الجمهورية الجزائرية الديمقراطية الشعبية

Demokratische Volksrepublik Algerien

Algerische Botschaft in Wien سفارة الجزائر بفيينا

Rudolfinergasse 18 A-1190 Wien, Österreich

Tel : +43 1 3698853, Fax : +43 1 3698856, Email : Algerianembassy.vienna@algerian-embassy.at

Vienna, 25 May 2022

Dear Member States,

At the outset, I would like to renew my gratitude and deep appreciation to all of you for your active participation and constructive involvement during the first negotiating session of the Ad Hoc Committee to Elaborate a Comprehensive Convention to Counter the Use of Information and Communication Technologies for Criminal Purposes, which allowed us to achieve a very positive outcome.

The second negotiating session of the Ad Hoc Committee, to be held in Vienna from 30 May to 10 June 2022, offers the opportunity to maintain this momentum and start to consider and build consensus on the provisions of the future convention.

At this session, the Ad Hoc Committee will undertake a first reading of the provisions on criminalization, general provisions and provisions on procedural measures and law enforcement, in accordance with the road map and mode of work of the Committee.

Also pursuant to the road map and mode of work, the Ad Hoc Committee will conduct its work on the basis of the written submissions of Member States, in the form of specific drafting suggestions or general comments on the provisions to be examined.

Ahead of this important meeting, I have the honour to share with Member States my proposal on the methodology of the consideration of the substantive items at this second session:

- **Firstly:** the floor will be open for preliminary and brief remarks (limited to 3 minutes) on the agenda item under discussion (organized by chapter, that is, provisions on criminalization, general provisions, or provisions on procedural measures and law enforcement).

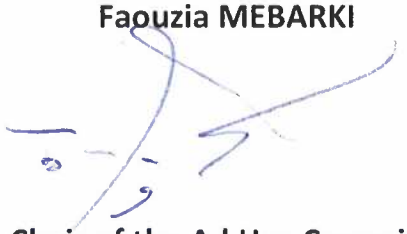
- **Secondly:** under each agenda item, the floor will be open for the specific interventions on the content and formulation of provisions. In order to organize the discussions, I will proceed by group of provisions.

To help having a focused and structured discussion, **I prepared with the assistance of the secretariat, a list of related guiding questions for each group of provisions, which I invite delegations to consider and address in their interventions**. The list, annexed to the present letter, is prepared on the basis of the written submissions of Member States. It is indicative and non-exhaustive, and any other questions and interventions on the formulation of the provisions under discussion may be made in the course of the debate.

I would like to thank you all once more for your cooperation, and I trust I can count on your continued support at this new stage of our process.

Please accept the assurance of my highest consideration.

Faouzia MEBARKI



Chair of the Ad Hoc Committee

Guiding Questions

I. Criminalization

A. First group[1] of questions:

1. What kinds of [mental/fault] elements (for example, [malicious/dishonest] intent) should be captured when considering the offences of [illegal/unlawful/unauthorized] access and interception? Should the convention consider putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, *inter alia*, penetration testers)?

2. Do you think that any of the proposed conducts must result or be intended to result in a specific or serious harm, or material damage, in order to be considered as an offence? How should "harm" be defined?

3. Should the infringement of security measures be considered as a condition for establishing some conducts as an offence, and if so under which circumstances?

[1] **First group: questions related to the following proposed provisions:**

*B. [Illegal] [unlawful] [unauthorized] access; C. [Data] [digital information] interference; D. Computer [system] [network], [telecommunication network] or [electronic device] interference; E. Obstruction of a computer, programme or data; F. Disruption of information and communications technologies networks; G. Attack on a site design; H. Unauthorised access to or interference with a critical information infrastructure; I. [Illegal] [unlawful] [unauthorized] interception;**Error! Bookmark not defined.** J. Dishonestly receiving stolen computer resource or communication device; L. Unlawful use or facilitation of the unlawful use of information and communications technologies; M. Misuse of devices or creation, utilization and distribution of malicious software. (See A/AC.291/CRP11).*

4. Could we consider the proposed provisions on "*Obstruction of a computer, programme or data", "Attack on a site design" and "disruption of information and communications technologies networks",* as forms of [illegal] [unlawful] [unauthorized] interference?

