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

Proposal related to the Revised Draft Text of the Convention

January 2024

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

Throughout the AHC process, INTERPOL has been actively contributing to the enhancement of international mechanisms that facilitate police cooperation in the evolving realm of information and communications technologies being utilized for criminal purposes - coupled with a steadfast focus on promoting the interests and needs of the global law enforcement community.

With reference to the revised draft text of the convention, as per A/AC.291/22/Rev.1, INTERPOL expresses its appreciation for the efforts and steps forward that the UN Member States have been taking, with the key support of the AHC Secretariat, to get closer to a final version of the International Convention.

To further the advancement and facilitate a consensus, INTERPOL proposes a single proposal for the consideration of negotiating parties, relating to **Article 47 on Law Enforcement Cooperation**. Although the proposal is not a new concept since it echoes ideas previously raised by various Member States in the Fifth Session (Vienna, April 2023) and Sixth Session (New York, August 2023), it is intended to reinforce the relevant Article on law enforcement cooperation and the Convention as a whole. INTERPOL believes that such proposal will significantly strengthen international cooperation and the exchange of information among law enforcement agencies, thereby enhancing the real-world impact of the future Convention.

INTERPOL PROPOSAL

INTERPOL proposes including a reference to the role of existing channels of communications available to competent authorities, agencies and services in **Article 47, paragraph 1(a) of the revised draft text of the convention:**

To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services ***[PROPOSAL: taking into account the existing channels available, including those of the International Criminal Police Organization, 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 recognizes and respects that the current language used in Article 47, including paragraph 1(a), is influenced by the United Nations Convention Against Transnational Organized Crime (Article 27) and the United Nations Convention against Corruption (Article 48). INTERPOL also takes note of the ongoing discussions regarding the scope of offenses that should be covered under Article 47.

Nevertheless, INTERPOL aligns with the sentiments expressed by numerous Member States during the Fifth and Sixth Sessions in support of direct reference to INTERPOL in the text of the Convention and encourages its re-introduction in Article 47, paragraph 1(a) of the revised draft text of the Convention. This proposal was initially introduced in the Fifth Session and subsequently supported by an increased number of Member States in the Sixth Session. Its purpose is to acknowledge the role of INTERPOL as an existing and established actor in exchange of information within the field of law enforcement cooperation.

According to the Constitution of INTERPOL[1], the aims of the organization are:

> (1) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights";
>
> (2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

For the last 100 years, INTERPOL has fulfilled this role by facilitating secure and rapid information exchange among law enforcement agencies and offering operational support and technical assistance worldwide. INTERPOL is in a unique position to provide a range of policing capabilities encompassing a mix of specialized expertise, tools and services designed to support law enforcement cooperation. These include:

- 19 global databases, accessible via I-24/7, the Organization's secure global communication system that links law enforcement in all member countries and enables authorized users to share sensitive and urgent police information to their counterparts around the globe;
- Forensics expertise, using specialist knowledge of fingerprints, DNA, facial recognition and digital forensics;
- In-depth criminal intelligence analysis, including operational and strategic analysis reports;
- Global and regional operational coordination and support, including fugitive investigative support;
- A 24/7/365 Command and Coordination Centre, which acts as a first point of contact for any country requiring urgent assistance from INTERPOL or from another country; and
- Special projects to address emerging challenges and provide customized capacity building and training programmes for law enforcement.

The support that INTERPOL provides to its 196 member countries is built on and enhanced by robust governance and legal frameworks. The INTERPOL Constitution is at the core of the Organization's goals, roles, and ethical guidelines, following the guiding principles of National sovereignty; Respect for Human Rights; Neutrality; and Constant and active cooperation. In addition, in an era where data is crucial to law enforcement, INTERPOL adheres to stringent Rules on the Processing of Data[2], which

[1] The Constitution of INTERPOL is available online: https://www.interpol.int/content/download/590/file/01%20E%20Constitution_2024.pdf.

[2] The Rules on the Processing of Data of INTERPOL are available online: https://www.interpol.int/content/download/5694/file/24%20E%20RPD%20UPDATE%207%2011%2019_ok.pdf.

ensure that privacy, security, and individual rights are meticulously respected in all data handling processes.

These factors distinguish INTERPOL as a unique and neutral leader in global law enforcement collaboration – and explain why many UN Member States are sharing the same position in including a direct reference to the Organization in Article 47, paragraph 1(a).

Additional recent operational examples of how INTERPOL enables law enforcement cooperation through facilitating secure and rapid information exchange are provided below.

RECENT INTERPOL OPERATIONAL EXAMPLES (AUGUST – DECEMBER 2023)

OPERATION SYNERGIA

Launched in September 2023, this is a global operation coordinated by INTERPOL to disrupt and dismantle criminal activities related to various cybercrimes such as phishing attacks, banking malware, and ransomware.

