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

Proposal related to the Draft Text of the Convention and the chapters to be examined at the sixth formal session of the Ad Hoc Committee

August 2023

INTRODUCTION

The International Criminal Police Organization (INTERPOL) welcomes the opportunity to submit its proposals in advance of the Sixth Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

With reference to the draft text of the convention, as per A/AC.291/22, INTERPOL wishes to make six (6) substantial recommendations for Member States' consideration:

a) Enhance the use of existing channels for the transmission of requests for extradition, including those provided by INTERPOL (Chapter V, Article 37);
b) Recognize to the fullest extent the existing channels for the transmission of requests for mutual legal assistance, including those provided by INTERPOL (Chapter V, Article 40);
c) Make use of INTERPOL's existing 24/7 networks for computer-related crime (Chapter V, Article 41);
d) Enhance international cooperation and information exchange between law enforcement organizations, specifically through INTERPOL, in accordance with their obligations under domestic and international law (Chapter V, Article 47);
e) Maximize the role of international organizations in promoting and developing preventive measures (Chapter VI, Article 53);
f) Leverage to the best possible extent the necessary contributions of international organizations, including INTERPOL, in providing technical assistance and capacity-building (Chapter VII, Article 54).

INTERPOL'S PROPOSALS

a) Enhance the use of existing channels for the transmission of requests for extradition, including those provided by INTERPOL	CHAPTER V ARTICLE 37

Proposals for the draft text of the convention:

To strengthen provisional arrest mechanisms in the future Convention, INTERPOL suggests additional language in **Article 37 on Extradition, paragraph 10**, with a reference to INTERPOL's existing and widely used channels for the transmission of requests for extradition:

> 10. 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 the person's presence at extradition proceedings. **[INTERPOL'S PROPOSAL: In case of urgency, the requesting State may transmit such a request through the International Criminal Police Organization - INTERPOL.]**

Rationale:

This general recommendation was supported by several Member States during the Fifth Session of the AHC, to include a direct reference to INTERPOL within the former Consolidated Negotiating Document, Article 58 paragraph 10.

This language addition is aimed at strengthening custodial mechanisms in the future Convention, ensuring that the earlier stages of a request for extradition are also receiving proper attention. These include – but are not limited to – the search for fugitives leading to the transmission of requests for arrest for purpose of extradition.

As a neutral intergovernmental organization with 195 member countries, INTERPOL provides an international mechanism for its membership to locate and arrest internationally wanted individuals and fugitives. Such requests may be transmitted using INTERPOL's Policing Capabilities in two ways: either directly to one or several member countries through the **I-24/7 secure global police communication network**, or through **Red Notices** issued under the INTERPOL International Notices System at the request of the National Central Bureau (NCB) of the requesting State acting on the request of its 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. Moreover, every Notice is vetted by a specialized multidisciplinary task force and published only if it complies with INTERPOL's Constitution and Rules on the Processing of Data (RPD) to ensure the legality and quality of information, as well as the protection of personal data.

Member States are encouraged to make use of INTERPOL's secure communication channels to exchange real time information regarding the location of fugitives and extradition processes, by sending requests for provisional arrest or custody of the individual, with a view to extradition. Within this context, INTERPOL's formal recognition within the text of the Convention will enhance law enforcement's ability to locate perpetrators globally for offences concerning [the criminal use of ICTs] [cybercrime] through the utilization of an established, effective tool in fugitive investigative support.

b) Recognize to the fullest extent the existing channels for the transmission of requests for mutual legal assistance, including those provided by INTERPOL	**CHAPTER V ARTICLE 40**

Proposals for the draft text of the convention:

INTERPOL welcomes the reference to its channels under **Chapter V – International Cooperation, Article 40**: **"General principles and procedures relating to mutual legal assistance", in paragraph 12 (d).** INTERPOL suggests considering removing the words "*in urgent circumstances*" from **Article 40, in paragraph 12 (d):**

> (d) 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, ~~in urgent circumstances,~~ where the States Parties agree, through the International Criminal Police Organization, if possible.

Rationale:

INTERPOL is conscious that the language in Article 40, paragraph 12 (d), has been used in the past in important mechanisms[1] and acknowledges the importance of language consistency throughout official documents. Under current language, the use of INTERPOL channels would be governed by three specific conditions: "where the States Parties agree", "if possible" and "in urgent circumstances".

