INTERPOL Statement on Technical Assistance and Information Exchange

Mr. Chairperson, thank you for giving INTERPOL the floor once again. In our statement, we would like to address question 23.

1.

Cybercrime is a truly global threat, affecting communities around the world. With offenders, victims and evidence often located in different jurisdictions, international coordinated enforcement action is key to effectively prevent, detect, investigate and prosecute cybercrime – as INTERPOL has repeatedly noted in its previous statements.

In turn, this means that we are only as strong as our weakest link – no one is safe if everyone is not safe. Indeed, as many States have indicated during past sessions, the capacity of states to prevent and combat cybercrime varies greatly from one country to the next.

Recognizing this challenge, INTERPOL has been delivering technical assistance tailored to the needs of law enforcement in our 195 member countries, to equip police with the skills, knowledge and technical capabilities needed to keep pace with rapidly evolving technological developments, at the national, regional and international levels.

For example, INTERPOL's **Cyber Capabilities & Capacity Development Project (C3DP)**[1] works to strengthen regional cooperation against cybercrime in Southeast Asia, with a particular focus on malware analysis and cryptocurrency investigations to address prominent cyber threats in the region. Funded by the United States, this project has been delivering specialized training courses and table-top exercises, both in-person and online, to enhance investigative capabilities of cybercrime law enforcement personnel. Regional expert groups have also been established, bringing together cybercrime investigators trained at the advanced level for enhanced operational support and knowledge exchange among Southeast Asian member countries.

Through such projects, mechanisms and platforms to build capacities, provide technical assistance and facilitate information exchange among States specific to cyber threats that they encounter, INTERPOL works with various stakeholders to ensure that police everywhere have the ability to combat cybercrime effectively.

[1] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project

2.

INTERPOL welcomes the Convention and its Chapter on Technical assistance as an important opportunity to do more under its strategic priority of closing gaps and bridging divides between different countries' capabilities, capacities and information sharing across the globe to overcome the shared challenges of countering cybercrime.

In terms of the specific provisions of the Convention, we would recommend the Committee to consider that even within countries, the various stakeholders involved in combating cybercrime – legislators, prosecutors, law enforcement, national Computer Emergency Response Teams (CERTs), etc. – may have very different technical assistance needs.

From a law enforcement perspective, the experience of INTERPOL's Global Cybercrime Programme shows that technical assistance should be closely connected to specific operational activities. This is because often technical assistance is delivered through single, one-off projects focused on training in methods of detection, investigation and prosecution of cybercrime, including the collection of e-evidence. Yet these projects lack sustainable, long-term coordinated support, with a gap between the classroom instruction and the practical application of newly acquired skills on a day-to-day operational basis.

An example of how INTERPOL addresses this gap and links the technical assistance we deliver to our member countries with operational matters is our Regional Cybercrime Operations Desk model, such as our Africa Cybercrime Operations Desk.

During INTERPOL's earlier statement on International Cooperation, my colleague mentioned the Africa Cyber Surge of 2022, a technical assistance initiative which conducts, facilitates and coordinates joint operations against cybercrime in the African region.

In fact, just a few days ago, INTERPOL, through our Africa Cybercrime Operations Desk and with the support of AFRIPOL, again sought to combat the growing threat of cybercrime on the African continent by commencing "Africa Cyber Surge 2.0" in Tanzania. During the first week of the Surge 2.0, law enforcement representatives from 20 African countries will be trained on cybercrime investigations through tabletop exercises and simulated scenarios designed with a wide range of stakeholders including INTERPOL officials, national CERTs, prosecutors, etc. Participants will also be given access to INTERPOL's Cybercrime Collaborative Platform-Operation for restricted and secure information exchange on operational activities. The skills and tools acquired by the participants through this first week will then by applied during the second week of coordinated operational activities featuring takedowns of cybercriminal infrastructure,

seizures, prevention and mitigation measures, using data and information provided by INTERPOL and some of its private sector Gateway partners.

Through such activities ranging from training and capacity building, information exchange to the provision of tools, the specialized technical assistance that INTERPOL provides to law enforcement is focused on ensuring operational successes, sustainable learning for law enforcement officials and reducing the harm from cybercrime regionally and globally.

3.

To have a real-world impact, the future Convention should recognize that addressing the needs of the diverse stakeholders involved in combatting cybercrime will require various forms of specialized technical assistance, which no single organization can provide.

This means the provisions in the Chapter on Technical Assistance should privilege inclusive language, to acknowledge and support the existing specialized roles of the many stakeholders who deliver technical assistance effectively - including INTERPOL's specialized, neutral and global technical assistance to law enforcement in terms of cyber threat response and operational activities.

In that regard, we welcome the inclusive reference to the role of various multistakeholders, including international organizations **in Article 54, paragraph 8; Article 55, paragraphs 1 and 2; and in Article 56, paragraph 2 (d) of the Zero Draft Convention.** Such inclusive language is essential for the Convention to leverage to the best possible extent the contributions of all relevant stakeholders.

4. Concluding remarks

We hope these remarks will be useful to States not just in drafting this Convention, but also when reviewing decisions on making voluntary contributions, to maximize the capabilities of all relevant stakeholders involved in delivering technical assistance, including international organizations, non-governmental organizations, civil society organizations, academic institutions and the private sector.

As an international community, we need to do more to work together and increase the capacity of our member countries to prevent and combat cybercrime, so that we can protect our communities for a safer world.

Before I end my Statement, I would like to take this opportunity to recall that INTERPOL will be submitting detailed recommendations on the Zero Draft in written in advance of the Sixth session in New York.

Thank you.