Role of international law enforcement cooperation:
During the three-month operation, law enforcement from over 50 different countries exchanged cyber intelligence through INTERPOL channels, resulting in the production of over 60 Cyber Activity Reports. In turn, these enabled investigators to take actions on thousands of malicious servers and to arrest suspects across multiple countries.

Operational outcomes:

- Actions were taken on over 1,300 suspicious IP addresses or URLs.
- 70% of the malicious Command & Control (C2) servers were taken down in collaboration with law enforcement agencies and Internet Service Providers (ISPs), while 30% are under investigation.
- Major cybercrime groups were uncovered.
- 70 suspects were identified and located.
- 31 individuals were arrested, and searches were conducted in 30 premises.
- There was significant cooperation by Singapore, who took down 86 C2 servers related to phishing, banking malware and ransomware.

Participating countries: Algeria, Australia, Bangladesh, Belarus, Belgium, Benin, Bolivia, Bosnia and Herzegovina, Brazil, Cameroon, Canada, China, Cyprus, Czech Republic, Dominican Republic, Ecuador, Estonia, Eswatini, France, Greece, Guatemala, Guyana, Hong Kong (China), India, Ireland, Israel, Jordan, Kuwait, Latvia, Lebanon, Lichtenstein, Maldives, Mauritius, Moldova, Nepal, Nicaragua, Nigeria, Palestine, Poland, Qatar, Russia, San Marino, Singapore, South Korea, South Sudan, Spain, Sri Lanka, Sweden, Switzerland, Tunisia, Türkiye, Uganda, United Arab Emirates, Uruguay, Tanzania, Tonga, and Zimbabwe.

OPERATION KINGFISHER[3]

In August 2023, INTERPOL coordinated a global operation against a 'phishing-as-a-service' (PaaS) platform known as '16shop'. The platform had sold phishing kits to hackers seeking to defraud victims

[3] For further information on Operation Kingfisher, please see the press release: https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

through email scams. It is estimated that before being shut down, '16shop' had contributed to compromising over 70,000 users in 43 countries.

Role of international law enforcement cooperation:
Through intensive intelligence sharing between the INTERPOL General Secretariat's Cybercrime Directorate, national law enforcement in Indonesia, Japan, the United States and INTERPOL private sector partners, investigators were able to determine the identities of the '16shop' PaaS platform administrator and facilitators and to build a case for their arrest. The operation has also strengthened international collaboration against cybercrime, particularly phishing.

Operational outcomes:
- The notorious '16shop' PaaS platform was shut down.
- The PaaS platform operator, a 21-year-old man, and two facilitators were arrested in Indonesia and Japan.
- Electronic items and several luxury vehicles were seized.

Participating countries**:** Indonesia, Japan, and United States.

OPERATION STORM MAKERS II[4]

For the first time in 2023, INTERPOL coordinated a global operation specifically targeting the growing threat from human trafficking-fueled fraud. In these criminal schemes, victims were lured through fake job advertisements and forced to commit online scams in cyber scam centres, including fake cryptocurrency investments, work-from-home, lottery, and online gambling schemes.

Role of international law enforcement cooperation:
The secure and rapid exchange of information between law enforcement agencies across different regions through INTERPOL channels was critical to the success of the five-month investigative coordination.

Operational outcomes:
- More than 270,000 inspections and police checks were carried out by law enforcement from participating countries at 450 human trafficking and migrant smuggling hotspots.
- 281 individuals were arrested for offences including human trafficking, passport forgery, corruption, telecommunications fraud, and sexual exploitation.
- About 800 potential victims, likely victims of fake recruiters, were intercepted across all countries.
- 149 human trafficking victims were rescued.
- Over 360 investigations were opened, many of which are ongoing.

Participating countries: Angola, Australia, Bangladesh, Brazil, Cambodia, China, Ethiopia, Ghana, India, Indonesia, Kazakhstan, Kenya, Laos, Malaysia, Myanmar, Nepal, Pakistan, Philippines, Singapore, South Africa, Sri Lanka, Tanzania, Thailand, Türkiye, Uganda, United Arab Emirates, and Vietnam.

[4] For further information on Operation Storm Makers II, please see the press release: https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further-insights-into-globalization-of-cyber-scam-centres

OPERATION NARSIL[5]

This is a global operation focused on disrupting networks of child sexual abuse websites designed to generate profits from advertising. The operation was one of the first INTERPOL operations to focus on criminals receiving advertising revenue from website visitors interested in child sexual abuse content. Targeting the financial mechanisms used by the website administrators for their online advertising campaigns, the main goals of the operation were to track the money made by perpetrators and prevent the revictimization of children involved.

