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

CHECK AGAINST DELIVERY

Madam Chairperson,

INTERPOL would like to extend our gratitude to you for leading the Ad Hoc Committee to elaborate a *Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* and to the Secretariat in all of the preparations for this session. INTERPOL is committed to engaging in this process and supporting Member States by offering the global law enforcement perspective and expertise. INTERPOL has also made a written submission to the second AHC session on our proposals for the chapter on 'Procedural measures and Law Enforcement'.

INTERPOL recognizes the progress made by this Committee at its first session and encourages that the views of multi-stakeholders shared during the intersessional consultation be considered. INTERPOL also considers the *Compilation of Draft Provisions* and the *Guiding Questions* prepared by the Chair and the Secretariat an excellent starting point for our deliberations.

Turning to the Criminalization chapter of the Convention, INTERPOL emphasizes the importance of reaching a broad consensus on the criminal offences to be established and the use of common language. This will also clarify for global law enforcement the types of illegal cyber-related activities. Moreover, harmonization will greatly facilitate effective international cooperation to counter cybercrime given its cross-border nature. For instance, certain dual criminality issues faced by law enforcement during cross-border investigation and disruption can be minimized.

To support Member States in this process, INTERPOL would like to share some trends we have observed in the field.

Firstly, there is an increasing volume and sophistication in cyber criminality, we are seeing now an advanced persistence of cybercrime globally. There is often an entire value chain and cybercrime ecosystem behind every attack. Notably, cyber threat actors may adopt a business model known as “cybercrime-as-a-service”. They may develop malicious tools necessary for a cyberattack for sale, sell illegal access to compromised systems or networks, etc. This means that multiple actors may be involved, ranging from those who supply such services and actors who eventually deploy the tools to execute the attack. As a result, the technical barrier for criminals to engage in cybercrimes has been lowered and attribution has become more difficult for law enforcement. It is thus key that national legislative and other measures target every stage of the cybercrime value chain.

Secondly, there is a diversity of cyber threats across regions, which has led to differences in prioritization by Member States. For instance, according to INTERPOL Cyberthreat Assessments in 2021, the top threat in Africa is Online Scams whereas, for the Southeast Asian region, it is Business Email Compromise. On the other hand, ransomware has been more prominent in the West. Adopting Criminalization that covers the whole suite of cybercrime is essential for making the Convention a comprehensive one.

Lastly, INTERPOL has witnessed cybercrime perpetuated through different technological means and targeting different entities, depending on the technical and social vulnerabilities that can be exploited at the time. Some offences identified by Member States may be viewed as instances of a broader class of illicit activities. They can thus be subsumed under more general offences that are at the same time clear and unambiguous. This will help the Convention stand the test of time while safeguarding human rights and fundamental freedoms.

INTERPOL looks forward to continuing our support to this process. Thank you.