Delegation of the Republic of Armenia

Statements

2nd session of the Ad Hoc Committee

Vienna, 31 May 2022

Madam Chair,

Armenia welcomes the opportunity to present its views on possible provisions of a new international convention on cybercrime.

We believe that this crucial endeavour of the Ad Hoc Committee to draft a new Convention within the framework of the UN has the potential of reinforcing our national and international efforts in combating cybercrime and other crimes committed with the use of ICT, which has become of transnational nature.

The new Convention offers an unrivalled opportunity to secure a widespread consensus on international cooperation to counter cybercrime, enabling states to better combat this pervasive and constantly evolving threat.

Therefore, we believe that the new Convention should take into consideration the existing international agreements, including the Budapest convention on cybercrime which has proved its effectiveness in our legal system. Also, following the international principle of “pacta sunt servanda” on fulfilment of international obligations.

Armenia considers that the crimes included in the new Convention whether there are cyber-dependent crimes or cyber-enabled crimes, should be drafted in line with the UN treaty language, to allow us to overcome the peculiarities of different legal systems of member states.

It is worth mentioning that almost all member states in their domestic laws envisage criminal responsibility for such crimes as child sexual exploitation, drug trafficking, terrorism, and other crimes, while every country has in a way unique national legislation which expresses features of their legal systems. Therefore, to bring all the countries to consensus, the provisions of the new UN convention including the ones on criminalization should cover the crimes in a general manner, thus allowing the member states to adapt them in their national legislation according to their legal principles and approaches.
We hope that this process will lead us to overcome the growing fragmentation in the international legal system in this field and will help the member states to align their different national experiences and expertise from the perspective of legal responses to such crimes.

Another benefit of such an approach could be the ability of states to respond to the everyday changes in the social relations and new types of crimes, thus allowing us to remain ahead of crime and have a convention flexible enough to allow us to devise necessary laws and regulations with regards to new and rapidly evolving crimes in this field.

Thank you Madame Chair!

Comments on guiding questions during the 2nd session
Vienna, 31 May to 10 June 2022

1. Criminalization

A. First group 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?
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”?

**Answers to the first group of questions**

Madam Chair,

Thank you for providing the guiding questions which are very useful to target specific issues. Taking this opportunity, I would like to present our position with regard to the first group of questions accordingly.

1) In response to the first question, regarding "mens rea" of cyber dependent crimes, we consider that intentionally committed crimes require criminal responsibility. At the same time, it should be noted that each country has its own types of intent, as well as different definitions thereof. For example, the terms malicious, fraudulent are used. In Armenia, intent can be direct or indirect. The concept varies from country to country. Therefore, the intent should be defined as a mandatory component without additional specifications on the type of intent,

2) Regarding the second question with respect to the infliction of harm, Armenian criminal law envisages a number of cyber dependent crimes, where the infliction of harm is a mandatory component, meanwhile in some cases the latter isn’t considered mandatory. It is noteworthy, that each country has different definitions and standards of the components of the concept of harm. Particularly, in some cases the harm is considered as only material harm, while cybercrime can attack person’s dignity and other objects, which are not material. Taking into account the above mentioned, we believe that the requirement of "harm" should not be considered in the context of the present convention, rather be regulated by the state authorities through domestic legislation.

3) With respect to the third question, it should be noted that in some cases the infringement of security measures is indeed considered as a condition of a crime. Similarly, in Armenian national criminal law, in some cases this is a mandatory condition, and in some cases it
isn’t. We believe that such a mandate should also be regulated by the domestic laws of the states.

4) Coming to the fourth question, we consider the unauthorized obstruction of the use of computer, program or data, attack on a site design, disruption of information and communications technologies as types of illegal interference.

5) Concerning the 5th question, the interference with the critical information infrastructure is also considered as a cybercrime and is already included in the definition of illegal interference. Thus, it is unnecessary to establish different types of crimes based on the confidentiality level of the information. It would also be impossible to find a common definition for critical information for every member state. It can be an aggravating circumstance and be regulated by national law.

Thank you Madam Chair

**B. Second group 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?*

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?*
Answers to the second group of questions

Thank you Mr. Chair,

1) First, it should be mentioned that the nature of computer-related fraud is the loss of property of the victim which is caused by any input, alteration, deletion or suppression of computer data, and any other interference with the computer system. We also have many crimes against property which are differentiated according different circumstances, for example fraud, theft, robbery and etc. But when we speak about computer-related fraud, all types of crimes against property, also theft, scam, financial offences, electronic payment tools offences should be included in the definition. In this case the key element of the abovementioned crime is the loss of property which can be caused by different actions committed by cyber means.