In line with its Written Contribution submitted for the AHC Fifth Session, INTERPOL would like to reiterate that:

i. INTERPOL's secure communication network I-24/7 allowing the real-time and secure transmission of MLA requests is and can be used in many different circumstances, including scenarios that would not necessarily classify as urgent;

ii. The expression "urgent circumstances" could be subject to contrasting interpretations. As there is no explicit definition of the expression in the text, "urgent circumstances" may be interpreted in terms of time-sensitive legal needs, situations of national or international crises and/or extreme cases, like an imminent threat to life. More importantly, the understanding of "urgent circumstances" may highly differ from State to State;

iii. The additional provision "in urgent circumstances" risks to restrict the use of INTERPOL channels for the transmission of MLA requests. This would particularly affect those States that do not have an MLA treaty or other pre-existing bilateral channels.

By removing "in urgent circumstances", the Convention would ensure that an important mechanism of cooperation on mutual legal assistance is recognized to the fullest extent, potentially empowering States with a significant tool to protect their communities.

IN THE FIELD: Use of INTERPOL channels to facilitate mutual legal assistance and extradition[2]

In 2022, two suspects were arrested in Greece and Italy for their alleged roles in a global Ponzi scheme. The suspects, a 49-year-old Polish national and a 61-year-old German national, were wanted

[1] UNCAC, Article 46, Paragraph 13.
UNTOC, Article 18, Paragraph 13.

[2] https://www.interpol.int/en/News-and-Events/News/2022/Ponzi-scheme-suspects-wanted-via-INTERPOL-arrested-in-Greece-and-Italy

internationally under INTERPOL Red Notices issued by Korean authorities for their suspected involvement in the scheme that embezzled approximately EUR 28 million from about 2,000 Korean victims. The arrests followed coordination between INTERPOL and the National Central Bureaus (NCBs) in Greece, Italy, Poland and 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. On the other hand, 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. **The extradition request from Korea to Greece and Italy was sent through INTERPOL channels provisionally and was followed by official communication through diplomatic channels under the EU-Korea Extradition Treaty**.

In addition, 4,778 BTC (about USD 109 million) in the cryptocurrency account of the Polish suspect was voluntarily restrained by its cryptocurrency exchange platform to prevent the laundering of criminal proceeds. The voluntary suspension of the suspect's account was backed by information provided by Korea through INTERPOL channels. The courts of Korea and Poland issued the freeze order against the suspect's account which was provisionally delivered through INTERPOL channels to the said cryptocurrency platform and its registered national jurisdiction, which was followed by official delivery of the order through diplomatic channels for mutual legal assistance.

c) Make use of INTERPOL's existing 24/7 networks for computer-related crime	**CHAPTER V ARTICLE 41**

Proposals for the draft text of the convention:

INTERPOL supports a reference to its existing 24/7 networks for computer-related crime, in **Article 41. 24/7 Network paragraph 6**:

> 6. States Parties may also use and strengthen existing authorized networks of points of contact, where applicable, and within the limits of their domestic laws, including *the 24/7 networks for computer-related crime of the International Criminal Police Organization* for prompt police-to-police cooperation and other methods of information exchange cooperation.

Rationale:

INTERPOL continues to emphasize the importance for the future Convention to foster international cooperation and optimize the use of existing global mechanisms - in line with the final recommendation of the Open-ended Intergovernmental Expert Group on cybercrime as adopted at its 7th session (April 2021). INTERPOL therefore welcomes Paragraph 6 of Article 41 as it acknowledges an important, existing network for international cooperation.

As noted in previous contributions, INTERPOL maintains an active secure law enforcement communications network for the prevention, detection and suppression of ordinary law crime. This 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 complemented by INTERPOL's I-24/7 secure communication network which facilitates the real time and secure exchange of information.

The 24/7 Contact Points for Computer-related Crime can ensure that gaps are bridged with other 24/7 networks of contact points that have a more limited membership – including those that may be established by the future Convention. In short, INTERPOL's many communication channels – such as I-24/7 network and its 24/7 Contact Points for Computer-related Crime – complement other networks or bilateral means of communications and allow real time transmission of information which can be vital to the investigation of a case or apprehension of a perpetrator.

