NCBs) in Greece, Italy, Poland and the Republic of Korea. The Polish suspect was arrested following real time information exchange between the NCB in Rome, Italy's Guardia di Finanza Investigation unit and INTERPOL. Police at Athens International Airport arrested the German suspect as he attempted to travel to Dubai after an identity check detected his Red Notice status.

Accordingly, **to facilitate the secure, real-time transmission of urgent and non-urgent MLA requests, INTERPOL would suggest referencing its channels in Art 61 (12) CND,** which encourages Member States to make MLA requests in electronic form if possible.

Art 61 (12) CND

- […] Where not prohibited by their respective laws, States Parties are encouraged to direct central authorities to transmit and receive requests for mutual legal assistance, and communications related thereto, in electronic form. Where acceptable to the central authorities of both States Parties involved, central authorities are also encouraged to transmit and receive electronic evidence. *States Parties are encouraged whenever possible to transmit such requests or evidence through the International Criminal Police Organization – INTERPOL.*

iii) INTERPOL 24/7 Contact Points for computer-related crime

INTERPOL also welcomes the direct reference to its channels in **Art 67 (6) CND** concerning 24/7 networks, made with regard to INTERPOL's submission to the third formal session of the AHC. INTERPOL recommends a slight rephrasing of the language currently proposed in the CND:

Art 67 (6) CND

- […] States Parties shall make full use of and strengthen existing authorized networks and points of contact, where applicable, and within the limits of their domestic laws, *including the existing network of the International Criminal Police Organization and including the 24/7 points of contact for computer-related crime.*

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

This article reaffirms the need to **foster international cooperation and optimize the use of existing global mechanisms** and is based on the final recommendation of the Intergovernmental Expert Group (IEG) on cybercrime as adopted at its 7th session (April 2021).

INTERPOL maintains an active secure law enforcement communications network for the prevention, detection and suppression of ordinary law crime, that includes 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 be exchanged and INTERPOL is also able to connect with and utilize its network of private partners.

INTERPOL's secure communications platform for its 195 Member Countries includes 24/7 Contact Points for Computer-related Crime which can ensure that gaps are bridged with other 24/7 networks of contact points that have a more limited membership. INTERPOL's I-24/7 network and its 24/7 Contact Points for Computer-related Crime thus complements other networks or bilateral means of communications.2

Given the established nature of existing networks, their complementarity and maturity, it is important that the Convention does not inadvertently create silos and fragmentation by duplicating existing mechanisms and communications networks. Harmonizing output with a view to creating a common set of principles and standards will allow practitioners to meaningfully utilize the Convention, leading to its successful operationalization.

INTERPOL therefore suggests referencing existing channels in Art **67 (1) CND:**

Art 67 (1) CND

- Each State Party shall designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate assistance for the purpose of investigations, prosecutions or other

proceedings concerning criminal offences established in accordance with this Convention, or for the collection, obtaining, preservation and sharing of evidence in electronic form of [offences set forth in this Convention] [any criminal offence] [serious crimes], *taking into account existing channels, such as those made available by INTERPOL.* Such assistance shall be provided without undue delay and in a secure manner.

c) Cluster 6: Articles related to Law Enforcement Cooperation

Art 75 (2) CND

- With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the Parties may consider this Convention as the basis for law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, *in particular INTERPOL's channels*, to enhance the cooperation between their law enforcement agencies. *States Parties may exchange information through the International Criminal Police Organization – INTERPOL.*

Law enforcement cooperation is the very bedrock of INTERPOL's mandate and, as mentioned above, INTERPOL holds tools and channels available to its 195 member countries to facilitate and foster such cooperation. Indeed, the Convention will not operate in a vacuum and it is crucial that it makes use of existing active law enforcement cooperation networks. INTERPOL remains the only global law enforcement organization with a dedicated secure communications platform, its constitutional neutrality and apolitical status allow it to play a unique role in international law enforcement cooperation.

In addition to its dedicated secure communication system I-24/7, INTERPOL connects law enforcement globally through its newly developed platforms, such as the Cybercrime Knowledge Exchange (CKE) for non-operational exchanges of information on cybercrime and the Cybercrime Collaborative Platform – Operation (CCP - Operation) for restricted and secure operational exchange of intelligence. Furthermore, each INTERPOL National Central Bureau has access to other systems and networks, including the data they contain; over 125 million records of criminals, stolen property, threats, weapons, etc. across 19 criminal databases and beyond. Any authorized national agency may be granted access to these data by its INTERPOL National Central Bureau.

INTERPOL's channels are regularly used by member countries to exchange information related to investigations. A general reference to the use of INTERPOL's channels to facilitate communication in the prevention and investigation of cybercrime may therefore be useful for States.

2. INTERPOL's proposals for Chapter V on Technical Assistance, including Information Exchange

a) Articles on Technical Assistance

Art 87 (9) CND

- […] States Parties shall entrust the United Nations Office on Drugs and Crime with the task of coordinating and providing specialized technical assistance to States Parties, upon request, in collaboration with other international and regional organizations, as appropriate, with a view to promoting the implementation of programmes and projects to prevent and combat offences covered by this Convention.

INTERPOL provides its 195 member countries with tools, channels, platforms and operational capabilities with a view to **enhance the provision of technical assistance and other capabilities development support to beneficiary countries.**

Technical assistance can be both part of the specialized support given when developing capabilities and increasing capacities of police services, but also the more direct support given in operational matters. INTERPOL offers such technical assistance and support to member countries through, among others, our Digital Forensic Lab and the coordination of joint investigations by member countries as part of INTERPOL's regional operations desk model. Recently at the request of our member countries, INTERPOL provided such capabilities development and technical assistance in a Cyber Surge event with AFRIPOL and African partner countries, which has led to several successful operational outcomes, in particular the arrest of 11 individuals, with one suspect linked to the abuse of children, and 10 others linked to scam and fraud activities worth USD 800,000 which had an impact on victims globally.

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 stakeholder.

b) Articles on Information Exchange

Art 88 (2) CND

- […] The States Parties shall consider developing and sharing with each other and through international and regional organizations statistics, analytical expertise and information concerning [cybercrime] [the use of information and communications technologies for criminal purposes], with a view to developing, insofar as possible, common definitions, standards and methodologies, including best practices to prevent and combat such offences. *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)

As proposed in previous submission, INTERPOL suggests this reference in order **to enhance exchange of information, analysis and knowledge about the nature of cybercrime.**

Art 88 (2) CND 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.

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.