INTERPOL's Comments - 6th meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime

1 INTRODUCTION

INTERPOL appreciates the opportunity to provide a written contribution on the Chapter 7 "International Cooperation" and Chapter 8 "Prevention" of the Draft Comprehensive Study on Cybercrime (hereafter, Draft Study) prepared by the UN Office on Drugs and Crime (UNODC) prior to the 6th meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

With the vision of connecting police for a safer world, INTERPOL supports 194 member countries in combatting all forms of transnational crime. As a neutral and global organization, INTERPOL enables law enforcement around the globe to share and access data on crimes and criminals, and offers a wide range of technical and operational support.

In today's highly digitalized world, cybercrime is one of the fastest growing crimes. Cybercriminals are developing and boosting their attacks at an alarming pace. According to INTERPOL's recent assessment, criminals are exploiting the fear and uncertainty caused by the unstable social and economic situation around the world due to the COVID-19 pandemic to launch cyberattacks.[1] At the same time, the higher dependency on connectivity and digital infrastructure due to the global lockdown has increased the opportunities for further cyber intrusion and attacks.

In June 2020, INTERPOL Cybercrime Directorate's Global Malicious Domain Taskforce has identified and analysed about 200,000 malicious domains affecting more than 80 countries. These domains were used for a wide variety of malicious activities exploiting the public's thirst for information during the pandemic. INTERPOL also identified a spike in online scams, phishing, ransomware, data-harvesting malware and misinformation related to COVID-19.[2]

In this context, collective efforts from law enforcement agencies need to be enhanced, particularly in information sharing and formulation of a joint operation framework to effectively tackle cybercrime. INTERPOL is uniquely positioned to lead the global law enforcement response to cybercrime together with member countries and its partners. This document outlines the views of INTERPOL on international cooperation and prevention of cybercrime and provides recommendations to reduce the global impact of cybercrime effectively.

[1] INTERPOL, *Factsheet on Global Landscape on COVID-19 Cyberthreats*, retrieved from https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

[2] INTERPOL, *COVID-19 Specialised Crime Report on Cybercrime.*

2 INTERNATIONAL COOPERATION

Cybercrime is borderless by nature and contains various technical components that could affect or involve multiple countries per incident. The Draft Study also notes cybercrime's transnational reach, which takes advantage of globalized information communication technology for committing criminal acts.[3] INTERPOL also shares the view stressed in the Draft Study that the increase in ubiquity of global connectivity presents a serious risk in terms of potential cyberthreats.[4]

INTERPOL's recent finding indicates that cybercriminals are being more targeted particularly amid the global pandemic.[5] To maximize damage and financial gain, cybercriminals are shifting their targets to businesses, governments and critical infrastructure, which play a crucial role in responding to the outbreak. Compounding a global health crisis with a sharp increase in cybercriminal activities related to COVID-19 is putting significant strains on the global law enforcement communities worldwide.

International police cooperation is needed more than ever, which is fundamental in keeping the highly interconnected world safe and secure. As recognized in the Draft Study, INTERPOL plays a unique role in facilitating police to police cooperation.[6] The role of INTERPOL is to connect member countries and share unique combination of cybercrime data, information and processing capacity to provide vital assistance in their investigations, and to enhance the understanding of global threats. There are a number of communication channels and tools that we utilize to foster international police cooperation as the following:

- **Connecting Police (National Central Bureaus)**

  As the Draft Study explained, INTERPOL has National Central Bureaus (NCB) hosted within every INTERPOL member country.[7] When a crime goes beyond their national jurisdiction, a country needs international support to detect, investigate, mitigate and prevent it. NCB connects their national law enforcement with other countries and with INTERPOL General Secretariat utilizing specialist capabilities, tools, skills, knowledge and coordination offered by INTERPOL. They seek the information needed from other NCBs to help investigate crime or criminals in their own country, and they share criminal data and intelligence to assist another country. NCBs are at the heart of INTERPOL and how we work.

