<u>ECOWAS Commission Comments:</u> based on the Conference room paper prepared by the Secretariat on Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020

I. Introduction

The challenges associated with cybercrime in West Africa is enormous and cannot be over-emphasized, as it poses developmental and security challenges to the region and it is associated with poverty, violence, illicit drug trafficking, human trafficking, smuggling of firearms and light weapons, and other transnational organized crimes to mention a few.

Cybercrime continues to evolve and is a dynamically developing phenomenon in West Africa. In addition, the prevalence of the COVID-19 pandemic and the increase in use of information technology and the internet exacerbates the challenges encountered to effectively control cyber activities perpetuated by criminals.

We note the significant differences in the legal framework to address cybercrimes in the region, particularly in prosecution and punishment of offenders. Cyber criminals. Therefore, prefer to perpetuate their activities in countries regarded as having less penalties and "better" sentencing for imprisonment.

We therefore, call for a standardized legal instrument and harmonization of laws to accelerate the process of legal convergence that will effectively tackle cybercrime in the region. In addition, it is also necessary to strengthen intra and inter agency collaboration, judicial cooperation and enhance mutual legal assistance across Member States.

II. General Comments

The working document is all encompassing and touches on all issues of Cybercrime from prevention to the existing legal framework, extradition and capacity building to mention a few.

However, in the interest of transparency, all comments and recommendations from the Member States have been retained in the document and this causes a lot of repetitions in the document. It also weighs down the working document for the 7th meeting of experts.

Capacity building cuts across the 6 themes addressed during the last 3 meetings (2018 to 2020), namely:

1. Legislation and frameworks
2. Criminalization
3. Law enforcement and investigations
4. Electronic evidence and criminal justice
5. International cooperation
6. Prevention

Therefore, in formulating a final production of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice (CCPCJ), there should be a dedicated section on Capacity Building to avoid repetitions. This section should also contain the awareness/sensitization aspect and the need for countries to develop a cyber-culture / cyber hygiene.

III. Amendments & Comments (in red):

Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018

B. Incrimination

(k) Member States should use the Organized Crime Convention or any other instrument that can facilitate the sharing of information and evidence for criminal investigations relating to cybercrime, given the frequent involvement of organized crime groups in cybercrime;

Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019

B. Electronic evidence and criminal justice

(g) Member States should take necessary measures to enact legislation that ensures the admissibility of electronic evidence, bearing in mind that admissibility of evidence, including electronic evidence, is an issue that each country should address according to its domestic law;

Admissibility should not be address according to individual domestic law but adhere to a global standard.

Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 July 2020

A. International cooperation

(z) Member States should establish domestic regimes that make the sharing of "subscriber information", as defined in article 18, paragraph 3, of the Council of Europe Convention on Cybercrime, faster and more efficient;

Explore the possibility of utilizing other instruments that can fast track the information sharing.

(kk) If extradition is authorized, States should carry out effective extradition cooperation. If a requested State intends to refuse to extradite a cybercriminal suspect, it should, upon request, make every effort to consult with the requesting State, so as to give the requesting State the opportunity to express its opinion and provide information. A requested State should provide the grounds of refusal to the requesting State;

(tt) It was recommended that any elaboration of a new convention should be handled among the experts in UNODC in Vienna and resource persons, particularly from developing countries to take into account their needs.

B. Prevention

(ss) Measures should be strengthened with the aim of preventing the spread of hate speech, extremism and racism. These measures should include the very rapid removal of these contents.

INTERPOL's Comments on the Conference Paper compiling the conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020

1 INTRODUCTION

INTERPOL is the world's largest international police organization in support of 194 member countries. INTERPOL is entrusted with the mandate to facilitating cross-border law enforcement cooperation and, as appropriate, supports governmental and intergovernmental organizations, authorities and services whose mission is to prevent or combat crime − within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.

In today's highly digitalized world, cybercrime is one of the fastest growing and diversifying crimes. The increased reliance on the digital environment has provided profound criminal opportunities, targeting governments, individuals, businesses, key infrastructure and even hospitals. INTERPOL has witnessed a broad range of threats in the last year, including ransomware-based extortion, Business Email Compromise, illegal data-harvesting operations and the re-emergence of older types of malware, repurposed to take advantage of the global pandemic.

Compounding a global health crisis with a sharp increase in cybercriminal activities has put significant strains on the global law enforcement community. Furthermore, cybercrime investigations feature a number of challenges that are not experienced in the physical realm. For law enforcement, it is difficult to know first-hand that an attack has occurred, and even then reporting rates are low. Investigating cybercrime also takes specific skills and technology, which is not universally available, and cybercrime being inherently global is often detrimental to effective response with evidence and suspects located in multiple jurisdictions simultaneously.

