INTERPOL submission to the 2nd Intersessional Consultation of the Ad Hoc Committee on "International Cooperation" – June 2022

INTRODUCTION

This is a submission by the International Criminal Police Organization-INTERPOL, in its role as Permanent Observer to the United Nations[1], to the second intersessional consultations of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes taking place in Vienna on 13-14 June 2022. This submission will focus on the agenda item "International Cooperation".

INTERNATIONAL LAW ENFORCEMENT COOPERATION

There is extensive cooperation on the global level between law enforcements authorities. This cooperation ranges from the bilateral to regional and multilateral international cooperation and is underpinned by a mesh of bilateral, regional and international agreements and conventions, including the United Nations Convention against Transnational Organized Crime. Law enforcement cooperation uses several different avenues for carrying out investigatory measures such as those enshrined in national legislation or conventions, regional or global networks for information exchange such as INTERPOL's platforms and tools as well as more informal cooperation measures that build on established good faith trusted contacts and partnerships, in line with respective national legislative rules.

Such **international law enforcement cooperation** aims to secure digital evidence and other formal investigatory measures as part of building the prosecution of a case and building the materials, information and intelligence needed to move an investigation forward. Such cooperation is also important when it comes to preventive measures, the exchange of information about new criminal modus operandi and keeping law enforcement authorities informed about changes in the threat environment. International law enforcement and police-to-police cooperation is also key for joint investigations and operations between states where law enforcement actions can be taken to disrupt cybercriminal activities and minimize harm and damage to individuals, societies and companies.

Hence, any new international convention on cybercrime should further promote the use of existing forms of cooperation between law enforcement that are well-established and have demonstrated proven success. This will avoid a duplication of structures and allow existing mechanisms for

[1] See A/RES/51/1. See also A/RES/75/282 op. 7.

cooperation and exchange to work more effectively. With that in mind, INTERPOL will elaborate on its tools, channels, and platforms used to facilitate international law enforcement cooperation in the next section of this submission for Member States' consideration.

INTERPOL TOOLS AND PLATFORMS FOR INTERNATIONAL COOPERATION BETWEEN LAW ENFORCEMENT AUTHORITIES

INTERPOL is the main structure and a neutral platform for international law enforcement cooperation and information exchange globally, connecting 195 member countries and their law enforcement authorities through a National Central Bureau in each country. The INTERPOL Global Cybercrime Programme was set up in 2018 to help member countries prevent, detect, investigate and disrupt cybercrime. The programme seeks to coordinate activities that reduce the global impact of cybercrime and protect communities for a safer world. A key component is the **regional cybercrime operational desks** that provide member countries with support tailored to their local context, needs and challenges.

INTERPOL's secure **I-24/7 global police communications system** connects law enforcement officers in all 195 member countries and enables authorized users to share sensitive and urgent police information with their counterparts. In 2021 alone, law enforcement across the world shared over 26 million messages via the INTERPOL global communication network, I-24/7. The network also enables investigators to access INTERPOL's range of 19 criminal databases containing over 120 million records shared by member countries Last year these databases were searches approximately 4 billion times by law enforcement across the world.

Notices issued by INTERPOL at the request of member countries is one of the main tools for law enforcement to, for example, trace wanted persons or inform one another about modus operandi of criminals. The notices are published by INTERPOL's General Secretariat after vetting to ensure they are in line with INTERPOL's Constitution and rules. Of special importance for cybercrime is the Red Notice for wanted persons and the Purple Notice for sharing modus operandi. Some notices, such as the Purple Notice, can also be issued by INTERPOL itself building on intelligence shared with it by member countries.

INTERPOL Notices:

RED NOTICE	*Wanted persons*
PURPLE NOTICE	*Modus operandi*
BLUE NOTICE	*Additional information*
GREEN NOTICE	*Warnings and intelligence*
ORANGE NOTICE	*Imminent threat*
YELLOW NOTICE	*Missing persons*
BLACK NOTICE	*Unidentified bodies*
INTERPOL-UN SECURITY COUNCIL SPECIAL NOTICE	*Groups and individuals subject to UNSC sanctions*

To ensure that information can be acted on quickly, 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. INTERPOL's 24/7 Contact Points for Computer-related Crime has global reach and thereby complements other regional contact points networks or bilateral contacts.

The INTERPOL **Cybercrime Knowledge Exchange** is open to law enforcement, governments, international organizations and cybersecurity industry experts to exchange non-police operational information on cybercrime. It is a dynamic communication channel that enables authorized users around the world to discuss the latest cybercrime trends, prevention strategies, detection technologies and investigation techniques.

The INTERPOL **Cybercrime Collaborative Platform – Operations** is a restricted-access platform that enables operational stakeholders to share intelligence in an interactive and secure environment. Member countries can use this platform to enhance their operational efficiency and effectiveness.

In order to conduct ingestion, correlation and analysis of operationally relevant cybercrime data, the INTERPOL **Cyber Fusion Platform** serves as a hub for aggregation of cybercrime data globally from both member countries and private partners,

INTERPOL tools and platforms under development

INTERPOL is working on the **e-Extradition Initiative** which aims to replicate step-by-step in an electronic format the traditional process for transmission of an extradition request via competent national authorities on the basis of existing bilateral and multilateral treaties, and in compliance with current legislation and practice at the national level. It 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.

Similarly, INTERPOL's **e-MLA Initiative** aims to foster international cooperation in criminal matters by providing a secure electronic transmission capability for requests seeking legal assistance in cross-border cases. 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. Both the e-Extradition Initiative and the e-MLA Initiative now require extra budgetary funding from interested member countries for their full implementation.

INTERPOL has recently developed, through the **WHOIS project**, a pilot testing model of a new restricted portal that will provide automated access to non-public domain registration information data contained in the WHOIS database for vetted law enforcement entities. This information is an essential building block of many investigations with cyber elements and has through recent regulatory changes become significantly harder to access for law enforcement.

The work engaged in the WHOIS project will also enable the establishment of a **secure police identifier** for officials from vetted, identified and accredited law enforcement authorities that are internationally recognized. Such a global identity for police services will simplify considerably the work of investigators when engaging with private companies for information requests, which is central to cybercrime investigations. INTERPOL, through its global institutional legitimacy, is well-placed to offer such verification of law enforcement authorities.