Submission by INTERPOL to the Open-Ended Working Group on Security of and in the use of Information and Communications Technologies – May 2022

INTRODUCTION

As a Permanent Observer to the United Nations[1], the International Criminal Police Organization – INTERPOL makes this submission to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG).

INTERPOL's aim according to its Constitution is "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" [and] to establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes." INTERPOL is a neutral intergovernmental organization and is "forbidden […] to undertake any intervention or activities of a political, military, religious or racial character" (INTERPOL Constitution, Articles 2 and 3). INTERPOL's mission is "preventing and fighting crime through enhanced cooperation and innovation on police and security matters".

INTERPOL focuses on non-state threat actors when supporting its member countries and their competent law enforcement authorities. **This submission focuses on the areas of the OEWG's remit where INTERPOL plays a role as the global criminal police organization with 195 member countries**, and mainly on the work of INTERPOL on cyber issues as carried out through the INTERPOL Global Cybercrime Programme.

The submission is guided, as expressed in United Nations General Assembly resolution 76/19 (para. 5), by the final substantive report of the previous OEWG[2] and the consensus report of the Group of Government Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE)[3].

[1] See A/RES/51/1.
[2] A/75/816.
[3] A/76/135.

INTERPOL's submission to the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)[4] provides additional information relevant for the work of the OEWG.

THREATS

As stated in the final substantive report of the previous OEWG on this topic, there is a growing use of information and communications technologies (ICTs) for malicious purposes by non-state actors, including terrorists and criminal groups and that some of these non-state actors have demonstrated ICT capabilities previously only available to states (A/75/816, Annex I, para. 13).

Indeed, INTERPOL has in its own assessments found that the increased attack surface resulting from more work being done online has allowed cyber threat actors to exploit vulnerabilities. To maximize damage and financial gain, many criminals have shifted to targeting major corporations, governments and critical infrastructure. The ramifications of these attacks are therefore increasing, resulting in broader societal harm and deteriorating security, even at the level of effecting international peace and security such as cases of attacks on certain critical infrastructure or the difficulty in correctly identifying a cyber threat actor carrying out an attack.[5]

The continuing growth of cybercrime has been facilitated through the diversification of traditional crime syndicates as well as a specialization in the crime area that has enabled a Crime-as-a-Service model making cybercriminal tools more widely available to a broader array of threat actors. Through a networked and decentralized approach, cyber threat actors have been able to leverage more extensive and effective access to exploit for criminal purposes.

Cybercrime will continue to grow and harm communities and have the potential to indiscriminately spread instability for the foreseeable future. As a truly global and borderless crime type, this necessitates a broader international cooperation between authorities and private companies in all countries to counter this threat. INTERPOL strives to facilitate such collaboration.

NORMS

Of the eleven voluntary norms for the responsible behavior of states, as stated in the 2015 GGE report[6] with additional relevant notes in the 2021 GGE report, norms 13(c), 13(d) and 13(h)[7] are especially relevant for the work of law enforcement. **The support and assistance INTERPOL provides its member countries enables them to implement and live up to these norms**.

[4] INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf

[5] See also A/76/135 para. 14.

[6] A/70/174.

[7] - Norm 13(c): "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."

- Norm 13 (d): "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect."

- Norm 13 (h): "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty."

As the 2021 GGE report mentions in regards to norm 13(c), states "may consider seeking assistance from other States or the private sector" and mentions structures and mechanisms to formulate and respond to such requests (para. 30(b) of 2021 GGE report). In relation to norm 13(d) the report mentions the existence of structures and mechanisms that facilitates cooperation across borders, including between law enforcement (para. 32) and to further develop mechanisms that facilitate exchanges of information and assistance (para. 33) as well as developing "cooperative partnerships with international organizations, industry actors, academia and civil society" (para. 35).

INTERPOL connects its 195 member countries through the I-24/7 platform for secure information exchange between law enforcement agencies across the globe. Through this platform, member countries can seek and provide criminal intelligence and information, ask for assistance and exchange other information in relation to crime. This can be used for both bilateral and multilateral exchange between law enforcement agencies. In addition to the INTERPOL I-24/7 network, INTERPOL maintains information exchange and analysis files to assist in providing actionable intelligence to member countries on cyber threat actors through the Cyber Threat Response capability. INTERPOL also provides member countries with the tailored platforms Cybercrime Knowledge Exchange for general exchange of good practices, the Cybercrime Collaborative Platform for secured operational communications, and Cyber Fusion Platform for analytical purposes.

In addition to a Global Cybercrime Expert Group, INTERPOL also maintains a 24/7 points of contact list for cybercrime to be able to quickly reach responsible units in urgent cases or during ongoing cyberattacks. The organization also organizes several regional cybercrime working groups and heads of cybercrime meetings.

INTERPOL would like to emphasize the importance of using existing and established international mechanisms for secure information exchange. INTERPOL's platforms, databases and secure network are important existing, recognized and proven global mechanisms used by law enforcement. Four billion searches were conducted in INTERPOL's 19 databases in 2021 alone. In addition to this, INTERPOL's system of Notices and diffusions are essential tools used by law enforcement across the world in their work to prevent and investigate crime.