International police cooperation is therefore vital in keeping the highly interconnected world safe and secure. As recognized in the Draft Comprehensive Study on Cybercrime, INTERPOL plays a unique role in facilitating police to police cooperation.[1] As a neutral and global organization, INTERPOL is uniquely positioned to lead and coordinate the global law enforcement response to cybercrime in cooperation with its member countries and partners. INTERPOL also enables law enforcement around the globe to share and access data on cybercrime and threat actors, and offers a wide range of expertise, technical and operational support.

[1] Draft Comprehensive Study on Cybercrime , p.195.

Based on its unique role, this document provides the views of INTERPOL on the conclusions and recommendations by the UN Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020. It underlines the importance of international police cooperation in addressing cybercrime and how INTERPOL could support the member countries in this respect.

2 MEETING OF THE EXPERT GROUP IN 2018

A. Legislation and frameworks

- INTERPOL supports the recommendations that recognize the importance of human rights protection in formulating legislation and legal frameworks. INTERPOL's Constitution ensures and promotes 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**.

- With respect to the fundamental rights mentioned in the paragraph 4(f), INTERPOL's **Rules on the Processing of Data** ensure the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels, with due respect for the basic rights of the persons who are the subject of this cooperation, in conformity with its Constitution.

- Access to critical **WHOIS data** is limited for law enforcement in the current regulatory environment. To support law enforcement in this key challenge, INTERPOL launched the design and the pilot testing of a new restricted portal, providing automated access to domain registration information to vetted law enforcement entities. Following the successful completion of the pilot phase of the system, INTERPOL is integrating this solution into its global police capabilities with the necessary legal agreements in place to expand the pool of private operators involved and open the system to the member countries.

B. Criminalization

- It is important to consider cyber-specific criminal legislation related to new criminal conduct associated with the misuse of information and communications technology as recommended in the paragraph 5(c). International efforts should continue to **harmonize criminalization** of core cybercrime offences taking into account widely recognized international standards as per paragraph 5(d) and in the context of the recent evolution of cyber criminality with use of new and emerging technologies as indicated in the paragraph 5(i).

- Member countries should bear in mind that the gaps in law enforcement cyber capacity across regions remain a fundamental enabler of crime networks to distribute their infrastructure and activities where risk is lower. The issue of underreporting of cybercrime also limits law enforcement's ability to assess the clear picture of the problem and effectively respond to it. This leads to an absence of cybercrime in prioritization within many law enforcement organizations across the globe which further exacerbates the challenges. Thus, it is important to create a safe environment based on trust for organizations, businesses and individuals to report suspicious activities and attacks in order to effectively identify, mitigate and investigate cybercrime.

- In terms of exchange of information among investigators referenced in the paragraph 5(l), INTERPOL offers a secure global police communications system called the **I-24/7**. It connects law enforcement officers in the member countries, enabling authorized users to share sensitive and urgent police information securely and in real time, available in INTERPOL's 4

official languages. It also allows investigators to access INTERPOL's range of 18 criminal databases to search and cross-check data in real time.

3 MEETING OF THE EXPERT GROUP IN 2019

A. Law enforcement and investigations

- Article 18, paragraph 13 of the Organized Crime Convention recognizes that "INTERPOL can be utilized in urgent circumstances as a communications conduit for mutual legal assistance should the need arise".[2] This underlines the importance of INTERPOL's unique capacity to be a single focal point for law enforcement across 194 countries. In support of the recommendation in the paragraph 6(c), INTERPOL could help facilitate the sharing of information or cybercrime investigation with the use of its network, tools and platforms.

- INTERPOL delivers policing capabilities in preventing, detecting and investigating cybercrime to all member countries through its **Global Cybercrime Programme,** which was adopted by the INTERPOL General Assembly. Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the Programme develops and leads the global law enforcement response to reduce the cybercrime threats that pose the highest risk and the most harm to communities. It has three core pillars of (1) cybercrime operations, (2) cybercrime threat response and (3) cyber strategy and capabilities development.

- In terms of cybercrime operations and investigative support, INTERPOL takes **a regional approach** for global coordination of operations targeted against cybercrime threat actors and groups undertaking criminal activities online. Reflecting the unique challenges and needs within the regions, it provides tailored operational support to help member countries prevent, detect and investigate cybercrime. The regional desks for joint operations against cybercrime are currently in development including for Africa, the Americas, Asia, Europe, and Middle East and North Africa. The ASEAN Cybercrime Operations Desk which was established in 2018 with support from the Singapore Government and the Japan-ASEAN Integration Fund (JAIF) 2.0 will be expanded to cover a wider Asian region.

- In terms of platforms, INTERPOL's **Cyber Fusion Platform** is an umbrella platform spanning tools for data ingestion, correlation and analysis of operational data to form insights on cybercrime. This enables INTERPOL to produce enriched actionable cybercrime information and enhance its cyber intelligence capability to provide more accurate and timely analytical products. Aiming at supporting police in obtaining, exchanging and disseminating actionable cybercrime criminal intelligence, INTERPOL also created **Cybercrime Knowledge Exchange** and **Cybercrime Collaborative Platform – Operations** to support member countries working on multi-stakeholder and multi-jurisdictional joint operational teams to combat crimes against computer systems.