Given the established nature of existing networks, their complementarity and maturity, it will be 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.

d) Enhance international cooperation and information exchange between law enforcement organizations, specifically through INTERPOL, in accordance with their obligations under domestic and international law	**CHAPTER V ARTICLE 47**

Proposals for the draft text of the convention:

INTERPOL supports the reference to the role of international organizations **in Article 47. Law enforcement cooperation, paragraph 2,** to enhance cooperation between law enforcement agencies.

> 2. 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 States Parties may consider this Convention to be the basis for mutual 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*, to enhance the cooperation between their law enforcement agencies.

In addition, it is suggested to include a reference to the role of existing channels of communications available to competent authorities, agencies and services in **Article 47, paragraph 1 (a):**

> (a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services **[INTERPOL'S PROPOSAL: taking into account the existing channels available, including those of the International Criminal Police Organization - INTERPOL, among others,]** 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;

Rationale:

INTERPOL proposes this recommendation in line with the positions stated by several Member States during the Fifth Session, where they asked to include a direct reference to INTERPOL within the former Consolidated Negotiating Document, Article 75 paragraph 1(a).

Law enforcement cooperation is the very bedrock of INTERPOL's mandate. With its dedicated secure communication platforms and constitutional principles of National Sovereignty, Respect for Human Rights, Neutrality and Constant and active cooperation, INTERPOL holds a unique, global role in enabling international law enforcement cooperation – both across and within borders.

INTERPOL's tools and channels are available to its 195 member countries to facilitate and foster such cooperation. This includes INTERPOL's I-24/7 secure global police communications system for police cooperation, accessible via INTERPOL National Central Bureaus (NCBs) located in each of its 195 member countries. Extensions of I-24/7 can be provided by NCBs to national authorities and agencies within the borders of member countries. In addition, INTERPOL offers mechanisms, channels, and platforms to specifically address [the criminal use of ICTs] [cybercrime], which include the Cybercrime Knowledge Exchange (CKE) for non-operational sharing of information within the global cyber security community, and the Cybercrime Collaborative Platform – Operation (CCP-Operation) for restricted and secure operational exchange of intelligence and police data through dedicated workspaces created to coordinate operations and investigations in relation to [the criminal use of ICTs] [cybercrime].

IN THE FIELD: Use of INTERPOL channels in law enforcement cooperation

INTERPOL was significantly involved in Operation "CrystalLink"[3], which uncovered and dismantled a transnational sextortion syndicate in the third quarter of 2022. The operation resulted in the arrest of 12 suspected core members of the syndicate and the identification of at least 34 victims who lost at least USD 47,000 to the syndicate.

The role of INTERPOL in coordinating this operation was fundamental due to the geographic spread of the criminal activity – the perpetrators were situated in China, while the servers hosting the evidence were located in Hong Kong (China) and most of the victims were based in Singapore. Therefore, INTERPOL brought together the relevant law enforcement agencies for proactive investigation, and an in-depth analysis was conducted on a zombie command and control server hosting the malicious application. These allowed the law enforcement agencies to identify and locate individuals linked to the criminal syndicate. The nearly instantaneous exchange of information through INTERPOL's communication channels was instrumental in the success of this operation.

e) Maximize the role of international organizations in promoting and developing preventive measures

CHAPTER VI
ARTICLE 53

Proposals for the draft text of the convention:

INTERPOL welcomes and supports the reference to the role of international and regional organizations in the field of prevention in **Article 53. Preventive measures, paragraph 6:**

> 6. States Parties may collaborate with each other *and with relevant international and regional organizations* in promoting and developing the measures referred to in this article. This includes participation in international projects aimed at the prevention of [cybercrime] [offences committed with the use of information and communications technologies].

[3] https://www.interpol.int/en/News-and-Events/News/2022/Asia-Sextortion-ring-dismantled-by-police

Rationale:

In dealing with [the criminal use of ICTs] [cybercrime] and its rapidly evolving nature, the adoption of robust preventive measures is key. INTERPOL is committed to a comprehensive, proactive, and cooperative approach to prevention, in alignment with its Global Cybercrime Strategy. As such, INTERPOL welcomes the inclusion of Chapter VI in the draft text of the Convention, and notes with appreciation the efforts of the Committee to streamline the text of this Chapter.

