INTERPOL Statement on Preventive Measures

INTRO

Chairperson,

In our statement, we would like to address Question 20 - What preventive measures, in your view, would be particularly effective in preventing and combating [cybercrime] [the use of information and communications technologies for criminal purposes]?

STATEMENT

In dealing with cybercrime and its rapidly evolving nature, the adoption of robust preventive measures is key. INTERPOL promotes a comprehensive, proactive, and cooperative approach to prevention, in alignment with our Global Cybercrime Strategy. With this in mind, INTERPOL welcomes the inclusion of Chapter VI in the Zero Draft of the Convention. We also note with appreciation the efforts of the Committee to streamline the text of this Chapter.

Addressing Question 20, based on INTERPOL's extensive experience and successful initiatives, we would like to underscore three particularly effective preventive measures– in line with Art 53, para 3: Strengthening Cooperation Between Law Enforcement and Relevant Stakeholders; Public Awareness; and Strengthening Criminal Justice Systems.

Please allow me to elaborate on these three preventive measures from our perspective.

In relation to Strengthening Cooperation Between Law Enforcement and Relevant Stakeholders, we do believe that enhancing cooperation and information exchange between law enforcement and entities in both the public and private sectors is paramount for preventing cybercrime. On this matter, INTERPOL supports this process through our secure platforms, such as the **Cybercrime Knowledge Exchange (CKE)** for non-operational information sharing and the **Cybercrime Collaborative Platform-Operation (CCP-Operation)** for operational data and intelligence exchange, as was highlighted in our earlier statements.

Furthermore, INTERPOL participates in global prevention projects such as the International Cyber Offender Prevention Network (InterCOP)[1] led by the Netherlands and co-signed by the United Kingdom, Finland, Sweden and Portugal – and regularly cooperates with key fellow organizations such as the World Economic Forum's Partnership Against Cybercrime. On an ongoing project, named "Cybercrime Atlas"[2] ,

[1] https://www.politie.nl/en/information/what-does-the-the-international-cyber-offender-prevention-network-intercop-do.html

[2] https://www.weforum.org/press/2023/01/forum-hosted-cybercrime-initiative-to-boost-coordination-between-private-sector-and-law-enforcement/

we are now identifying and analyzing the actors, infrastructures and operations behind major cybercrime groups.

Secondly, in relation to Public Awareness, we do value the role of communication campaigns and initiatives to increase public understanding of cyber threats – based on the notion that we can all be victims of cybercrimes. INTERPOL regularly conducts global campaigns to raise public awareness of various forms of cybercrime and provide preventive advice against such crimes. For instance, the **#YouMayBeNext** campaign in June 2022 focused on digital extortion threats including ransomware and Distributed Denial of Services (DDOS), and delivered practical tips to help individuals and businesses protect their systems, networks, and devices. Our previous global cyber awareness campaigns such as #JustOneClick (targeting online scams, phishing and business email compromise) and #OnlineCrimeIsRealCrime (targeting cryptojacking and online crimes against children among other crimes) have also highly contributed to various facets of cybercrime prevention.

Eventually, concerning Strengthening Criminal Justice Systems, we are committed to strengthening cooperation between law enforcement, prosecutors and other relevant stakeholders that can enable the secure and timely delivery of information to appropriate entities poised to take action - which is crucial to prevent cybercrime. Within this context, the **INTERPOL Cyber Fusion Centre** produces actionable intelligence via **Cyber Activity Reports**, which are based on the accumulated and analyzed cybercrime data – and are key to foster prevention at the national and regional level. This was the case, for instance, of the Africa Cyber Surge Operation[3] conducted from July to November 2022 – where 28 Cyber Activity Reports were produced to support multiplying preventive efforts. In addition to that, INTERPOL also implements externally-funded projects that are proving to be successful in increasing the capacity of criminal justice practitioners. These include – but are not limited to - the Global Action on Cybercrime Extended (GLACY+)[4], a joint initiative of the European Union and the Council of Europe with INTERPOL as a joint implementer[5]. Among different objectives, GLACY+ strenghtens the capacity of criminal justice authorities in 19 beneficiary countries worldwide to apply cybercrime legislation, policies and strategies, as well as for effective international cooperation in these areas.

CONCLUSION

While we have identified the three preventive measures above as particularly important from a global law enforcement perspective, we acknowledge there are other useful preventive measures, including those encapsulated in Article 53 paragraph 3 of the Zero Draft. This leads us to our final point:

INTERPOL would like to reiterate that international cooperation among a wide array of stakeholders is key to effectively counter cybercrime through preventive measures. This shared responsibility transcends any single organization's capacity, given the complex and global nature of cybercrime, and should be

[3] https://www.interpol.int/en/News-and-Events/News/2022/Operation-across-Africa-identifies-cyber-criminals-and-at-risk-online-infrastructure
[4] https://www.coe.int/en/web/cybercrime/glacyplus
[5] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Glacy

integrated in the future Convention. To that end we would like to highlight INTERPOL's appreciation for the recognition of the role of international and regional organizations in Article 53 paragraph 6 of the Zero Draft, and look forward to contributing further to this discourse.