INTERPOL

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

Proposals related to the Consolidated Negotiating Document and the chapters to be examined at the fourth formal session of the Ad Hoc Committee

December 2022

Introduction

As discussions 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 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 countries in formulating their contributions and negotiations around the fourth formal session of the AHC. These reflections are based on 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. With its member countries, INTERPOL continues its ongoing efforts to align global strategies against cybercrime to provide a unified answer to the misuse of Information and Communications Technologies (ICT) for criminal purposes.

The previous contributions detail the strategic priorities which, in INTERPOL's view, are essential for this new international legal instrument to become an effective and practical tool to combat and counter cybercrime. INTERPOL welcomes the strong congruence between INTERPOL's strategy and global programme against cybercrime juxtaposed with the consolidated negotiating document of the Convention. INTERPOL submits three general comments for consideration by Member States, specifically with a focus on Chapter 3 of the proposed structure of the Convention entitled "Procedural Measures and Law Enforcement", which is relevant to the mandate of the Organization:

> **1. Fostering cooperation and information exchange between national agencies and law enforcement within State parties is critical, in particular if the Convention is to cover a wide range of cybercrimes.**

2. The Convention presents a unique opportunity to enhance and strengthen cooperation between law enforcement and the private sector to the mutual benefit of both parties.

3. State parties would gain to build on and maximize the use of existing, trusted and proven mechanisms developed and used at the operational level by law enforcement.

1. Fostering cooperation and information exchange between national agencies and law enforcement within State parties is critical, in particular if the Convention is to cover a wide range of cybercrimes.

In the context of cybercrimes, different national law enforcement agencies and other entities like the National Computer Emergency Response Team-CERTs possess different information relevant for the same investigation. For instance, in case of frauds enabled via computer systems, the national Financial Intelligence Unit (FIU) may find it necessary to cooperate closely with the National Cybercrime Unit. Both may need to access data that sits with the country's INTERPOL National Central Bureau (NCB) which serves as the liaison point between INTERPOL and various departments and agencies in the country.

Therefore, a key element in Chapter 3 "Procedural Measures and Law Enforcement" is the need to foster relationships and information exchange between national agencies. The Convention would benefit to stress the internal challenges and offer responses to foster inter-agency cooperation within State parties.

Additionally, many countries have legal and/or regulatory frameworks in place imposing the duty for cyber infrastructure owners to report cyber incidents to national CERTs or cybersecurity agencies, especially if critical information infrastructures are affected. In contrast, under-reporting of cybercrime to law enforcement is a perennial issue. Therefore, cooperation and information exchange between law enforcement and these national entities is critical in order to have a comprehensive appreciation of both the incident and threat, and to facilitate robust responses inclusive of remediation and attribution.

In this regard, Member States may elect to consider the following additional article –under Chapter 3, Cluster 2:

> ***"State parties shall, in particular, take effective measures 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 offenses covered by this Convention".***

In order to foster intra-national cooperation, INTERPOL would see value in having its channels explicitly mentioned. INTERPOL connects its 195 member countries through dedicated secure communication system I-24/7, the only global communication system for law enforcement along with newly developed global platforms that INTERPOL uses to connect law enforcement like 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 national INTERPOL 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. For instance, the global communication system I-24/7 grants access to INTERPOL's criminal databases such as the INTERPOL International Child Sexual Exploitation database (ICSE), which holds over 4.3 million images and videos and has helped identify more than 30,000 young victims of abuse worldwide. As such, ICSE is a key tool for national specialized units investigating cases dealing with online child sexual abuse.

The INTERPOL General Secretariat encourages and supports the expanded access to its criminal data to facilitate cooperation between different national agencies. As highlighted in the 2008 INTERPOL General Assembly resolution GA-2008-RES-07 and reaffirmed many times since then including in the 2021 INTERPOL General Assembly resolution GA-2021-89-RES-11, INTERPOL's General Assembly agrees to-

> *"INVITES all [195] member countries, through their National Central Bureaus, in conformity with the Rules on the processing of information for the purposes of international police co- operation, to extend access to the I-24/7 communications system to their national cybercrime units."*

The UN General Assembly has also called member countries on expanding access to INTERPOL's systems and data to all relevant national agencies. In particular, since 2016, the UNGA resolution on the cooperation between the United Nations and INTERPOL:

> "*acknowledges the importance of extending real-time access to the I-24/7 global police secure communications system from the national central bureaux of Member States that are also member countries of INTERPOL to their other national law enforcement entities at strategic locations*". The latest such resolution was adopted in 2022 under reference A/RES/77/20.