2) With respect to the second question, like cyber-dependent crimes these crimes also should be committed intentionally to lead to criminal responsibility. We believe that any element of intent like malicious or dishonest elements should not be envisaged in the Convention taking into consideration the fact that the concepts vary from country to country. Therefore, the intent should be defined as a mandatory component without additional specifications on the type of intent.

We also believe that the convention should consider putting in place legal protections for cyber-security researchers and other professionals working in cyber-security, based on the lawfulness of their actions.

3) Regarding the 3rd question, we believe that the creation and use of digital information to mislead the user, can be recognized as a form of ICT-related forgery.

4) With respect to the fourth question, we consider the possibility of inclusion identity related crimes in the convention. But it should be noted that different countries have different approaches relating to this type of crime and different components of the objective side of these crimes. So, the criteria defining the certain action as an identity theft vary from country to country. Also there can be some overlaps with other offences such as illegal interference, illegal access and fraud. Taking into consideration abovementioned facts it would be expedient not to include these crimes in the convention.

5) In response to the 5th and last question, we would like to emphasize again the role of
already existing international instruments, which proved their effectiveness in combating cybercrime. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. Taking into consideration the abovementioned facts we do not have any objection of inclusion of offences related to the infringement of copyright in the new Convention.

Thank you Mr. Chair!

C. Third group 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 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”? 


Answers to the third group of questions

Thank you Madam Chair, for giving me the floor!

1) With regard to the first and 4th questions we believe that the new convention should cover child sexual exploitation, child sexual abuse, sexual extortion, and other offences related to pornography. These crimes nowadays are mainly committed and enabled through ICT, and this phenomenon needs proper response from the states. The justification of inclusion of the mentioned crimes in the UN Convention leads to the seriousness of the threats posed by the opportunities of ICT, which enable and facilitate these highly dangerous crimes. All forms of sexual abuse of children are destructive to children’s health and psycho-social development.

Regarding the terminology, we believe that the definitions should include the behavior as referred to in Lanzarote convention of Council of Europe on the protection of children against sexual exploitation and sexual abuse, which is in line with our national legislation as well.

2) Answering the second question about criminalizing the access or viewing of child sexual abuse material, we do believe that these actions should also be addressed in the new Convention. The Armenian criminal code also envisages criminal responsibility for getting access through ICT, to child pornography in the computer system or watching child pornography.

3) With regard to the third, additional question on the age limit for the definition of a child to be under 18 years of age, our opinion is that the definition of child in the new Convention should contain the provision on the age limit, which is in line with the Convention on the Rights of Child, Lanzarote Convention, other international treaties and also our national legislation.

5) Responding to the 5th question, we do consider the possibility of inclusion of the encouragement of or coercion to suicide in the present convention.

In response to the 2nd point of the 5th question, we do not have an objection of including the involvement of minors in the commission of unlawful acts considering that the well-being and best interests of children are fundamental values shared by all member states.
But at the same time the criminalization of this action should not depend on whether it endangers children’s lives or health or not, as it is drafted in the 17th article of the convention.

Also, to lead to criminal responsibility the mentioned crime should be committed by the person who is elder that 18 years.

6) With regard to the 6th question we consider that sending offensive messages through communication service, threat and blackmail, violation of privacy are crimes which threaten the stability and security of society, democratic institutions and values. But at the same time the criminalizing provisions should take into consideration the existing standards and not to lead to disproportionate limitation and violation of the freedom of expression.

Thank you Madam Chair!

**D. Fourth group 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 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 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?

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 stricter or severe measures than those provided in this Convention...”) be a solution to cover all these offences?

Answers to the fourth and fifth groups of questions

In response to the 4th group of questions, Armenia does not have objections of the inclusion of the crimes enumerated in this group in the new Convention. Especially the offences related to discrimination, racism or xenophobia, terrorism-related offences and extremism-related offences, dissemination of Nazism, justification of genocide or crimes against peace and humanity, and offences established under international law. We believe that the criminal misuse of ICT offers ample opportunities for committing the abovementioned crimes.

At the same time, we should bear in mind already existing international instruments which address the mentioned specific types of crimes to avoid the contradictions and legal collisions between the provisions. The commonly accepted UN treaty language should be followed which considers the variety of domestic laws of every country.
Also the conditions and safeguards should be taken into consideration providing for the adequate protection of human rights and liberties, especially commonly recognized safeguards which member states has undertaken under applicable international human rights instruments.

1) With regard to the first question of the 5th group of questions about criminalization of obstruction of justice and the laundering of proceeds of crimes, we believe that ICT can be used to facilitate and enable these actions. So we do not have any objection of inclusion these crimes in the present convention.

2) We are convinced that the Convention should contain the provisions which are establishing additional offences related to attempt and aiding or abetting the commission of the offences defined in the Convention.