- As recommended in the paragraph 6(q), INTERPOL encourages to foster **public-private partnership**. In 2019, INTERPOL member countries have endorsed a framework (Gateway) that enables INTERPOL to have data sharing agreements with private sector companies. INTERPOL currently has 12 private partners under this framework which share up-to-date cybercrime information and expertise on recent trends as well as provide technical assistance for law enforcement agencies. The access to data – from both the public and private sectors – allows INTERPOL to provide unique operational support and technical guidance to member countries.

[2] https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf

B. Electronic evidence and criminal justice

- INTERPOL is committed to addressing the challenges pertaining to the access to electronic evidence by judicial and police authorities across the globe. In line with the recommendation in the paragraph 7(v), INTERPOL published the **Guidelines for Digital Forensics First Responders** which offers guidance for identifying and handling electronic evidence through methods that guarantee their integrity. INTERPOL also developed the **Global Guidelines for Digital Forensics Laboratories** that outlines the procedures for establishing and managing a Digital Forensics Laboratory and provides technical guidelines for managing and processing electronic evidence.

- In 2018, INTERPOL proposed the **e-MLA Initiative** to its member countries with the aim to foster effective international cooperation in criminal matters by providing the competent national authorities of all member countries with a transmission capability for requests seeking judicial assistance in cross-border cases. This initiative requires financial support from the member countries which will help fulfil the recommendations provided in the paragraphs 7(d) and 7(h).

- In line with the recommendation in the paragraph 7(b), INTERPOL delivers projects to support member countries to enhance their cyber skills, knowledge and technical capabilities that are customized to their needs, in line with INTERPOL standards. As indicated in the paragraphs 6(e) and 6(f), member countries are also encouraged to support INTERPOL to deliver capacity building and capabilities development projects for law enforcement. The ongoing projects include the following:

    - **ASEAN Cyber Capacity Development Project**: This project strengthens the ability of countries in the 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 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.[3]

    - **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 15 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.[4] Under this project, INTERPOL has published **Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence** to help criminal justice authorities worldwide acquire the statistics on cybercrime and electronic evidence by providing good practices and recommendations.[5]

[3] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project
[4] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/GLACY
[5] https://www.interpol.int/en/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf

4 MEETING OF THE EXPERT GROUP IN 2020

A. International cooperation

There is a need for greater and more efficient **international police cooperation** particularly in tackling cybercrime in a highly interconnected world. In particular, cybercrime investigations often rely on cross-border data exchange and transnational coordination. Therefore, INTERPOL recommends to increase the use of **I-24/7** secure communication which fosters **trust in police communication** and provides an added security value for international cooperation. INTERPOL's **Cybercrime Knowledge Exchange** and **Cybercrime Collaborative Platform – Operations** will also help achieve the effective communications and operational exchanges. INTERPOL will further put efforts in enhancing the **rules of data protection** on a global scale through INTERPOL National Central Bureaus in all member countries.

- To further elaborate on the recommendations in the paragraphs 8(c) and 8(t), INTERPOL maintains the **Regional Working Groups of Heads of Cybercrime Units** and **INTERPOL Global Cybercrime Expert Group** to increase the efficiency of international police cooperation in combating cybercrime. INTERPOL also maintains and updates the list of **INTERPOL 24/7 Contact Point for computer-related crime** to ensure that the information exchanged through the appropriate INTERPOL channels reaches the national cybercrime units with the least possible delay. The Contact Points are an essential prerequisite for the establishment of the early warning system.

B. Prevention

- Given the continued growth in the number of cybercrime globally, enforcement by itself is an inadequate solution; prevention is the key. As indicated in the paragraph 9(i), **Public-Private Partnership** is essential to successfully mitigate and prevent ever-evolving cyberthreats. In this context, INTERPOL seeks to strengthen partnerships with diverse actors in the global ecosystem of cybersecurity. INTERPOL is also collaborating with World Economic Forum to build an alliance for the Partnership Against Cybercrime initiative gathering the law enforcement, private sector and civil society.[6]

- As stressed in the paragraph 9(x), collecting a broad range of **data** is fundamental in shaping cybercrime policies and operational responses to combat cybercrime. INTERPOL builds cybercrime threat response leveraging on private partners' expertise and cybercrime data. It provides quality advice and actionable intelligence, as well as the evidentiary opportunities to operations. For instance, INTERPOL is currently working with CERTs to stop open resolvers and provide prevention strategies to the relevant member countries.

- In line with the United Nations Guidelines for the Prevention of Crime highlighting the importance of public education and awareness[7], INTERPOL focuses on prevention of cybercrime and raising awareness through a series of **global awareness campaigns**. In close cooperation with member countries and external partners, INTERPOL empowers the public to be safe on the Internet and keep good cyber hygiene. The recent campaigns include #BECareful on Business Email Compromise (October 2019), #WashYourCyberHands on COVID-19 cyberthreats (May 2020) and #OnlineCrimeIsRealCrime (October 2020) under the Cybercrime Capacity Building Project in the Americas funded by the Government of Canada.