Role of international law enforcement cooperation:

- Over two years, law enforcement in INTERPOL member countries worked together using the INTERPOL Worst of List (IWOL), sharing targeted intelligence, pinpointing suspects and coordinating arrests of persons managing the websites. The IWOL was created in 2010 and contains a watchlist of websites with extreme child abuse material, and more than 20,000 domains disseminating child sexual abuse imagery have been seized by INTERPOL in collaboration with law enforcement partners over 13 years.

Operational outcomes:

- Two suspects were identified and arrested as a result of investigations by Argentinian law enforcement authorities, as well as IWOL digital clues and intelligence provided by the global police community. Cash, credit cards and 14 electronic devices were seized from the home of the suspects who are siblings. They are thought to have created, maintained and financially benefitted for more than a decade from websites featuring child sexual abuse materials and associated advertising campaigns.
- A male individual was arrested by Bulgarian law enforcement for operating an online forum sharing child sexual abuse materials. Bulgarian Police also closed the forum, which had been running since 2020 and is thought to have facilitated access to thousands of media files depicting serious child sexual abuse materials.
- A male individual was arrested for possession and distribution of child sexual abuse materials by Thai police, with the support of the United States Homeland Security Investigations. Large amounts of child sexual abuse materials and financial transaction records associated with online distribution of abuse photographs were also uncovered in his residence.
- Russian police authorities arrested two citizens for production and online circulation of materials depicting the sexual violation of minors. Authorities searched the suspects' homes and seized computer equipment containing specialized software for creating and administrating websites, as well as removable hard drives containing child sexual abuse materials.

Participating countries**:** Austria, Argentina, Belarus, Bulgaria, Canada, Cyprus, Estonia, France, Germany, Italy, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Moldova, Netherlands, New Zealand, Norway, Poland, Romania, Russia, Singapore, Spain, Switzerland, Thailand, United Kingdom, and United States.

[5] For further information on Operation Narsil, please see the press release: https://www.interpol.int/en/News-and-Events/News/2023/Operation-Narsil-disrupts-network-of-child-abuse-websites-designed-to-generate-profits-from-advertising

OPERATION HAECHI IV[6]

The transcontinental operation targeted online financial crimes, focusing on voice phishing, romance scams, online sextortion, investment fraud, money laundering linked to illegal online gambling, business email compromise fraud, and e-commerce fraud.

Role of international law enforcement cooperation:
Over the six-month investigation, law enforcement across borders used INTERPOL channels to exchange information on virtual assets accounts linked to transnational organized crime. Notably, investigators worked together to detect online fraud and freeze associated bank and virtual asset service provider (VASP) accounts using INTERPOL's Global Rapid Intervention of Payments (I-GRIP), a stop-payment mechanism which helps countries work together to block criminal proceeds.

Operational Outcomes:

- Working with VASPs, INTERPOL helped to identify 367 virtual assets accounts linked to transnational organized crime, enabling police in member countries to freeze the assets and commence investigations.
- About 3,500 persons were arrested and assets worth USD 300 million were seized across the involved countries.
- 82,112 suspicious bank accounts were blocked, with the seizure of USD 199 million in hard currency and USD 101 million in virtual assets.
- A high-profile online gambling criminal in Manila was arrested as a result of significant cooperation between Filipino and South Korean authorities.
- INTERPOL published two Purple Notices[7] warning member countries about emerging digital investment fraud practices, including Non-Fungible Token (NFT) scams and the use of artificial intelligence (AI) and deep fake technology in fraud.

Participating countries: Argentina, Australia, Brunei, Cambodia, Cayman Islands, Ghana, Hong Kong (China), India, Indonesia, Ireland, Japan, Kyrgyzstan, Laos, Liechtenstein, Malaysia, Maldives, Mauritius, Nigeria, Pakistan, Philippines, Poland, Korea, Romania, Seychelles, Singapore, Slovenia, South Africa, Spain, Sweden, Thailand, United Arab Emirates, United Kingdom, United States, and Vietnam.

In closing, INTERPOL thanks Member States and the AHC Secretariat in advance for their consideration of this proposal and reiterates its commitment to undertake an integral role in the implementation of the new Convention in order to reduce the impact of information and communications technology being used for criminal purposes.

For further information, discussion, and/or to join this proposal, please contact the INTERPOL Global Cybercrime Programme at **EDPS-CD@interpol.int**.

- - - - - -

[6] For further information on HAECHI IV, please see the press release: https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

[7] Purple Notices are issued by INTERPOL to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals. For further information on INTERPOL Notices, please see: https://www.interpol.int/en/How-we-work/Notices/About-Notices