5. How do you think the convention should deal with the question of "*unauthorised access to or interference with a critical information infrastructure*"?

B. Second group[2] of questions

1. Do you think that the offence of fraud, committed in whole or in part online, is sufficient to cover other conducts such as theft, scam, financial offences, and electronic payment tools offences?

2. Regarding computer/ICT-related forgery, what kinds of [mental/fault] elements (for example [malicious/dishonest] intent) should be included in the criminalization of such act? Should the convention consider putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, *inter alia*, penetration testers)?

3. Could we consider the proposed provisions on "*creation and use of digital information to mislead the user",* as a form of [computer] [ICT]-related forgery?

[2] ***Secound group: questions related to the following proposed provisions:***

K. Identity-related offences; R. Infringement of copyright and related rights by means of information and communications technologies; S. [Computer] [ICT]-related forgery; T. Creation and use of digital information to mislead the user; V. Information and communications technologies-related theft; X. Computer- [ICT-] related fraud; W. Illicit use of electronic payment instruments. (See A/AC.291/CRP11).

4. How do you think the convention should deal with identity-related offences?

5. What would be the justification for the inclusion of offences related to the infringement of copyright in the scope of the convention, since this issue is already covered by other international instruments?

C. Third group[3] of questions:

1. How can offences relating to online child sexual abuse be defined so as to provide children with the greatest protection from harm? What should be considered in the choice of terminology?

2. Should the access or viewing of child sexual abuse material be criminalized; if yes, should a condition be made for the obligation of the criminalization of these acts such as "consistent with a State party's legal principles/domestic legislation" or "without prejudice to a State party's domestic law"?

3. What would be the justification (lack of harmonization, new forms of online sexual abuse emerging due to new means of technology, insufficiency of current international instruments…) for the inclusion of the

[3] **Third group: questions related to the following proposed provisions:**

N. Online Child Sexual Abuse; O. Sexual extortion; P. Non-consensual dissemination of intimate images ("revenge porn"); Q. Offences related to pornography; U. Violation of privacy; Y. Threat and blackmail; Z. Encouragement of or coercion to suicide; AA. Involvement of minors in the commission of illegal acts; FF. Sending offensive messages through communication service. (See A/AC.291/CRP11).

proposed provisions on: "*sexual extortion, non-consensual dissemination of intimate images and other offences related to pornography*"?

4. What would be the justification for the inclusion of the proposed provisions on: "*encouragement of or coercion to suicide and involvement of minors in the commission of illegal acts*"?

5. What would be the justification for the inclusion of the proposed provisions on: "*sending offensive messages through communication service; threat and blackmail; violation of privacy*"?

D. Fourth group[4] of questions:

1. What would be the justification for the inclusion of the following proposed provisions:

   a) *"Offences related to discrimination, racism or xenophobia";*

   b) *"Offences related to the distribution of narcotic drugs and psychotropic substances, arms trafficking, illegal distribution of*

[4] ***Fourth group: questions related to the following proposed provisions****:*

BB. Incitement to subversive or armed activity; CC. Terrorism-related offences; DD. Extremism-related offences; EE. Offences related to discrimination, racism or xenophobia; GG. Offences related to the distribution of narcotic drugs and psychotropic substances; HH. Offences related to arms trafficking; II. Rehabilitation of nazism, justification of genocide or crimes against peace and humanity; JJ. Illegal distribution of counterfeit medicines and medical products; KK. Use of information and communications technologies to commit acts established as offences under international law, LL. Offences related to terrorisme, arms manufacturing, traffocking in persons or drugs; MM. Offences related to organized or transnational crime committed using ICT. (See A/AC.291/CRP11).

counterfeit medicines and medical products; arms manufacturing, trafficking in persons, criminal association"?

2. What would be the justification for the inclusion of a provision on "*terrorism-related offences and extremism-related offences*"?

