Statement by INTERPOL at Third Session of the Ad Hoc Committee on Preventive Measures

CHECK AGAINST DELIVERY

Madam Chairperson,

Many Member States have highlighted the important role of international organizations and other multi-stakeholders in the prevention of cybercrime, which INTERPOL fully agrees. Prevention forms a key element of our global cybercrime strategy in order to reduce the harm caused to communities from cybercriminals.

To support Member States in answering the guiding questions, INTERPOL believes that there are broadly three areas that preventive efforts should focus on. We will give concrete examples of preventive measures in this context.

* * *

Firstly, strengthening the collection, analysis and exchange of cybercrime statistics and trends is key. Gaining a good understanding of the evolving scale, types, and impact of crime in cyberspace is the first step to developing effective counter measures. It is for this reason that INTERPOL, jointly with the Council of Europe and the European Union, published the Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence as part of the Global Action on Cybercrime Extended (GLACY+) project.

INTERPOL also provides research and analytical expertise. The INTERPOL Cyber Fusion Centre and our Lynx analytics platform ingest, aggregate, and analyze data from member countries, INTERPOL databases and private partners to generate actionable intelligence. Based on what national law enforcement and our private partners witness on the ground, INTERPOL also releases regular threat assessments of cybercrime emanating from or affecting countries.

INTERPOL further facilitates the sharing of information between countries through its global early detection and warning system, of which its Notices and Diffusions is a key component. Notably, member countries use INTERPOL’s Purple Notices to disseminate information about criminal modus operandi they have encountered, thereby alerting other member countries to deploy necessary prevention and mitigation techniques. For example, in March 2022, INTERPOL in collaboration with the Irish police released a Purple Notice on the deployment of Conti Ransomware against critical infrastructure and organizations globally.

* * *
Secondly, in response to question 37, raising awareness through public campaigns and educational programmes targets the human vulnerabilities element of the equation. Every year, INTERPOL organizes a global awareness campaign to provide the public with cyber hygiene advice. It aims to equip individuals and businesses with the knowledge on how to protect their systems and data.

The campaign in 2021 with the hashtag #JustOneClick – focusing on ransomware, online scams, phishing, and Business Email Compromise – reached over four million people online. More than 80 partnering countries, private companies, non-governmental organizations (NGOs) and international organizations joined hands to make this possible.

* * *

Lastly, public-private partnership is another important piece of the puzzle. In response to question 34, the private sector – including service providers, cybersecurity companies and Computer Security Incident Response Teams (CSIRTs) – can enrich our understanding of the cyberthreat landscape. INTERPOL’s Gateway initiative, endorsed by heads of national police at the INTERPOL General Assembly 2019, provides the legal framework for INTERPOL to exchange data with private partners in compliance with data protection standards.

Another good model is the World Economic Forum’s Partnership Against Cybercrime, of which INTERPOL is a member. The alliance of 50 global organizations and companies aims to address the challenge of cybercrime through close collaboration and collective efforts. Its Cybercrime ATLAS project, which maps out and analyses major cybercrime criminal groups, has demonstrated great success.

Chair, prevention of crime is a key element of policing; and as such, this chapter should be prioritized within this international cooperation.

Thank you.