[6] https://www.weforum.org/reports/partnership-against-cybercrime

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

5 CONCLUSION & WAY FORWARD (incl. relevant information in relation to the future work of the expert group)

The impact of cybercrime will continue to rise as cybercriminals are diversifying and taking a targeted approach. They are also exploiting 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 imperative given the evolution of these transnational cyberthreats**. In addition, the sharp increase in COVID-19 cyberthreats globally highlighted the importance of police to police cooperation more than ever.

To this end, INTERPOL will continue to coordinate and support the national law enforcement authorities for **cross-border cybercrime investigation** and **exchange of data**. As a neutral and global data aggregator, INTERPOL will **host multiple data sources** on its Cyber Fusion Platform related to cybercrime and victim datasets from police, private partners and open source intelligence. **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.**

Going forward, law enforcement needs to position itself as a willing partner in a global effort between member countries, and between the public and private sector. **Partnerships** based on trust within the global ecosystem of cybersecurity will be a deciding factor in formulating timely and effective response to cybercrime. In this sense, INTERPOL will further develop, enhance and diversify its partnerships to mitigate the high-risk and high-impact cyberthreats.

In the face of the rapidly changing cybercrime landscape, INTERPOL stands ready to support the member countries; and contribute to the future work of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

INTERPOL's Proposal for Amendments

[PAGE 4] 4(o) UNODC should seek synergies and cooperate closely with other stakeholders or organizations such as the Council of Europe, INTERPOL and the Organization of American States (OAS) in the field of capacity-building programmes on combating cybercrime to ensure that activities and initiatives in this area are not dispersed or fragmented;

[PAGE 4] 4(r) Member States should evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on a regular basis, with substantive contributions by Member States, an assessment of cybercrime trends, taking into account INTERPOL's cybercrime threat assessment;

[PAGE 4] 4(u) Existing legal instruments and mechanisms, including the United Nations Convention against Transnational Organized Crime and INTERPOL, should be taken advantage of by as many States as possible to strengthen international cooperation;

[PAGE 6] 5(l) Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7 and making use of INTERPOL channels;

[PAGE 6] 5(o) Member States should identify trends in the activities underlying cybercrime through research and should further evaluate the possibility and feasibility of mandating the Expert Group, UNODC and INTERPOL to conduct and make available on an annual basis, with substantive contributions by Member States, an assessment of cybercrime trends;

[PAGE 7] 6(c) In view of the transnational nature of cybercrime and the fact that the large majority of global cybercrimes are committed by organized groups, Member States should also make greater use of the United Nations Convention against Transnational Organized Crime and INTERPOL to facilitate the sharing of information and evidence for criminal investigations relating to cybercrime;

[PAGE 7] 6(f) States are encouraged to continue to provide UNODC with the necessary mandates and financial support with a view to delivering tangible results in capacity-building projects together with other partner organizations such as the Council of Europe, INTERPOL and OAS in that area;

[PAGE 7] 6(i) Given that cybercrime requires medium- and long-term law enforcement strategies to disrupt cybercrime markets, including cooperation with international partners such as INTERPOL, those strategies should be proactive and preferably target organized cybercriminal groups, which may have members in numerous countries;

[PAGE 8] 6(q) Member States should foster public-private partnerships to combat cybercrime, including through the enactment of legislation and the establishment of channels for dialogue for that purpose, in order to promote cooperation between law enforcement authorities, communication service providers and academia with a view to enhancing knowledge and strengthening the effectiveness of responses to cybercrime, reflecting INTERPOL's Gateway framework to share information with the private entities on cybercrime;

[PAGE 10] 7(m) Through the Global Programme on Cybercrime, UNODC and other partner organizations such as the Council of Europe, INTERPOL and OAS should promote, support and implement, as appropriate, technical cooperation and assistance projects, subject to the availability of resources. Such projects would bring together experts in crime prevention, computer security, legislation, prosecution, investigative techniques and related matters with States seeking information or assistance in those areas;

[PAGE 11] 7(vi) Utilization ~~Development~~ of a network of contact points between law enforcement authorities developed by INTERPOL, judicial authorities and prosecutors;

[PAGE 12] 7(v) States are encouraged to strengthen capacity-building for the collection of electronic evidence, create professional teams equipped with both legal and technical expertise and enhance experience-sharing and training cooperation in that regard. UNODC and other relevant organizations such as INTERPOL are encouraged to play a role in those efforts;

[PAGE 14] **8(e)** The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation, as well as channels of communication through liaison officers and information technology systems, such as INTERPOL, between national authorities for the cross-border collection of evidence and online transfer of electronic evidence;