3. What would be the justification for the inclusion of a provision on "*incitement to subversive or armed activity*"?

4. What would be the justification for the inclusion of a provision on "*rehabilitation of Nazism, justification of genocide or crimes against peace and humanity*"?

5. Should the convention contain a provision to criminalize "*the use of ICT to commit acts established as offences under international law*"?

E. Fifth group[5] of questions:

1. Would Member States be supportive of the inclusion of provisions on the criminalization of obstruction of justice and the laundering of proceeds of crimes covered by the convention?

2. How do you think the convention should deal with participation in, attempt of, as well as aiding and abetting in a crime?

[5] ***Fifth group: questions related to the following proposed provisions****:*

OO. Money-laundering; PP. Obstruction of justice; QQ.Failure to protect data; RR. Other illegal acts; SS. Liability of legal persons; TT. Aiding, abetting, attempt; UU. Sanctions and other measures. (See A/AC.291/CRP11).

3. Should criminal liability be extended beyond individuals to legal persons?

4. Could the convention follow the formulation of liability of legal persons contained in article 10 of UNTOC? Would there be a need for a separate offence punishing the negligence of legal persons in maintaining required security measures?

5. Do you think that the convention should include a provision on aggravating circumstances? If so, should this be a general provision on aggravating circumstances, or should specific articles include a qualifying element of aggravating circumstances? What about mitigating circumstances?

II. General Provisions

1. How can we best ensure a fit for purpose convention considering the diverse range of technological means used to perpetrate the range of offences to be criminalized under this convention?

2. How can we ensure that the convention remains fit for purpose considering future technological developments?

3. Do you think that a chapter on general provisions, following the same structure as in UNCAC and UNTOC, could be possible for this convention? (In their chapter on general provisions, the two aforementioned conventions contain a provision on "*statement of purpose*", "*use of terms*", "*scope of application*" and "*protection of sovereignty*"). If not, what provision should be added or removed and why?

4. Should the statement of purpose contain more than three main ideas (these being, in broad terms, measures to prevent and combat [use of ICTs for criminal purposes] [cybercrime], related international cooperation and related technical assistance)? What other elements would Member States be interested in including in the statement of purpose? On which of these additional elements could Member States reach consensus?

5. Is a reference to the protection of human rights necessary in the statement of purpose, if an article exclusively on this matter is included in the convention, as proposed by some Member States?

6. Should clauses/articles on electronic evidence be limited to the offences established in the convention? Should the scope of application of the convention take into account the scope of application defined for procedural measures, and/or for international cooperation?

7. Should the scope of application include a clause on freezing, seizure, confiscation and return of the proceeds of the offences established by the convention, as proposed by some Member States?

8. Would the language in articles 4 of UNTOC and UNCAC cover all concerns from Member States with regard to the protection of sovereignty? Are considerations of sovereignty different in the context of the use of ICTs than in other – traditional – contexts?

9. Among the long list of terms proposed for including as definitions under the convention, could you propose a key list of terms that the Ad Hoc Committee has to consider as a priority (in the understanding that a final

list would need to be made after a review of the finally agreed provisions, especially on crime types, procedural measures and international cooperation)?

10. Do you think that the AHC has to first define these terms, or that definitions should only be addressed after the substantive articles of the convention are negotiated? What would be the best stage in the negotiating process to discuss definitions in a focused manner?

11. Do Member States wish to consider, at this stage, the differences between "computer systems" and "ICT devices" and their impact on the scope of application of the convention?

12. How should the convention take into consideration gender perspective throughout its provisions?

III. Procedural measures

A. First group[6] of questions:

1. Under which chapter should "*jurisdiction*" be addressed (in this regard, Member States have made proposals under all three chapters: criminalization, general provisions and procedural measures and law enforcement)?

[6] **First group: questions related to the following proposed provisions:**

A. Jurisdiction; B. Scope of procedural measures; C. Conditions and safeguards. D. Criminal Procedures. (See A/AC.291/CRP11).

