THE UNITED REPUBLIC OF TANZANIA

SUBMISSION OF THE COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

8th APRIL, 2022

1. Introduction

The United Republic of Tanzania is pleased to respond to the invitation to the Member States to submit their views on the preamble, general provisions, criminalisation, law enforcement and measures of the new international instrument on cybercrime, in accordance with General Assembly resolutions 74/247 and 75/282, of 27th December, 2019 and 26th May, 2021 respectively. The submission includes tentative elements proposed for inclusion in the body of the aforementioned convention, in the hope of achieving the desired objectives by strengthening international cooperation and formulating a common crime policy aimed at countering all ICT-related offences.

Cybercrime is an emerging form of transnational crime and one of the fastest-growing worldwide. Its rise is closely linked to the evolution and exponential development of ICTs affecting millions of citizens and businesses every year.

2. Preamble

Taking into account technological advancements, today's World is like a village, where information may flow instantaneously from one jurisdiction to another through the use of ICT. Due to this fact, the commission of crime with facilitation of ICT has become a global concern. To combat the existing challenge a need for mechanism to manage and control cyber space is inevitable.

The United Republic of Tanzania proposes the convention to indulge itself into addressing the following aspects in the Preamble:-

a. The magnitude of cross boarder cybercrimes
b. The effects of cybercrimes in relation to social, economic and political stability of Member States
c. Adherence to the UNGA Resolution 1314 (XIII) of 12th December, 1958 on the sovereignty of each state and other relevant International instruments which safeguard principles of sovereign equality and territorial integrity of States and

that of non-intervention in the domestic affairs of other States in handling cybercrimes

d. Encourage international cooperation between states in preventing, controlling and combating cybercrimes
e. Recognizing the efforts done by different international stakeholders and states in preventing, controlling and combating cybercrimes
f. Encouraging the use of asset forfeiture as a tool to combat all forms of cybercrimes
g. Encouraging harmonization of cybercrime laws of states so as to ease the process of preventing, controlling and combating cybercrimes
h. Encourage technical assistance, information and experience sharing, and capacity building to developing countries in preventing, controlling and combating cybercrimes
i. To acknowledge the existence and protection of vulnerable groups within the member states

3. General Provisions

The purpose of the Convention should be to promote cooperation on Countering the Use of ICTs for Criminal Purposes. The Cyber world is revolving and there is a wide range of terminologies used in ICTs to date. It is imperative that the Convention defines terms that are universally applied in ICTs to avoid ambiguities or misunderstandings.

3.1 Definition of terms

It is in the view of the United Republic of Tanzania that the Convention should provide for definition of terminologies in a neutral technological manner to accommodate rapid technological changes. The terminologies should include the following:-

a) Access
b) Access provider
c) Caching provider
d) Child
e) Child pornography

f) Computer system
g) Computer data
h) Confiscation
i) Contraband
j) Cryptography
k) Cyber terrorism
l) Data
m) Data message
n) Data storage medium
o) Electronic data
p) Freezing
q) Hinder in relation to a computer system
r) Interactive message system
s) Interception in relation to a function of computer
t) Interconnection
u) Originator
v) Racist and xenophobic material
w) Seizure
x) Service provider in relation to ICT
y) Traffic data

3.2 Jurisdiction

The Convention should provide for legislative and such measures as may be necessary for each State Party to establish its jurisdiction over the offences established under the Convention when:-

a. The offence is committed in the territory of that State Party
b. The offence is committed on board a vessel that is flying a flag of that State Party or an aircraft that is registered under the laws of that State Party
c. The offence is directed against computer system, device or data or person located in the territory of that State Party

d. The offence is committed by or against a national of that State Party.

4. Criminalization

Recently, there has been an exponential increase of the use of ICTs for criminal purposes by groups of criminals worldwide due to technological development.

