



Statement by INTERPOL at Second Session of the Ad Hoc Committee on General Provisions

CHECK AGAINST DELIVERY

Madam Chairperson,

INTERPOL very much welcomes your decision that multi-stakeholders be given the opportunity to speak today and tomorrow. The ability to share our views and participate in the discussion for each agenda item is key to ensuring multi-stakeholders' meaningful participation in this process.

For member states' consideration, INTERPOL – in its capacity as Permanent Observer to the United Nations – will offer some perspectives on Agenda Item 5 regarding General Provisions first. At the heart of implementing the intended aims of the Convention lies enhancing international cooperation – including law enforcement cooperation – and promoting capabilities development.

At the center of any cross-border investigation is a formal or informal law enforcement collaboration. INTERPOL's mission is to prevent and fight crime through enhanced cooperation and innovation on police and security matters. Moreover, INTERPOL's Global Cybercrime Programme aims to reduce the global impact of cybercrime and protect communities for a safer world. We support our member countries in the prevention, detection, investigation, and disruption of cybercrime.

Throughout the almost 100 years that INTERPOL has existed, we have repeatedly seen the need for effective international law enforcement cooperation. It would be useful for the Convention to recognize and build upon existing structures and platforms for such cooperation. INTERPOL has existing channels, tools, and platforms available for the effective implementation of the Convention. First of all, INTERPOL has an I-24/7 secure network that connects all our 195 member countries and their law enforcement authorities. Authorities are also able to use

INTERPOL's Cybercrime Knowledge Exchange Platform to collaborate and share best practices and information on the cyber threat landscape. INTERPOL also has the Cybercrime Collaborative Platform – Operations for secured and rapid communications in relation to joint operational activities. All of these INTERPOL channels have inbuilt safeguard mechanisms, including comprehensive data protection standards, access control for contributing Member States, and legal compliance processes.

INTERPOL sees on a daily basis how cybercriminals enhance and develop their tactics and modus operandi. INTERPOL has been able to see a change towards a more advanced persistence of cybercrime threat, especially over the last couple of years. We continuously inform our member countries of these evolutions and new attack patterns through Cyber Threat Reports, Cyber Activity Reports, and INTERPOL Purple Notices. Therefore, as has been mentioned, a forward-looking and technologically-neutral language would ensure an enduring and relevant Convention.

INTERPOL has seen the evolution to a situation where electronic evidence is now a part of most criminal investigations. Challenges and the type of evidence differ somewhat between different crimes, also within the wide range of cybercrimes. This can be taken into account by member states when deciding whether the procedural measures and international cooperation outlined in the Convention should apply to specific offenses or all crimes.

Human rights, fundamental freedoms and the rule of law are especially relevant in this context. This is likewise recognized by Article 2 of INTERPOL's Constitution which references the Universal Declaration of Human Rights.

Based on our experience facilitating and coordinating cross-border investigation and disruption of cybercrime, INTERPOL has witnessed time and again the value of having a harmonized international legal framework and a common set of principles and standards. This is especially important when it comes to the exchange of information, expertise, technical assistance and best practice.

Thank you.