As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

3) Responding to the 3rd and 4th questions, we believe that the measures as may be necessary to ensure that legal persons can be held liable for a criminal offence, committed for their benefit by any natural person should be included in the new Convention. The corporate liability should not exclude the individual liability. The liability may be criminal, civil or administrative which will provide the states to have the flexibility to choose to provide for any or all of these forms of liability, in accordance with the legal principles of each country.

5) With regard to the 5th question, the commitment of the most part of discussed crimes through ICT is already an aggravating circumstance according to our national legislation. In this case, as we are dealing with the variety of crimes, which can have specific aggravating circumstances because of their nature and it will be impossible to envisage the aggravating circumstances applicable for all crimes. For example, there is an aggravating circumstance for child sexual abuse, when the crime is committed by a member of family, a person cohabiting with the child or a person having abused his or her authority. This circumstance will not be applicable for most types of crimes covered by the Convention. Thus, our opinion is not to include the article on aggravating circumstances in this convention, leaving the mentioned question to the regulation of other specialized international treaties and national legislation.
Thank you Madam Chair!

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?

**Answers to the questions on General provisions**

Thank you Madam Chair,

Armenia welcomes the opportunity to submit its views on the general provisions of a new international convention on cybercrime.

1;2) With regard to the first and second questions, we are of the view that many delegates have already mentioned that the convention should not define many technological means used to perpetrate the offences. We encourage to limit the set of definitions which should be drafted in technologically neutral manner. This approach gives an opportunity to consider future technological developments and peculiarities of the domestic laws of member states.

3) Responding to the 3rd question on the structure of general provisions of the Convention, Armenia supports following the same structure of general provisions as in UNTOC and
UNCAC. But we believe that the content of those provisions deserve more thorough consideration before reflecting in the new convention in order to ensure proper adaptation to the peculiarities of the digital domain.

4.5) With regard to the 4th and 5th questions, we believe that ensuring the high level of protection of human rights and fundamental freedoms, the purpose of the convention should be prevention, investigation and prosecution of cybercrime, including international cooperation, support of the capacity building and technical assistance in the fight against cybercrime and other ICT related crimes, also the protection of victims’ rights. So, we are of the view that the statement of purpose should include the protection of human rights and fundamental freedoms and the protection of victims’ rights. Certainly the present convention is not an international instrument for human rights protection, but we are dealing with the international agreement which provides procedural powers to investigate crimes. The balance of law enforcement measures and the protection of human rights should be followed. The powers and procedures should incorporate the principle of proportionality not to lead to the violation of human rights.

6) With regard to the 6th question we are of the view that the specific criminal investigations or proceedings, the powers and procedures should be applied not only to the offences established in accordance with the convention, but also to the collection of evidence in digital form of any other criminal offence. We should ensure that the digital evidence of any criminal offence can be obtained or collected by means of powers and procedures set out in the convention.

7) In response to the 7th question, we consider the possibility of including provisions on freezing, seizure, confiscation and return, but the specificity of cybercrime should be taken into consideration.

8) With regard to 8th question we are not of the view that the language in articles 4 of UNTOC and UNCAC is fully applicable for the present convention. With respect to the mentioned international treaties they address other types of crimes. We should keep in mind that provisions designed for off-line applications may not be fit and thus may become more problematic in the online environment and raise difficulties in the implementation of criminal justice procedures. The principle of sovereignty is one of the fundamental principles of international law which is accepted by all member states. But a number of issues arises when we speak about cybercrime and cyberspace, the traditional principle
becomes complex in this context. Cybercrime is transnational and it means that a criminal in one country can attack an information system under the sovereignty of another state, the data can be transferred from the jurisdiction of one country to the others in one second and the digital evidence on such crime could be preserved in the cloud or elsewhere. Taking into consideration the abovementioned we will refrain from expressing final views on this issue and remain open for future consideration.

9;10) In response to the 9th and 10th questions we believe that the Convention should contain a limited number of definitions, which are “computer system, computer data, service provider, traffic data, subscriber data, content data, central authority, competent authority”. These definitions have proven to be sufficient, adaptable to changing technology and work in practice, and they have been agreed upon most part of the member states. Also the broad list is unlikely to find consensus in a UN treaty.

11) With regard to the 11th question, we believe that the term computer systems should be used. The mentioned term is used in domestic laws of most of member states, also this term is already agreed in the Budapest convention to which 67 states are parties.

12) With regard to the twelfth question, gender equality is also a priority area for Armenia, but we do not believe that the present Convention on combating cybercrime has specific gender issues, but we consider the possibility of these perspectives which will become more obvious through the future negotiations.

III. Procedural measures

A. First group 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)?

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?

Answers to the first group of questions on procedural measures

1) In response to the first question we believe that the jurisdiction article should be in the procedural measures and law enforcement chapter, where it is more applicable.