To enable a vital exchange of information with the private sector, INTERPOL has a legal framework called the Gateway Project that allows for such exchange with private entities, such as cybersecurity companies, through formal agreements and in line with rules on processing of data. Through this framework, INTERPOL is able to receive unique and important threat actor information from its partners that can be analyzed by the INTERPOL Cyber Fusion Centre in INTERPOL's cybercrime databases and produce relevant actionable intelligence products for dissemination to affected member countries where the competent authorities can initiate actions to prevent and disrupt cybercrime.

To reduce the operating space for online criminal activities[8] INTERPOL is actively supporting member countries to coordinate global cybercrime operations to disrupt and/or arrest cyber threat actors. This is done through a regional cybercrime operations desk model enabling closer collaboration and trust building between law enforcement agencies in a specific region.

CONFIDENCE-BUILDING MEASURES

As confidence-building measures are a manifestation of international cooperation, much of the work carried out by INTERPOL with its member countries contribute to fostering such confidence-building as well as trust between authorities in different countries. As noted above, INTERPOL can as a neutral interlocutor be a platform for technical exchange between countries, in many cases in spite of geopolitical differences that otherwise would have made such bilateral cooperation difficult.

[8] See para. 33 of the 2021 GGE report.

INTERPOL maintains points of contact networks for cybercrime at a technical level with law enforcement authorities in member countries. INTERPOL also organizes regional cybercrime working groups to enable more efficient cooperation on a regional level. **INTERPOL would like to highlight the need for better exchange and understanding between cyber "first responders", including national computer security incident response teams (CSIRTs) and law enforcement agencies, as well as with the diplomatic and political level (e.g. in cases of public attribution).**

CAPACITY-BUILDING

INTERPOL is actively engaged in capacity-building and providing technical assistance to member country beneficiary law enforcement agencies to equip them with the knowledge, skills and best practices needed to meet today's security challenges. These include training projects, good practices exchange, digital learning, courses, table-top exercises and workshops. INTERPOL also produces guidebooks such as on national cybercrime strategies and on electronic evidence. In its capacity-building work INTERPOL often partners with other organizations to enable a project tailored to the specific needs of the beneficiary.

For the OEWG process, it is important to stress the need for capacity-building pertaining to law enforcement as there exists a clear gap also between member countries capabilities. INTERPOL also encourages countries to develop analytical expertise concerning cybercrime as well as collection of cybercrime statistics and criminal data to understand the crime trends and what capabilities need to be strengthened.

REGULAR INSTITUTIONAL DIALOGUE AND OTHER ISSUES

INTERPOL sees a value in ensuring that the two major ongoing international cyber-related policy processes, i.e. the OEWG and the AHC – while covering different aspects of cyber issues – have adequate input pertaining to law enforcement cooperation, especially where the issues of cybercrime and international peace and security intersect. This can be done through formats such as common workshops, side events and informal dialogues. INTERPOL is open to support and facilitate such exchanges.

INTERPOL is actively involved in the AHC process and reiterates its main aims in the AHC process as they are also relevant to the work of the OEWG, namely 1) to enhance international law enforcement cooperation for a timely and effective global response to cybercrime, 2) to reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime, 3) to close gaps and bridge divides in capabilities, capacity and information sharing across the globe and 4) to maximize prevention efforts through public-private partnerships for proactive disruption of cyber threats.

CONCLUSION

As the global criminal police organization, INTERPOL is able to effectively engage with its 195 member countries' law enforcement organizations as well as foster connection and collaboration between these countries' authorities. The focus of INTERPOL is on non-state actors and ordinary law crimes, staying neutral and steering clear of issues of a political, military, religious or racial character. At the same time, the support INTERPOL provides its member countries contribute substantially to the capabilities and capacities of these countries and by extension their implementation of the norms of responsible state behavior in cyberspace.

The threat from cybercrime actors and the malicious use of ICTs will continue to grow at an exponential rate, involving enormous amounts of illicit gains as well as substantial harm to individuals and

companies as victims of cyberattacks. The potential to indiscriminately spread instability, not least through attacks in critical infrastructure, will also be a defining feature of this crime type for the foreseeable future.

INTERPOL makes the following points and recommendations for the consideration of the OEWG:

1. **A continued emphasis to use existing and established international mechanisms for secure information exchange and build and improve on these instead of only creating new global mechanisms. A thorough inventory of such mechanisms would be useful.**
2. **There is a need for better exchange and understanding between national cyber "first responders", including national computer security incident response teams (CSIRTs) and law enforcement agencies but also with the diplomatic and political level. Methods for this include national coordination mechanisms, but also increased confidence-building measures that include law enforcement and other first responders.**
3. **It is important for the OEWG to recognize the need for capacity-building also pertaining to law enforcement as there exists a clear gap in the capabilities also between many states.**
4. **States should be encouraged to develop analytical expertise concerning cybercrime as well as collection of cybercrime statistics and criminal data to understand the crime trends and what capabilities need to be strengthened.**
5. **Ensure that both the AHC and OEWG processes have adequate input pertaining to law enforcement cooperation, through formats such as informal dialogues between the two groups or inter-sessional consultations, workshops and side events. INTERPOL is open to support and facilitate such exchanges.**