INTERVENTION BY THE REPUBLIC OF SOUTH AFRICA

ON THE OCCASION OF THE

FIRST 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: OBJECTIVES AND SCOPE OF THE CONVENTION

28 FEBRUARY – 11 MARCH 2022

NEW YORK

Check against delivery

Madam Chair,

The complex nature of cybercrime requires a dynamic and transnational approach to counter the use of ICTs for criminal purposes. In this regard, South Africa welcomes the Chair's proposal on the **objectives** of the envisaged international convention. South Africa is of the view that in addition, the **objectives** should be to:

a) Pursue a common criminal policy aimed at the protection of society against cybercrime, while guaranteeing fundamental human rights including freedoms and privacy.
b) Address gaps that exist in national criminal laws that do not comprehensively deal with cybercrime especially in relation of cross-border cooperation;
c) enhance international cooperation in the fight against cybercrime;
d) create enforceable mutual legal assistance (MLA) provisions to facilitate and expedite sharing and assistance in cybercrime matters; and have capacity building at its centre.

Madam Chair,

In terms of the **scope,** South Africa is of the view that the convention should create an understanding of trends; and developments in cybercrime, including the modus operandi as well as enable investigation, combating and prosecution of cybercrime in a comprehensive manner across different jurisdictions.

In this regard, the Convention should include, among others:

a) Substantive criminal offences - This would include offences to be criminalised and measures to be taken at a national level. The focus should be on criminalising the misuse of ICTs for criminal purposes rather than the technology itself. Criminal offences must be clearly defined and narrowed with a view to reaching a common understanding in order to avoid legal uncertainty caused by vague provisions resulting in gross violation of human rights and fundamental freedoms.

b) The Convention must describe procedural measures to be taken at the national and international levels for the purpose of criminal investigation of the offences committed by means of a computer system and the collection of electronic

evidence for litigation purposes. The Convention should describe action to be taken and procedures to be followed for electronic evidence admissibility in a cybercrime investigation.

c) As articulated in the Chair's proposal, enhanced international cooperation should be a priority in the Convention when considering the extent of cybercrime and its impact on economic development, particularly in developing countries. It is the duty of all States to ensure that criminals do not have anywhere to hide hence the general scope of the obligation for States to cooperate needs to be dealt with in the Convention. The Convention must clearly indicate that international cooperation is to be provided amongst all parties "to the widest extent possible" to repatriate assets, extradite those who are evading justice and to ensure that citizens of the world benefit from crime free cyberspace. To this end, the establishment of 24/7 points of contacts could be beneficial.

d) Capacity building, technical assistance and adequate financing should be prioritised and be based on the receiving State's objectives and request. Law enforcement agencies in some countries often do not have sufficient capacity to investigate complex cybercrime cases and should be assisted to build adequate capacity. There must be requisite technology transfer and finance to facilitate capacity building within developing countries.

e) The Convention must determine criteria under which parties are obliged to establish jurisdiction over the criminal offences based upon the principles of territoriality and sovereignty.

f) Finally, the Convention should clearly define the respective roles and responsibilities of service providers, especially ISPs in the investigation and combating of cybercrime. There should also be enhanced public-private partnerships in the prevention of cybercrime as a significant proportion of the internet infrastructure is owned and operated by the private sector.

I wish to thank you chair.