[PAGE 16] **8(ii)** A formal arrangement with organizations such as INTERPOL, the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre, the Cyber Crimes Center of the United States of America, the Japan Cybercrime Control Center and the National Cyber Security Centre of the United Kingdom of Great Britain and Northern Ireland will be helpful in sharing information related to the latest cybercrime threats, modi operandi, emerging technology for cybercrime investigations and access to each other, best practices, etc.;

[PAGE 17] **8(pp)** UNODC and other partner organizations such as the Council of Europe, INTERPOL and OAS are encouraged to further provide capacity-building and training programmes in combating cybercrime to national governmental experts to strengthen capacities to detect and investigate cybercrime. Such capacity-building should address the needs of developing countries, focus on the vulnerabilities of each country in order to provide tailor-made technical assistance and promote the exchange of the most up-to-date knowledge in the best interests of practitioners and stakeholders;

[PAGE 18] **8(ggg)** For acquiring data to conduct investigations in relation to cybercrime acts, States should make wider use of INTERPOL's channels and capabilities and build on tried-and-tested international instruments, as such investigations are complex and require an institutional framework that has proved its resilience and added value.

[PAGE 19] **8(kkk)** States should establish a quick-response mechanism and communication channel for judicial assistance and law enforcement cooperation in combating cybercrime, especially through INTERPOL channels, and consider enabling the online exchange of legal documents and electronic evidence, supported by electronic signatures and other technical means;

[PAGE 20] **9(o)** Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities such as raising awareness about the risks of cybercrime, targeting such campaigns at modi operandi such as phishing or malware ("ransomware") and at different groups such as youth and elderly people. Member States are also encouraged to continue to focus on the likelihood of prosecution and punishment of offenders and efforts to prevent crime by identifying and disrupting ongoing illicit activities online. Police and public prosecution services should invest in signalling, detecting and reacting to cybercrime threats in collaboration with INTERPOL. Public-private partnership is indispensable. These prevention activities do not require extra laws or regulations;

[PAGE 21] **9(aa)** Member States should avail themselves of capacity-building assistance from the UNODC Global Programme on Cybercrime and other initiatives, including the Council of Europe Global Action on Cybercrime Extended programmes and INTERPOL Global Cybercrime Programme;

[PAGE 22] **9(mm**) It was recommended that a global database on cryptocurrency abuses and the exploitation of data by criminals on a large scale should be created, taking into account the existing systems and platforms within INTERPOL, as well as a globally coordinated strategic overview of the threats posed by criminal offences committed on the darknet;

[PAGE 22] **9(nn)** Regional and international initiatives aimed at strengthening cybersecurity should be encouraged, in particular the exchange of information on large-scale cyberattacks through INTERPOL channels;

[PAGE 22] **9(oo)** States may consider establishing an international cyberthreat information - sharing system to share and study the technologies and modi ope randi of new threats, acknowledging the existing systems within INTERPOL;

[PAGE 22] **9(rr)** National, ~~and~~ regional and international prevention experiences should be brought together to create a multilateral repository that would allow the dissemination of good practices in diverse contexts utilizing INTERPOL's cybercrime capabilities.

[PAGE 22] **9(uu)** Capacity-building and cooperation should be provided for the prevention of cybercrime with other regional and international actors and organizations (such as INTERPOL and OAS) and with multi-stakeholder forums such as the Global Forum on Cyber Expertise;

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Comments to the Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020

Kaspersky Position Paper

March 2021

Introduction

Kaspersky supports the Open-ended intergovernmental Expert Group, which is convened to conduct a comprehensive study of the problem of cybercrime. The group is tasked to conduct the important work for addressing the problem of cybercrime and for identifying responses to it through exchanging information with the international community, including the private sector. We also share the principles of the Group to encourage the exchange information on best practices, national legislation, technical assistance and international cooperation to examine the current responses and strengthen them, where needed.

Before the seventh session of the Open-ended intergovernmental Expert Group, we are grateful for the opportunity to provide our comments to the preliminary conclusions and recommendations as suggested by Member States during the meeting of the Expert Group held in Vienna from 27-29 July 2020 (UNODC/CCPCJ/EG.4/2020/2) (*further* – the 2020 report).

<u>Section A on International cooperation</u>

Paras recommending establishing new mechanisms for international cooperation, points of contact

We note the following recommendations on:

- establishing rapid response mechanisms for international cooperation, as well as channels of communication through liaison officers and information technology systems between national authorities (para ‘e’);
- setting up a genuine 24/7 point of contact at State level (para ‘u’); and
- investing or establishing a strong central authority for international cooperation in criminal matters (para ‘hh’);
- establishing specific units to investigate cybercrime (para ‘hh’);
- considering establishing separate cybercrime units within central authorities for mutual legal assistance (para ‘ddd’), and
- establishing a quick-response mechanism and communication channel for judicial assistance and law enforcement cooperation (para ‘kkk’).

