



Statement by INTERPOL at Second Session of the Ad Hoc Committee on Procedural measures and Law Enforcement

CHECK AGAINST DELIVERY

Madam Chairperson,

With increased reliance on technology and the digital environment, most crime types now have a cyber element and electronic evidence is central to the work of law enforcement and judicial authorities. As such, INTERPOL urges Member States to consider extending the scope of procedural measures and international cooperation to offences beyond those established in the Convention, of course with due regard to adequate protections for individuals' rights.

The issue of jurisdiction should also be addressed because of the inherently cross-border nature of cybercrime. There are no clear territorial boundaries in cyberspace, and this is further complicated by emerging technologies such as the Cloud or decentralized data storage. Conditions and safeguards, general or specific to a provision, may also be included.

Furthermore, INTERPOL notes that Member States have advocated a comprehensive list of procedural powers for competent authorities to detect, investigate, disrupt, and prosecute cybercrime.

With reference to our written contribution for the Second Session of the Ad Hoc Committee, INTERPOL has made several proposals under this chapter.

Firstly, INTERPOL invites Member States to recognize in this Convention the need for cooperation between law enforcement and the private sector, including through INTERPOL channels and framework. The private sector is where a significant amount of relevant data on cybercrime resides. For example, based on INTERPOL's experience working with private companies under our 'Gateway' legal framework in compliance with rigorous data protection standards, these

data can be transformed through analytics into actionable intelligence for countering cybercrime. Industry players also have the unique technical expertise to support training and capacity building.

The Convention can also clarify the rights and obligations of service providers, and how best they can assist the competent authorities. Without clear guidance, it would be overly burdensome for service providers to be regulating and policing the digital space – a task that public authorities and law enforcement should be responsible for.

Secondly, INTERPOL would like to highlight the importance of law enforcement cooperation. It is imperative to enhance the exchange of information, experiences, and best practices *within* and *between* Member States, as supported by paragraphs 6, 13, 18(a) to (c) of the IEG recommendations. INTERPOL channels such as our Notices and Diffusions, I-24/7 network or other general knowledge exchange platforms are already in use by law enforcement to facilitate this process. As such, they may be referenced in the Convention to reflect the reality of international law enforcement cooperation and foster it further.

Thank you.