Moreover, given the complex and global nature of [the criminal use of ICTs] [cybercrime], INTERPOL reiterates that effective prevention needs to be a shared responsibility, as it will inevitably transcend any single organization's capacity. International cooperation among a wide array of actors will be essential to effectively counter and combat [the criminal use of ICTs] [cybercrime] through preventive measures. To that end, INTERPOL supports the recognition of the role of international and regional organizations in promoting and developing preventive measures, as encapsulated in Article 53 paragraph 6 of the draft text of the Convention.

IN THE FIELD: How INTERPOL brings relevant stakeholders together to prevent cybercrime

In August 2020, INTERPOL published its Global Assessment Report on COVID-19 related Cybercrime based on its unique access to data from its international membership and private-sector partners to provide a comprehensive overview of the cybercrime landscape amid the pandemic. Key findings highlighted by the report included online scams and phishing, disruptive malware (Ransomware and Distributed Denial-of-Service (DDoS) attacks), data harvesting malware and malicious domains.[4]

To support member countries to prevent and combat cybercrime during the pandemic, INTERPOL organized emergency virtual meetings with a variety of stakeholders, including strategic meetings of the Heads of National and Regional Cybercrime Units and the INTERPOL Global Cybercrime Expert Group. INTERPOL Purple Notices[5] were also published and sent through the INTERPOL secured network to inform the law enforcement community of emerging and high-risk cyberthreats, including ransomware attacks against critical infrastructure and hospitals, use and dissemination of banking and malicious software Trojans, and the mailing of malicious USB devices. A Global Malicious Domain Taskforce comprising cybercrime intelligence officers, experts from private-sector partners and national law enforcement officials was convened to identify and target threat actors and common infrastructure behind malicious domains, in order to disrupt and mitigate the threats. About 200,00 malicious domains were identified and analyzed, and Cyber Activity Reports (CARs) containing relevant data were disseminated to more than 80 member countries that were affected based on the findings of the Taskforce.

In addition, INTERPOL led a Global Awareness Campaign on COVID-19 Cyberthreats, #WashYourCyberHands, with member countries 23 external partners to alert the public to key cyberthreats linked to the pandemic, and to promote good cyber hygiene. The visual materials and social media posts of the campaign developed by INTERPOL and its partners reached some 7.5 million users online.

[4] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[5] Under the INTERPOL International Notices System, INTERPOL publishes Purple Notices to member countries to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

f) Leverage to the best possible extent the necessary contributions of all international organizations, including INTERPOL for providing technical assistance and capacity-building	**CHAPTER VII ARTICLE 54**

Recommendation for the draft text of the convention:

INTERPOL welcomes the inclusive reference to the role of international and regional organizations for technical assistance and capacity-building, including in **Article 54. Technical assistance and capacity-building, paragraph 8.** To ensure that the Convention is able to maximize the existing and potential contributions of all the organizations involved in delivering technical assistance and capacity-building, INTERPOL suggests amending **Article 54, paragraph 8**:

> 8. States Parties are encouraged to strengthen, to the extent necessary, efforts to maximize the effectiveness of **[INTERPOL'S PROPOSAL: technical assistance and capacity-building through]** operational and training activities in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements.

Rationale:

INTERPOL recommends greater coherence between Article 54, paragraph 8 and the rest of Article 54 – by using the same language as in the title of the Article "Technical assistance and capacity-building". The amendment to Article 54, paragraph 8 would have three benefits:

i. Recognizing the existing and potential capabilities of all international and regional organizations committed to delivering technical assistance and capacity-building – which may often extend beyond operational and training activities *per se*.

ii. Enabling relevant actors in recipient States to have access to greater and more specialized support that is better tailored to their needs.

iii. Empowering States providing financial support for technical assistance to have more options and therefore greater flexibility when reviewing decisions on making voluntary contributions.

During past sessions, many Member States have indicated that the provisions on technical assistance and capacity-building will be key to implement the future Convention and address effectively the crimes covered therein. As offenders, victims and evidence are often located in different jurisdictions, investigations will typically require international coordinated law enforcement action. This means that gaps in the capacity of one country can severely undermine the safety of communities in other countries.

Technical assistance and capacity-building are key tools to address this challenge. However, to have a real-world impact, the future Convention needs to recognize that addressing the needs of the diverse actors involved in combating [the criminal use of ICTs] [cybercrime] will require various forms of specialized technical assistance, which no single organization can provide. Even within countries, the various actors involved in combating [the criminal use of ICTs] [cybercrime] – including legislators, prosecutors, law enforcement, national Computer Emergency Response Teams (CERTs) – may have very different technical assistance needs.