The above proposed paragraph (page 2) would therefore help foster cooperation between relevant agencies/entities within State parties, which is critical to tackle a wide range of cybercrime offences. Moreover, the same proposed paragraph would encourage State parties and their national INTERPOL National Central Bureaus to empower all relevant national agencies with access to critical data that INTERPOL holds available to any authorized user.

2. The cooperation between law enforcement and the private sector shall be enhanced and strengthened in a holistic way to the mutual benefit of both parties.

The Convention presents a unique opportunity to enhance and strengthen the cooperation and the exchange of information between law enforcement and the private sector in a holistic way.

The relationship between law enforcement and the private sector shall indeed go beyond *Article 46. Search and seizure of [information stored or processed electronically] [stored computer data]*, *Article 47. Real-time collection of traffic data,* and *Article 48. Interception of content data*.

In this regard, Member States may elect to consider the following additional article or paragraph under Chapter 3, Cluster 2:

> ***"States Parties shall take such measures as may be necessary to encourage and facilitate, in accordance with their domestic laws, 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".***

In 2019, INTERPOL General Assembly recognized the importance of its partnership with the private sector by endorsing a legal framework entitled "Gateway", which enables INTERPOL to exchange information with which it has signed data sharing agreements (see resolution GA-2019-88-RES-11). INTERPOL works with a wide range of private-sector companies where majority of data and expertise lies in relation to cybercrime and can combine their knowledge and information with that of law enforcements' to produce various actionable cyber intelligence products for Member States.

INTERPOL can build on its experience to establish solid, trustful, and long-term cooperation/partnerships with the private sector to receive and analyze a wide range of data including but not limited to imminent threats, long term trends, critical intelligence on criminal actors and groups, and modus operandi. All member countries are therefore equipped to carry out follow-up preventive action, investigations or disruptions such as arrests, searches, and seizures.

INTERPOL is well placed to act as an interlocutor between law enforcement and the private sector, enabling crucial information flow. For instance, in May 2021, the Irish Heath Service Executive was impacted 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 private-sector 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.

3. State parties would gain to build on and maximize the use of existing, trusted and proven mechanisms developed at the operational level by law enforcement.

The Convention will not operate in a vacuum. Beyond the existing legal instruments, there are also effective and trusted mechanisms that were already put in place by and for law enforcement to address the criminal use of ICTs. These mechanisms will support the operationalization of the Convention; and their further use in this frame would help maximize the significant resources already channeled into them by INTERPOL's 195 member countries.

INTERPOL has identified two articles in which its existing mandate and channels would gain to be explicitly referenced. In doing so, the Convention would help generate a unified approach for the international

community to address cybercrime more effectively, which combines political commitments, legal obligations and operational reality.

Chapter 3, cluster 1**,** *Article 42. Jurisdiction* may further recognize the need for cross border cooperation and highlight the mandate given to INTERPOL by its Member States in cross-border coordination and support.

Chapter 3, cluster 2, *Article 45. Production of orders* could reflect the reality of existing action taken by countries and highlights their success with the sharing of orders. In some countries, INTERPOL is the only authorized channel for foreign law enforcement agencies to get e-evidence from national Service Providers, eg. Indonesia, Kenya, and to some extend Russia[1].

Referring to INTERPOL could help emulate similar positive developments in countries which do not yet have a mechanism in place and indicate that they can take advantage of the existing and proven INTERPOL mechanisms which are already at their disposal nationally. An additional paragraph under *Article 45* could include:

> ***"Member States are given the possibility to send these orders as per their domestic law, including through INTERPOL's secure channels".***

When using agreed language from previous international legal frameworks, INTERPOL would recommend modifying and updating it in line with its real-world applicability and new developments made over the past decades. For instance, the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC) were established before the INTERPOL I-24/7 communication system, the databases, and other tools were operationalized. INTERPOL's channels are not reflected in these conventions beyond the sharing of mutual legal assistance (MLA) requests. However, the role of INTERPOL today is a lot more extensive and integral to the global fight against cybercrime.

Conclusion

The ongoing elaboration process provides a unique opportunity to align the legal, policy, and operational levels in order for the international community to address the criminal use of ICTs more effectively. The Convention would increase its operational impact if designed – and implemented by relying on existing, proven and trusted international cooperation mechanisms in use by law enforcement, including those that INTERPOL makes available in its 195 member countries.

As such, INTERPOL holds available all its tools and services to operationalize the Convention, and also conducts an active reflection on the new tools and means that the Organization could develop with a view to assisting the States parties to translate their commitments into concrete actions to counter the criminal use of ICTs.

[1] Source: UNODC/CTED/IAP "Practical guide for requesting electronic evidence across borders"