Resolution No. 11

GA-2021-89-RES-11

Subject: Tackling global cybercrime threats through INTERPOL channels

The ICPO-INTERPOL General Assembly, meeting in Istanbul, Turkey, from 23 to 25 November 2021 at its 89th session:

BEARING IN MIND Article 2(1) of INTERPOL's Constitution, to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights,

RECALLING INTERPOL's General Assembly Resolution GA-2008-RES-07, which invited all member countries, through their National Central Bureaus, to extend access to the I-24/7 communications systems to their national cybercrime units, as well as INTERPOL's General Assembly Resolution GA-2012-RES-08, encouraging member countries to set up 24/7 contact points at their cybercrime investigative units,

FURTHER RECALLING INTERPOL's General Assembly Resolution GA-2014-RES-04 establishing the INTERPOL Global Cybercrime Expert Group (GCEG), which encourages it to take a multi-stakeholder approach to engage relevant institutions and encourage member countries to actively participate in the GCEG to share cybercrime information in a timely manner and facilitate cybercrime investigation across borders,

RECALLING also INTERPOL's General Assembly Resolution GA-2019-88-RES-11, which authorized, through the legal framework of Project Gateway, the receipt and sharing of data with private entities and urged member countries to enhance cooperation in combating cybercrime, *inter alia* by providing data for cybercrime analysis to INTERPOL,

CONSIDERING the threats posed by cybercrime and its exponential growth in scale and severity, coupled with the accelerated digitalization worldwide,

NOTING that the borderless nature of cybercrime necessitates enhanced and increased international law enforcement cooperation through INTERPOL's support, as well as partnerships with private entities and non-governmental organizations,

EMPHASIZING that the inherent transnational nature of cybercrime requires broad, global collaboration in sharing of information and *modi operandi* to enable a more effective response and action to counter such crimes,

BEARING IN MIND that in many global cybercrime cases, the analysis of cyber-information from multiple sources, including the resources of private entities, is of paramount importance in preventing and fighting cybercrime,

REAFFIRMING the value of INTERPOL in assisting law enforcement in member countries to identify and share intelligence leads, bridge information gaps and support the disruption of organized criminal networks who operate behind a range of cybercrimes that are often interlinked,

CONSIDERING INTERPOL's commitment to continued development of capabilities to help fight cybercrime and promotion of a multi-stakeholder approach to that end, through INTERPOL's Global Cybercrime Programme,

HIGHLIGHTING the value of utilizing INTERPOL's communication platforms and global databases for exchange and analysis of information pertaining to cybercrime, allowing for production of cyber analytical reports for member countries as well as assisting in better planning and coordination of cybercrime operations and action,

TAKING INTO ACCOUNT the INTERPOL High-Level Forum on Ransomware convened on 12 July 2021, bringing together member countries and INTERPOL Project Gateway Partners under the themes of Knowledge, Impact, Trust, Response and Actions, and welcoming the outcomes endorsed by the forum with the aim to create a global leadership framework for action to disrupt and mitigate the impact of cybercrime,

ENCOURAGES member countries to use INTERPOL's global network and capabilities in their efforts to prevent cybercrime, by raising awareness-, using partnerships and sharing information, to aim for preventive disruption of cybercrime through global law enforcement actions both reactively and proactively, to provide in-event emergency support against cyberattacks and ensure post-event support following any attacks to increase resilience, agility and responsiveness;

ENDORSES continued work by INTERPOL to broaden the network of partners within the framework of Project Gateway and conclude new agreements with private companies for exchange of information pertaining to cybercrime between INTERPOL and private entities under INTERPOL's Constitution and Rules on the Processing of Data (RPD);

URGES member countries to increase sharing and exchanging cybercrime data and information, in compliance with their respective national legislations and through INTERPOL's unique channels of communication as well as its capabilities and services in the fight against cybercrime in order to enable relevant analysis and action.

Adopted