- **I-24/7**

  INTERPOL developed the I-24/7 global police communications system to connect law enforcement officers in all our member countries. It enables authorized users to share sensitive and urgent police information with their counterparts around the globe, 24 hours a day, 365 days a year. It also enables investigators to access INTERPOL's range of criminal databases. Authorized users can search and cross-check data in a matter of seconds, with direct access to INTERPOL databases.

  National police can search our databases in real time as part of their investigations. This can be done via their INTERPOL National Central Bureau, or directly at the frontline, for instance by specialized crime units and border officials. Our member countries contribute data on a voluntary basis. This is subject to a strict legal framework and data protection rules in order to foster trust and ensure the quality of the information.

- **INTERPOL Purple Notices**

[3] Draft Study, p.4.
[4] Draft Study, p. 6.
[5] INTERPOL, retrieved from: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[6] Draft Study, p.195.
[7] Draft Study. p. 187.

INTERPOL published Purple Notices to provide information on modus operandi, objects, devices and concealment methods used by criminals. It is used to alert the global law enforcement community to emerging and high-risk cyberthreats. These global alerts, sent through the INTERPOL secured network, included the ransomware attacks against critical infrastructure and hospitals[8] and the use and dissemination of multiple malicious software in the first half of 2020.

INTERPOL Global Cybercrime Programme

To make the cyberspace safe and secure, INTERPOL launched a Global Cybercrime Programme within its Cybercrime Directorate based in Singapore in 2016. Its overarching goal is to support member countries in reducing the global impact of cybercrime and protecting communities for a safer world focusing on three core pillars of Cybercrime Threat Response, Cybercrime Operations and Cyber Strategy and Capabilities Development. The Programme responds effectively and proactively to our member countries' requests and needs in tackling cybercrime. Its main objectives involve:

- Develop a better understanding of the cybercrime threat landscape to help member countries prioritize their resources and capabilities against cybercrime threats;
- Continuously undertake and improve the collection, processing, storage, analysis, evaluation and dissemination of cybercrime data and information to support member countries in developing cyberthreat responses;
- Lead and coordinate operational activities with member countries in tackling cyberthreats that cause significant harm on a national, regional and global scale;
- Strengthen and enhance the cyber capabilities of member countries to enable them to prevent, detect and investigate cybercrime.

The Programme also puts great emphasis on Public-Private Partnership, which plays a pivotal role in achieving these objectives. In close collaboration with its private partners, the Programme ultimately supports member countries in understanding cyberthreats so as to help mitigate, prevent, detect and investigate cybercrime on a national, regional and global scale. To fulfil this, the Programme utilizes a number of effective tools and platforms such as:

- **INTERPOL Cyber Analytical Platform**

  The Cyber Analytical platform, known as Lynx, is an umbrella platform spanning tools for data ingestion, correlation and analysis of operational data in INTERPOL Cybercrime Directorate to form insights on cybercrime. This would enable our internal cybercrime officers and analysts to produce enriched actionable cybercrime information to fulfil operational objectives under INTERPOL's Global Cybercrime Programme. It will also enhance its cyber intelligence capability to provide more accurate and timely analytical products.

- **INTERPOL Cybercrime Collaboration Capabilities**

  Aiming at supporting police in obtaining, exchanging and disseminating actionable cybercrime intelligence, INTERPOL Cybercrime Directorate initiated the creation of cybercrime collaboration capabilities within the Cybercrime Pavilion of INTERPOL Global Knowledge Hub. Designated for the purpose of knowledge exchange[9] and operational coordination[10], these capabilities support member counties working on multi-stakeholder and multi-jurisdictional joint task forces to combat crimes against computer systems.

[8] INTERPOL, retrieved from: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[9] INTERPOL Cybercrime Knowledge Exchange was launched in the second quarter of 2020.

[10] INTERPOL Cybercrime Operation Exchange will be launched in the third quarter of 2020.

Its recent analysis projects that the global cyberthreat landscape is likely to continue to deteriorate. Despite this outlook, INTERPOL is taking proactive steps and all relevant measures to support member countries in an unprecedented crisis. The global pandemic has proved the importance of a global response in a collaborative and coordinated manner. The most urgent priority to address these growing cyberthreats is to further enhance international police cooperation for operational activities and to improve cybercrime information exchange with diverse partners within the global ecosystem of cybersecurity.

