INTERVENTION

BY

SOUTH AFRICA

DURING THE SECOND SUBSTANTIVE SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

AGENDA ITEM 4: PROVISIONS ON CRIMINALISATION – 4TH AND 5TH GROUP OF QUESTIONS

30 MAY – 10 JUNE 2022

VIENNA

Check against delivery

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

B. 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 terrorism, arms manufacturing, trafficking in persons or drugs; MM. Offences related to organized or transnational crime committed using ICT. (See A/AC.291/CRP11).

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"?

Thank you Madam Chair. South Africa will proceed to provide comments on the 4th Group of Questions. With regards to the first question on the inclusion of offences related to discrimination, racism or xenophobia, our view is that these offences are already covered by other international instruments and domestic law systems and should not be included in the future Convention.

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

Turning to question 2, we are of the view that inclusion of provisions on terrorism-related and extremism-related offences may delay progress in reaching agreement on the future Convention as the term "terrorist" does not enjoy universal understanding. However, we are keen to hear the views of other delegations.

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

On question 3, the inclusion of a provision on incitement to subversive or armed activity" we believe that this can be governed through domestic laws. However, since this offence has an element of cyber dependency based on the current trends of inciting violence and

insurgencies which involve the use of digital platforms such as social media for crowd funding, we are open to proposals from other delegations.

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"?

With regards to question 4 we are of the view that these provisions are already in already covered in international instruments and domestic laws. We submit that they be excluded from the future Convention.

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

Lastly Madame Chair, on the inclusion of a provision to criminalise "the use of ICTs to commit acts established as offences under international law", our answer is "NO". These acts are sufficiently regulated by domestic laws. Consideration could be given only if the element of cyber dependency exists.

Madam Chair, South Africa will now response to the 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?

With regards to question one, although provisions on the criminalization of obstruction of justice and the laundering of proceeds of crimes are covered in other international instruments, we are of the view that they could be considered in the future convention where such activities of money laundering are cyber dependent. Laundering of proceeds are uniquely enabled by the new cyber technologies such as blockchain and cryptocurrency to obscure and facilitate the laundering of proceeds and criminal assets.

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

On question two, participation in, attempt of, as well as aiding and abetting in a crime is fully catered for in international and domestic instruments. However, if the act goes

beyond cyber enabled activities of aiding and abetting, consideration may be given to its inclusion as cyber dependent, especially where digital information is given to equip the criminal to use it or assist the criminal to commit a crime like hacking for purposes of identity theft and/or for cyber-fraud activities.

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

On question three, South Africa is of the view that criminal liability should be extended beyond individual to legal persons to give effect to professional enablers who hide behind laundering vehicles/entities. South Africa's legislation provides for corporate liability. In addition, the concept of legal persons should also be explored towards virtual entities where the legal definition or framing of a legal person might not yet be mature in law or at a transnational level.

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?

On question four, South Africa submits that the convention could follow the formulation of liability of legal persons contained in article 10 of UNTOC as legal persons need separate punishment, such as corporate probation with a fine etc. Furthermore, South Africa is of the view that consequences of contravention by legal persons should be strengthened internationally by not only allowing fines but by also having international probation or baring by other states on the request of a Member State especially on repeat offending legal entities.

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?

Regarding question five, South Africa's response is Yes, aggravated circumstances are crucial and should be included within the future convention. In particular when there are cyber attacks on the systems of Government or corporations such as financial institutions or any institution that performs essential or critical services, whether private or public,

such offences should be classified as aggravated offences especially to deal with repeat offending.

South Africa is of the view that it is not necessary to have mitigating circumstances for sentences purposes as that may be prescriptive and inappropriate. Mitigating circumstances should be dealt with in domestic law.

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?

Regarding question 6 on other illegal acts, South Africa is in agreement with para 3 of article 34 of UNTOC as State Parties ought to be given that prerogative, especially for more stricter measures in their domestic legislations. Moreover, if dealing with cyber dependent crimes broadly that covers most illegal acts.

I thank you Madam Chair.