2) With regard to the 2nd question we believe that the state should be able to establish its jurisdiction over any crime when the offence is committed against the State part. Thus, we believe that like UNCAC, the basis to establish jurisdiction should include a state party being the object of a crime.

3) In response to the 3rd question we believe that the article on jurisdiction should cover some extradition-related matters, like UNTOC, UNCAC and the Budapest convention. In particular, the state should have the right not to extradite an alleged offender in cases where he or she is present in its territory, on the basis of his or her nationality.

4) With regard to the 4th question we are of the view that the specific criminal investigations or proceedings, the powers and procedures should be applied not only to the offences established in accordance with the convention, but also to the collection of evidence in digital form of any other criminal offence. We should ensure that the digital evidence of any criminal offence can be obtained or collected by means of powers and procedures set out in the convention.

5;6) With regard to the 5th and 6th questions, as we have already mentioned in our previous statement, ensuring the high level of protection of human rights and fundamental
freedoms, should be included in the purpose of the Convention. The procedural powers and procedures should be subject to conditions and safeguards which shall provide for the adequate protection of human rights and liberties. Like EU we believe that the specific human rights treaties like Un international covenant on civil and political rights and other applicable human rights instruments should be referenced. These are minimum standards to which parties must adhere. Also such conditions and safeguards should inter alia include judicial or other independent supervision.

The universal legal principles such as necessity, proportionality, legality should also be other safeguards. The procedural powers should be applied whether they are envisaged by law, when it is necessary and also should be proportional to the nature and circumstances of the offence. Every procedural law enforcement measure deals with human rights limitation and not to lead to the violation of human rights and collect admissible evidence, the mentioned principles should be followed.

B. Second group 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. 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?

**Answers to the second group of questions**

1. In response to the first question, the procedural law chapter of the Convention should include expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure, which are already included in existing international instruments. What about real-time collection of traffic data and interception of content data, as they are highly intrusive measures we should consider including them if proper conditions and safeguards are applied.

2. Responding to the second and third questions, we believe that there are certain procedural measures that should apply to certain types of data. The application of certain procedural measure depends not only on the type of data, but also whether it is stored or is not stored and is in real-time. Consequently, there should be different requirements for obtaining subscriber data, traffic data and content data. Interference with rights of individuals considered to be substantially different when obtaining content data and subscriber data. Also, for example the conditions and safeguards applicable to real-time interception of content data may be more stringent that those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data. Shortly, different procedural measures are applicable for different types of data, consequently there are different requirements for procedural measures, taking into consideration the difference of degree of interference to the privacy of a person.

4. With regard to the 4th question the power of a Party to oblige a person to preserve and maintain the integrity of computer data should have time limitation of 90 days.

5. On question 5 the term computer data is commonly accepted term which is used not only in existing international instruments but also in domestic laws of member states. So we do not see the necessity to address the differences between mentioned definitions.

6. With regard to the 6th question we believe that the definition of subscriber data should be included in the general provisions as other definitions.
7. On question 7, we believe that the grounds of enforcing certain procedural measure should not be addressed in the present Convention and be left to the national legislation and practice. Instead we should focus on the scope and definitions of procedural powers.

8. With regard to the 8th question, we believe that in general the declarations or reservations should be allowed, which will make the Convention more flexible. But as many delegates have already mentioned we should firstly come to the consensus on the scope and the definitions of the procedural powers, then turn to declarations and reservations.

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

D. List of the fourth group 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)?

**Answers to the third and fourth groups of questions**

1) With regard to the first question of the third group of questions, we believe that the provisions of already existing global instruments can be followed and be accepted as basis for the future. Also we hope that the present Convention will address the issues on freezing, seizure and confiscation of cryptocurrencies and digital assets. Minimum basic regulations on these issues can become a basis for future regulation of these relations in domestic laws, taking into consideration that these new types of currencies are subject for consideration for all member states.

2) In response to the second and third questions we support using the formulations of UNTOC provisions on protection of witnesses and the assistance to and protection of victims.

1) On question 1 of the fourth group of questions, we do not believe that the standards for the collection and admissibility of digital evidence should be included in the Convention. The rules on the admissibility of evidence is primarily a matter for regulation under national law. At the same time as we have already mentioned in our previous statement, human rights protection should be one of the main goals of the Convention, the procedural powers should be subject to the safeguards and conditions. The principles of legality, necessity, proportionality should be referenced and followed.

2;3;4) With regard to the questions 2,3,4 we believe that the provisions on special investigative techniques, on establishment of criminal record, and on measures to enhance cooperation with law enforcement authorities can be included in the Convention. The formulations of UNTOC on these matters are acceptable.