3 PREVENTION

Given the continued growth in the number of cybercrime globally, enforcement by itself is an inadequate solution; prevention is the key. INTERPOL seeks to strengthen partnerships, develop sound cybercrime strategy and promote good cyber hygiene empowering the communities to stay safe and prevent themselves from becoming victims of cybercrime.

- **Public-Private Partnership**

  Public-Private Partnership has been key to successfully mitigating and preventing emerging cyberthreats. The Draft Study also acknowledges the need for law enforcement authorities to collaborate with other stakeholders including private sector to increase reporting and for intelligence purposes.[11] INTERPOL is in full agreement with the statement and has been developing and nurturing its partnerships with various entities within the global ecosystem of cybersecurity. More specifically, INTERPOL member countries have endorsed a framework (Gateway) that enables INTERPOL to have data sharing agreements with private sector companies at the General Assembly in 2019. INTERPOL Cybercrime Directorate currently has 13 private partners, which share up-to-date cybercrime information and expertise on recent trends as well as provide technical assistance for law enforcement agencies. The direct access to data – from both the public and private sectors – allows its Cyber Fusion Centre to provide unique operational support and technical guidance to member countries. INTERPOL is also working closely with World Economic Forum to build an alliance against cybercrime gathering the law enforcement, private sector and civil society.[12]

- **Cybercrime Strategy**

  INTERPOL's recent survey identified the absence of a National Cybercrime Strategy (NCS) in a number of member countries. The finding underscores the necessity of developing and implementing NCS to build resilience of national infrastructure and services, which can help countries counter and prevent cyberthreats effectively as well as protect communities from data breaches. INTERPOL Global Cybercrime Programme currently oversees two projects outlined below focusing on the development of strategic capacity of member countries in combating cybercrime for the specific regions.

  ○ **ASEAN Cyber Capacity Development Project**: This project strengthens the ability of countries in the Association of Southeast Asian Nations (ASEAN) to combat cybercrime and work together as a region. The project also fosters regional strategic discussion, identifies trends and provides a foundation for improved information exchange. Comprising all 10 ASEAN member countries (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam), the project was initially funded for two years (2016-2018) by the Japan-ASEAN Integration Fund (JAIF) 2.0, via the ASEAN

[11] Draft Study, p.120.

[12] World Economic Forum, retrieved from: https://www.weforum.org/agenda/2019/11/why-public-private-partnerships-are-critical-for-global-cybersecurity/; https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/

Secretariat and with the Singapore Ministry of Home Affairs as the project proponent. The second phase (2019-2021) focuses on cybercrime strategy development, specialized cybercrime training and digital evidence.[13]

- **The Global Action on Cybercrime Extended (GLACY+) Project**: This project is a joint initiative of the European Union and Council of Europe to strengthen the cyber capacity of 12 priority countries in Africa, Asia-Pacific, and Latin America and the Caribbean. It builds upon the outcomes of the first GLACY project which concluded in 2016. The five-year (2017-2021) project is jointly implemented by the Council of Europe, which focuses on policies, legislation and prosecution; and INTERPOL, which focuses on the law enforcement aspects. Through the project, the participating countries will become catalysts for operational cooperation and strengthening the global fight against cybercrime. INTERPOL's role is to strengthen the capacities and operational skills of police in the participating countries to investigate cybercrime and engage in international police cooperation.[14]

- **Cybercrime Prevention: INTERPOL Global Awareness Campaigns**

In line with the United Nations Guidelines for the Prevention of Crime highlighting the importance of public education and awareness[15], INTERPOL Global Cybercrime Programme focuses on prevention of cybercrime and raising awareness through a series of global awareness campaigns. Through these campaigns organized in close cooperation with member countries and external partners, INTERPOL strives to empower the public to be safe on the Internet and keep good cyber hygiene. This also helps overcome the challenges faced by law enforcement authorities arising from underreporting of cybercrime by focusing on prevention. Based on INTERPOL's global outreach, it encourages the national law enforcement organizations in 194 member countries to share the key messages within their communities through social media platforms during the campaigns. The two most recent campaigns are summarized below.