Given that the Section A does not include thematic sub-sections, the presence of multiple recommendations calling for creating new mechanisms for international cooperation seem overlapping.

kaspersky

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

We would recommend simplifying and harmonizing, where possible, these recommendations to provide a clear institutional framework at the international level for combatting cybercrime and exchanges of information. The streamlined and clarified institutional framework would help avoid multiple contact points and thus would not create administrative barriers to exchange of information. The clear framework and clearly designated contacts of point at State level will be also very helpful for the private sector, including cybersecurity researchers, and technical community to identify the right people for providing assistance in investigation of cybercrime or ICT-enabled crime.

Additionally, for the seventh meeting, it would be helpful for the international community to have a clear understanding how recommendations, to be produced by the Expert Group, relate to the recently adopted the UN Open-Ended Working Group (OEWG) consensus report A/AC.290/2021/CRP.2[1]) which contains a recommendation, in the section on Confidence-Building Measures (CBMs), for States to consider nominating a national Point of Contact at the technical, policy and diplomatic levels.

Paras recommending considering the improvement of mechanisms and the creation of new protocols for the exchange of information, including intelligence and evidence of criminal acts

In the same vein, we note multiple paras calling for improvement of mechanisms or for the creation of new mechanisms for cross-border information sharing. These paras include recommendations on:

- considering the creation of innovative protocols for the exchange of information, including intelligence and evidence of criminal acts (para ‘g’);
- working towards standardizing and disseminating procedural tools for the expedited production of data and extending searches (para ‘ff’);
- facilitating the development and standardization of interoperable technical standards for digital forensics and cross-border electronic evidence retrieval (para ‘gg’); and
- considering enabling the online exchange of legal documents and electronic evidence, supported by electronic signatures and other technical means (para ‘kkk’).

Given that the Section A does not include thematic sub-sections, the presence of multiple recommendations calling for creating new mechanisms for international cross-border information exchange seem overlapping.

We would recommend uniting these conclusions/recommendations into a harmonized single para with clarifying details that strengthened mechanisms for information sharing can include, but not limited to creation of protocols, standardizing and disseminating procedural tools, developing interoperable technical standards and enabling the online exchange of legal documents and electronic evidence. This would provide a greater clarity to the international community on conclusions of the Expert Group and, therefore, would help to enable a more effective implementation.

[1] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

kaspersky

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Para recommending strengthening cooperation to protect critical infrastructure

The 2020 report also includes the para recommending to States to continue strengthening cooperation to protect critical infrastructure (para 'f'). We would like to suggest providing a clarification how this recommendation relates to the 2015 UN GGE (A/70/174[2]) non-binding norms on critical infrastructure protection (norms 'f' and 'g') as well as to the recently adopted the UN OEWG consensus report (A/AC.290/2021/CRP.2[3]), which contains the similar recommendation in para 31.

We would also recommend considering an additional provision encouraging and/or clarifying the role of the private sector in the critical infrastructure protection and in strengthening the collaboration with computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) in the event of a significant cyber ICT incident affecting critical infrastructure located in one State or across several States' jurisdictions.

Paras recommending addressing challenges of attribution and facilitating of the development and standardization of interoperable technical standards for digital forensics and cross-border electronic evidence retrieval

The 2020 report recommends countries to address the challenges of attribution and capacity to investigate cybercrime cases (in para 'ee') as well as to facilitate the development and standardization of interoperable technical standards for digital forensics and cross-border electronic evidence retrieval (in para 'gg'). We support both these paras and seem them interconnected. At the same time, we would like recommend an additional provision clarifying and encouraging a development of universally accepted methodology/methods for technical attribution and technical malware analysis within efforts to standardize interoperable technical methods for digital forensics.

Paras recommending public-private partnerships and cooperation with the multi-stakeholder community, including private sector, technical community and academia

We are pleased to note numerous paras in the report recommending strengthening public-private partnerships and cooperation with non-State actors for combatting cybercrime or ICT-enabled crime. These recommendations are expressed, particularly, in paras 'n', 'p', 'r', 's', and 'bbb'.

Additionally we would like to recommend strengthening the participation of non-governmental organizations, including the private sector and cybersecurity researchers, academia and technical community, by encouraging their support or contribution to resolving existing challenges in combatting cybercrime or ICT-enabled crime in paras: 'bb', 'cc', 'gg', 'll', 'nn', and 'lll'. Particularly, we would firmly support clear encouragement and mentioning of non-State or non-governmental actors or organizations in implementation of these recommendations (paras).

[2] https://undocs.org/A/70/174
[3] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

kaspersky

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Para recommending the exchange of information between States

We support the recommendation in para 'y' on enhancing synergies for the collection and sharing of information between States. Recalling the recommendation for States within the UN OEWG consensus report (A/AC.290/2021/CRP.2) on sharing relevant information, including through the Cyber Policy Portal of the United Nations Institute for Disarmament Research (para 50), we would recommend considering the same conclusion, in the report after the seventh meeting, calling for both exchange and transparency in States' approaches and States' laws on combatting cybercrime. This information can be also collected at the central hub of information (e.g. the UNIDIR Cyber Policy Portal).