From a law enforcement perspective, the experience of INTERPOL's Global Cybercrime Programme shows that technical assistance is most effective when it is connected to specific operational activities. Otherwise, technical assistance tends to be delivered through single, one-off projects which lack

sustainable, long-term coordinated support, with a gap between the classroom instruction and the practical application of newly acquired skills on a day-to-day operational basis.

Given the varying needs of all the various actors involved in combating [the criminal use of ICTs] [cybercrime] for different kinds of technical assistance, INTERPOL recommends emphasizing and acknowledging the diverse mandates and complementary capabilities of international organizations in technical assistance and capacity-building. For example, organizations such as the United Nations Office on Drugs and Crime (UNODC), the World Bank, the Global Forum on Cyber Expertise (GFCE), and INTERPOL play important roles in areas that range from fostering the development of policy and legal frameworks to allocation of resources, sharing of best practices and law enforcement cooperation. Collectively, international organizations cater to the various dimensions of [the criminal use of ICTs] [cybercrime] and represent an example of how together we can deliver an effective, coordinated and enhanced global response.

Therefore, INTERPOL reiterates the need for inclusive and flexible language in the Chapter on Technical Assistance. As an international community, we must work together to increase the capacity of all States to prevent and combat [the criminal use of ICTs] [cybercrime]. This is only possible if the Convention is able to maximize to the best possible extent the necessary contributions and specialized roles of the different organizations who deliver technical assistance.

IN THE FIELD: How INTERPOL delivers specialized technical assistance to support law enforcement in 195 member countries

An example of how INTERPOL addresses this gap and links the technical assistance we deliver to our member countries with operational matters is the INTERPOL Africa Cybercrime Operations Desk[6]. With the support of the African Union Mechanism for Police Cooperation (AFRIPOL), the Desk seeks to combat the growing threat of [the criminal use of ICTs] [cybercrime] on the African continent, notably through Africa Cyber Surge Operations.

During the **Africa Cyber Surge Operation 1.0**, which took place from July to November 2022, law enforcement officials from 27 African countries came together under the coordination of INTERPOL's Command Centre in Kigali, Rwanda, to combat cybercrime across the continent. Prior to the operation, INTERPOL conducted a training event to equip national law enforcement officials with essential skills in cybercrime and cryptocurrency investigations.

To achieve optimal operational outcomes, the exchange of actionable intelligence was coordinated by INTERPOL between the national investigators and partners from the private sector. This collaboration enhanced the effectiveness of efforts in countering cyber threats. Additionally, the investigators worked closely with National Cyber Emergency Response Teams, Internet Service Providers, and Hosting Providers to mitigate risks and bolster cyber resilience in the region.

Notable achievements during the operation include the arrest of 11 individuals involved in cybercriminal activities, including one associated with child abuse, and ten others linked to scams and frauds that caused a global financial loss of USD 800,000. The operation also resulted in the takedown of a Darknet Market in Eritrea, the resolution of cryptocurrency scam cases in Cameroon, and the successful recovery of over USD 150,000 for victims in Tanzania. Furthermore, action was taken against more than 200,000 malicious cyber infrastructures, and participating countries proactively improved their national cyber security by addressing vulnerabilities.

[6] https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

The Africa Cyber Surge Operation 1.0 demonstrated the effectiveness of international cooperation and proactive measures in countering cybercrime, safeguarding businesses, and protecting individuals from online threats in the African region.

Following the success of the first operation, **Africa Cyber Surge 2.0** has been held in June 2023 in Tanzania. During the first week, law enforcement representatives from 20 African countries were trained on cybercrime investigations through tabletop exercises and simulated scenarios and given access to INTERPOL's CCP-Operation for restricted and secure information exchange via a dedicated workspace set up for the operation. The skills and tools acquired by the participants during the first week were then applied during the second week comprising coordinated operational activities, such as takedowns of cybercriminal infrastructure, arrests, seizures, prevention and mitigation measures, using data and information provided by INTERPOL and some of its private sector Gateway partners.

The operation has linked cases to an estimated USD 39.4 million in financial loss and, based on the initial successes, it has been decided to extend it further.

- - - - - -