- **Business Email Compromise Awareness Campagin #BECareful:** In October 2019, INTERPOL launched a month-long global awareness campaign on Business Email Compromise (BEC) called #BECareful during the 7th Europol-INTERPOL Cybercrime Conference. The aim was to inform the public about this growing type of fraud and provide information security and prevention tips for how to stay safe. To gain the widest global reach, INTERPOL has signed on police and financial authorities in around 60 member countries to support the campaign by sharing information on BEC fraud and using the #BECareful hashtag to start a global conversation. A number of private sector companies in the cybersecurity field, international organizations and non-profits are also supporting the campaign by sharing information on BEC cases, as well as on tools available to help members of public protect their systems from this threat.[16]

- **COVID-19 Cyberthreats Awarenss Camapgin #WashYourCyberHands:** The month long (May 2020) global awareness campaign was aimed at keeping communities safe from cybercriminals seeking to exploit the outbreak. The key message was to alert the public to the main cyberthreats linked to the coronavirus pandemic and to #WashYourCyberHands

[13] INTERPOL, retrieved from: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project

[14] INTERPOL, retrieved from: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/GLACY

[15] United Nations Guidelines for the Prevention of Crime, Economic and Security Council resolution 2002/13, Annex. Para.6 and 25.

[16] INTERPOL, retrieved from: https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-urges-public-to-BECareful-of-BEC-fraud

to promote good cyber hygiene. Each week had different theme (1) global landscape of COVID-19 cyber threats, (2) ransomware attacks, (3) online scams and phishing, and (4) threats against the remote workforce. The campaign was supported by member countries and 23 external partners. In total 21 languages were used to inform the public of the campaign's key messages and the visual materials and social media posts of the campaign developed by INTEPROL and its partners reached some 7.5 million users online. On Twitter (@INTERPOL_Cyber) alone, the campaign's hashtag of #WashYourCyberHands was mentioned about 10,000 times.

4 CONCLUSION

The impact of cybercrime is expected to rise as cybercriminals are becoming more sophisticated with the use of emerging technologies and taking a targeted approach. They are also taking advantage of the borderless playing field in the digital world and the challenges pertaining to national law enforcement structure to tackle cybercrime. Enhancing international police cooperation is therefore vital given the evolution of these transnational cyberthreats. The sharp increase in COVID-19 cyberthreats globally highlighted the importance of police to police cooperation more than ever. It also demonstrated that the future collaboration should cover a wide spectrum of innovative and holistic efforts to protect entire societies through raising public awareness, partnership with industry, security by default and cybersecurity automation.

With this in mind, INTERPOL will continue to support the national law enforcement authorities for cross-border cybercrime investigation, detection and prevention. As part of this effort, INTERPOL Global Cybercrime Programme leads global coordination of national and regional operations targeted against cybercrime threat actors and groups undertaking criminal activities online. Taking a regional approach, the Programme coordinates these operations in close cooperation with member countries, private and public partners as well as National Computer Emergency Response Team (CERT) communities.

Another urgent priority to address these growing cyberthreats is to foster Public-Private Partnership. Information sharing among the key actors within the global ecosystem of cybersecurity through partnerships based on trust is imperative in formulating timely and effective response to cybercrime. INTERPOL will further develop and diversify its partnerships to be able to identify, triage and develop actionable intelligence on identified threats to design disruption and prevention strategies that mitigate the high-risk and high-impact cyberthreats.

Further to this, INTERPOL will also support member countries in developing national cybercrime strategies, skills, knowledge and technical capabilities that are customized to their needs. Maximizing the use of INTERPOL's tools and platforms, it will enhance member countries' capacity and capabilities in combatting cybercrime globally. The INTERPOL global network will be also used for our continued efforts in prevention of cybercrime and raising awareness globally.

In response to the rapidly changing cybercrime landscape, INTERPOL works closely with member countries, private entities and many other stakeholders to reduce the global impact of cybercrime and protect communities for a safer world. INTERPOL also stands ready to contribute to the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime in support of the UN Member States.