Additionally, as a separate recommendation, we would support the efforts, perhaps within the seventh meeting or beyond, to align the use of terminology and definitions relating to cybercrime.

Section B on Prevention

For the Section B we would like to suggest the following additional areas for a further consideration by the Expert Group:

(1) When developing more structured global technical and operational cooperation, it is important to ensure that CERTs/CSIRTs remain neutral – the same way that, for example, firefighters focus on extinguishing a fire, not on attribution or chasing arsonists. We would support this recommendation/conclusion on the necessity of the neutral status for CERTs/CSIRTs in investigations of cybercrime or ICT-enabled crime.

(2) Where principles and norms of responsible State behavior in cyberspace is discussed (as it is in para 'u'), we would recommend providing a clarification on how it relates to the mentioned-above 2015 UN GGE[4] and 2021 UN OEWG[5] consensus reports. This would provide a harmonized and consistent international framework to the international community.

(3) Where necessary to collect, process, and exchange data on incidents, as it is expressed in paras 'x', 'ff', 'jj', we would welcome an explicit encouragement of the non-governmental/non-State actors' participation, including the private sector and cybersecurity researchers, for both developing tools and implementing frameworks leading to a more effective information sharing.

(4) As a measure preventing cybercrime or ICT-enabled crime, we would welcome the consideration to add a separate conclusion recommending responsible reporting of ICT vulnerabilities and establishing coordinated vulnerabilities programs.

[4] https://undocs.org/A/70/174

[5] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Conclusion

We hope that these comments will be helpful to the seventh meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime. We at Kaspersky will continue to support the work of the Expert Group and, if any further information or expertise is needed, would be glad to provide such support to the UN Member States and global community, including other stakeholder groups, at large.

Microsoft response to the Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020

Microsoft would like to commend the United Nations (UN), and in particular the Expert Group to Conduct a Comprehensive Study on Cybercrime, for the transparency of their work in terms of the Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of said Expert Group in 2018, 2019 and 2020. We further welcome the invitation for interested stakeholders to provide comments on this document. Microsoft has followed the discussions in this group with interest. We were also honored to participate in the sixth meeting, which took place in 2020.

Microsoft is a strong advocate for multistakeholder diplomacy in this space. By way of example, and in the spirit of cooperation among all relevant stakeholders, we have also shared our thinking on multistakeholder inclusion with other UN entities discussing various aspects related to threats emanating from cyberspace. In this respect, we would like to reiterate that recommendations we offered in 2019 as well as more recently, remain valid. It is in the same spirit, that we are now taking this opportunity to share our thoughts on this Compilation.

While respectful of the unique responsibility governments have in matters of security, the inherently shared nature of cyberspace requires collaboration between and across stakeholder groups to protect the safety and integrity of the online world. To that end, we appreciate efforts to seek out and include the perspectives from all relevant stakeholders in these matters.

Before going into more detail below, we would like to specifically agree that options to counter cybercrime and to protect societies must always ensure the protection of human rights as well as privacy and promote a free, open, secure and resilient cyberspace for all.

Multistakeholder input & public-private partnerships

Looking at the evolution of recommendations and conclusions over between 2018 and 2020, we are encouraged by the increasing recognition of the importance of multistakeholder input and the need for effective public-private partnerships. No single actor is equipped to effectively and sustainably deal with the diversity and sophistication of threats in cyberspace today, let alone tomorrow. Cooperation among all relevant stakeholders is therefore crucial and we call on states to further prioritize multistakeholder cooperation and inclusion – including at future cybercrime related discussions and negotiations at the UN, such as the open-ended ad hoc intergovernmental committee of experts, established pursuant to General Assembly resolution 74/247.

Moreover, we strongly agree with calls that non-governmental organizations and academia must also form part of the effort to prevent and counter cybercrime, as they provide an inclusive, multifaceted and comprehensive perspective to, inter alia, ensure the protection of human rights, especially freedom of expression and privacy. In addition, we also particularly support calls for increased collaboration between the public and the private sectors in terms of protecting critical infrastructure and sectors that are particularly vulnerable, such as the health sector, especially during the current pandemic.

Importance of leveraging existing and well-functioning frameworks

Both the threats and damage caused by cybercrime continue to grow. Informed by over 8 trillion daily security signals and observations from our security and threat intelligence experts, Microsoft's Digital Defense Report 2020 presented telemetry and insights about the current state of cybersecurity. To deal with this reality, it is crucial to act right *now*, leveraging existing tools and frameworks that are functioning well, rather than advocate for a new instrument.

In addition to being the most comprehensive international agreement on cybercrime and electronic evidence to date, the Budapest Convention provides an unparalleled legal framework for international cooperation on cybercrime. Microsoft agrees with calls supporting the use and utility of the Budapest Convention and we encourage more States to sign and ratify the Convention and its provisions. In this respect, we would note that the 20th anniversary of the Budapest Convention in 2021 and the forthcoming adoption of its "Second Protocol" provide a particularly timely opportunity to join this landmark Convention.