2. Should the basis to establish jurisdiction include a State party being the object/target of a crime (which was included in UNCAC but not UNTOC)?

3. Should the article on jurisdiction also cover extradition-related matters, i.e. jurisdiction when extradition is not possible (*aut dedere aut judicare)*?

4. What is the scope of the chapter on procedural measures and law enforcement? Should it apply only to the list of offences established by the convention (in its chapter on criminalization)? Could it also apply to other offences? Why would such enlargement to other offences be necessary?

5. Which conditions and safeguards should procedural measures be subject to?

6. Should specific international or regional human rights treaties be referenced under this chapter, in particular under a provision on conditions and safeguards? If so, what are the specific human rights treaties that should be referenced (regional vs. global treaties)? Should there be also a reference to universal legal principles (e.g., necessity, proportionality), and which ones could be agreed upon?

B. Second group[7] of questions

1. Which powers and procedures should the convention foresee for the purposes of detecting, disrupting, investigating, prosecuting and adjudicating the concerned offences?

2. Are there any specific conditions and safeguards that should apply to certain procedural measures?

3. Should certain procedural measures apply to certain types of data?

4. What time limits should apply to the preservation of data pending a request by competent authorities for its disclosure?

5. Do Member States wish to discuss nomenclature differences between electronic information vs. computer data; accumulated v. stored (data or information) at this stage of the negotiations?

6. Member States may wish to consider whether the definition of subscriber information, under a provision on "*production order*" would be (1) required; and (2) better kept within this provision, or under the convention's general provisions on the use of terms.

[7] **Second group: questions related to the following proposed provisions:**

E. Collection of information/content and meta data transmitted by means of information and communications technologies; F. Expedited preservation of stored computer data; G. Expedited preservation of accumulated electronic information; H. Expedited preservation and partial disclosure of traffic data; I. Production order; J. Search and seizure of information stored or processed electronically or stored computer data; K. Real-time collection of traffic data; L. Interception of content data; M. Retention of data. (See A/AC.291/CRP11).

7. Should the suspicion of ICT-related crimes or the commission of criminal offences be stated as grounds for search and seizure, or for interception of content data?

8. Do Member States see a necessity in allowing for declarations or reservations with respect to the provisions on procedural measures, in order to allow for broader ratification of this convention?

C. Third group[8] of questions:

1. Which level of detail should be in the provisions on freezing, seizure and confiscation, as well as the disposal of confiscated proceeds of crime or property?

2. Should the convention contain a provision on the protection of witnesses? If yes, which factors of protection are important to include in such a provision, and what level of detail, in terms of definitions and description of related procedures, should be expected? Would the committee like to follow the formulation of UNTOC (article 24)?

3. Should the convention contain a provision on the assistance to and protection of victims? If yes, which factors of protection are important to include in such a provision, and what level of detail, in terms of definitions and description of related procedures, should be expected? What role

[8] **Third group: questions related to the following proposed provisions:**

O. Freezing, seizure and confiscation; P. Disposal of confiscated proceeds of crime or property; S. Protection of witnesses; T. Assistance and protection of victims. (See A/AC.291/CRP11).

should victims and reporting persons have? Would the committee like to follow the formulation of UNTOC (article 25)?

D. List of the fourth group[9] of questions:

1. Should the convention set standards for the collection and admissibility of digital evidence in general? What would be the advantages and disadvantages of this approach?

2. Should the convention contain a provision on special investigative techniques? If yes, which ones should be referenced, and what level of detail, in terms of definitions and description of related procedures, should be expected? Would the committee like to follow the formulation of UNTOC (article 20)?

3. Should the convention contain a provision on the establishment of criminal record by following the formulation of UNTOC (article 22)?

4. Should the convention contain a provision on measures to enhance cooperation with law enforcement authorities by following the formulation of UNTOC (article 26)?

***

[9] **Fourth group: question related to the following proposed provisions:**

N. Addmission of digital evidence; Q. Special investigative techniques; R. Establishement of criminal records; U. Measures to enhance cooperation with law enforcement authorities. (See A/AC.291/CRP11).