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; 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*"?

6. Why do some Member States choose to use the term "illegal", and others choose "unlawful", and others "unauthorized", and what would be the difference in you view?

7. Why do some Member States choose to use the term "without right", others chose "without due authorization", and others "unlawful" And what would be the difference in you view?

8. Is there any difference between "data" or "digital information", and what would be the appropriate term to use?

9. Was there a reason for some proposals not to include deterioration of data in their proposals, and for others to prefer the term "blocking" to "suppressing"?

10. Is the act of "copying" part of data interference?

11. Regarding the criminal acts related to [system/network] interference, what are in your view the devices (and nomenclature thereof) to which this article

applies: computer system, computer network, telecommunication network, electronic device, or ICT networks?

12. Would there be a need for the interception to be carried out fraudulently?

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?

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

[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).

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. Would there generally be agreement on the age limit for the definition of a child to be under 18 years of age, and for the purposes of Articles (*that would be in line with the Convention on the Rights of the Child*).

4. 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*"?

5. 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*"?

6. 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?

6. Regarding "other illegal acts", could para. 3 of art. 34 of UNTOC ("States parties may adopt more strict or severe measures than those provided in this Convention…") be a solution to cover all these offences?

***