Importantly, we also agree that any potential new instrument should not conflict with existing instruments, which already enable real-time international cooperation for many and that, therefore, States should ensure that any new instrument on cybercrime avoids conflict with existing treaties.

Human rights

Respecting human rights is a core value of Microsoft. It is inseparable from our mission to empower every person and every organization on the planet to achieve more with our technologies. We believe that people, organizations, and societies will only use technologies they trust, and they will only trust technologies that respect their rights and advance human dignity, agency, and wellbeing.

At the same time we do recognize the need to balance human rights with security concerns, and we were welcome the references in the recommendations that reflect that equilibrium. When developing and implementing cybercrime legislation, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy, and should uphold the principles of legality, necessity and proportionality in criminal proceedings relating to the fight against cybercrime.

Capacity-building & awareness raising

Microsoft strongly supports the recommendations related to increased and improved capacity building. We also support the related notion of raising awareness of all relevant stakeholders and decision makers. We particularly share the concerns of the international community that vulnerabilities may be amplified in times of crisis (such as the current global pandemic), and therefore support calls for the immediate increase of investments in capacity building globally to ensure the global community – irrespective of sector – will be able to weather any significant online storm. In doing so, the expertise, experience and resources of all relevant stakeholder groups should be leveraged.

At the same time, we encourage the Member States to adopt a set of principles to guide capacity building efforts. Based on our experience in this field, we believe the following framework would substantially help improve capacity building outcomes:

1) Understand the need. Capacity building efforts can only succeed if they are responding in a targeted way to a real need. They therefore need to begin with participants' understanding of what issues matter to them and why, as well as with an understanding of where they have gaps in capacity or capability. Inevitably, these needs will vary depending on regional or local context.
2) Develop an all of government approach. All too often, capacity building efforts focus on the technical aspects of cybersecurity at the expense of others – diplomatic, judicial,… etc. Against the background Microsoft believes is excited to read the references to different sets of capacity building initiatives, and encourages States to also consider local civil society and private industry in their efforts.
3) Be culturally responsive and ensure initiatives locally owned. While we increasingly all connect to the same public Internet, the ways in which we use modern technology and the way we learn new information is heavily influenced by local customs and cultures. With this in mind, it is critical that capacity building efforts consider the local context and ensure that recipients are bought into the process.

4) Maintain relevance of capacity building. Technology is evolving rapidly, and it is important to ensure that capacity building efforts move with the times. Trainings should therefore strive to incorporate understandings of the latest technologies. Even more importantly, capacity building needs to be treated as a continuous process, rather than a one-off engagement.
5) Be inclusive of all stakeholders. It is critical that capacity building focuses not just on government stakeholders, but industry and civil society as well. Moreover, effective cybersecurity capacity building programs also rely on the support of government stakeholders as well as industry and civil society organizations with relevant expertise to develop trainings, exercises, and other initiatives. This essential multistakeholder dynamic in capacity building – in both delivering and receiving – should therefore be recognized in any guidance produced on the subject.

Finally, we are also encouraged by recommendation that highlight some of the important work on capacity building that is already underway by numerous actors around the world, including international organizations, regional and sub-regional bodies, civil society, the private sector, and academia. We nevertheless note the call for reflection on how to promote coordination, sustainability, effectiveness and reduction of duplication across these efforts. We agree with this sentiment and would like to stress the importance of complementing and leveraging existing efforts such as, in this context, the work done by the Global Forum for Cyber Expertise (GFCE).

Ongoing negotiations at the United Nations

As mentioned above, to deal with the growing threats and damage caused by cybercrime it is crucial to act right now, leveraging existing tools and frameworks that are functioning well, rather than advocate for a new instrument. As such, we urge Member States to ensure that negotiations on any potential new instrument (a) are chaired by a neutral party, (b) that they are governed by consensus, and (c) that the discussions take place in a venue that is conducive to fostering and delivering the best possible *expert* discussions – and that, in this respect, the UN offices in Vienna, which have also provided the home for this Expert Group, would likely be an ideal choice.

Similarly, we encourage Member States to ensure that there is a forum at the international level, such as the current Expert Group, that provides for an exchange of views, sharing of best practices, and contributes to capacity building efforts.

Final observations

In closing, we would like to express our gratitude for the opportunity to share these comments. Looking ahead, we call on States to continue and further expand the opportunities for input and participation by all relevant stakeholders. Ideally, this should occur in a systematic and ongoing manner.

We hope the above comments provide a helpful contribution in advancing a shared objective: effectively countering the threat caused by cybercrime. More than anything else, we believe accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in this space, underscoring the value of precisely this sort of outreach.

Please let us know if we can provide any additional input or clarify any of the contributions provided here and we look forward to additional opportunities to collaborate in the future.