4.1 List of Offences

Owing to this challenge the United Republic of Tanzania sees the need for each State Party to adopt such legislative and other measures, as may be necessary, to establish as criminal offences, when committed wilfully and intentionally, the following actions but not limited to:-

a. Illegal access

b. Illegal interception

c. Illegal destruction of electronic data and computer system

d. Data espionage

e. Illegal system interference

f. Owning illegal devices and/ or software for purposes of committing crimes

g. Computer related forgery and fraud

h. Pornography and child pornography

i. Identity related crimes

j. Publication of false information

k. Racist and xenophobic materials

l. Genocide and crimes against humanity

m. Cyber bullying

n. Attempt, Aiding and abetting

o. Participation in an organised criminal group

4.2 Corporate liability

The United Republic of Tanzania proposes that the convention should require member states to include, in their domestic legislations, the provisions that impose liability to the legal persons in relation to offences established by the Convention. The liability may extend to natural persons acting on behalf of, or under the cover of the corporate.

5. Procedural Measures

Cybercrime laws identify standards of acceptable behaviour for ICT users; establish socio-legal sanctions for cybercrime; protect ICT users, in general, and mitigate and/or prevent harm to people, data, systems, services, and infrastructure. The United Republic of Tanzania proposes the convention to encompass the following aspects in procedural measures section: -

a. Expedited preservation ad disclosure of electronic data

The Convention should have a provision for member states to include measures in their domestic legislations, as may be necessary, to enable its competent authorities to order or similarly obtain the expeditious preservation of specified electronic data, including traffic data, which has been stored by means of a computer system. In particular, where there are grounds to believe that the electronic data is particularly vulnerable to loss or modification.

Where, by means of an order to a person to preserve specified stored electronic data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that electronic data for a period of time necessary to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

The Convention should contain provisions for member states to adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

b. Production Order

There should be a provision within the convention for legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium.

c. Search and seizure of stored computer data

It is imperative for the Convention to set obligations to member states to have provisions in their legislations and other measures as may be necessary to empower their competent authorities to search, access and seize of a computer system or part of it, computer data stored therein and in which computer data may be stored in its territory.

d. Protection of whistle blowers and witnesses

The Convention should provide for the obligation to state parties to provide for protection of whistle blowers, witnesses and victims of cybercrimes, as the circumstance of the case may require.

It is further proposed that the Convention should direct member states to take appropriate measures within their means to provide effective protection from potential retaliation or intimidation for whistle blowers and witnesses in criminal proceedings who give information or testimonies concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them in accordance with their domestic laws. These measures should not prejudice the rights of the defendant, including the right to due process.

6. Law enforcement

The proper management of cybercrimes and related offences requires the involvement of different processes which are prevention, detection and combating. Thus, these processes mandated to law enforcement agencies need to be acknowledged. Therefore, the United Republic of Tanzania is of the view that the Convention should cover the following aspects in relation to law enforcement.

a. Training, technical assistance and exchange of expertise

To effectively prevent and combat the use of ICTs for criminal purposes, it is essential to provide technical assistance to developing countries and strengthen the exchange of information. Technical assistance and exchange of expertise should focus on the following:

i. Detection, prevention, and combating of the offences covered by the Convention;
ii. Techniques used by persons suspected of involvement in offences covered by the Convention, and appropriate countermeasures;
iii. Monitoring of the movement of contraband;
iv. Detection and monitoring of the proceeds of crime, property, equipment or instrumentalities and methods used for the transfer, concealment or disguise of such proceeds and instrumentalities, as well as methods used in combating cybercrimes;
v. Collection of evidence;
vi. Modern law enforcement equipment and techniques, including the use of developed new software and undercover operations;
vii. Methods used in combating cybercrimes committed through the use of computer systems, telecommunications networks or other forms of modern technology
viii. Planning and implementing, research and training programmes designed to share expertise in the protection of cyberspace.

b. Joint Investigations

Cybercrimes are borderless in nature which may involve more than one country. The Convention should provide for the obligation to state parties to make arrangements in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States. The competent authorities concerned may establish joint investigative bodies. The state parties involved are urged to ensure that the sovereignty of the State Party, in whose territory such investigation is to take place, is fully respected.

c. Financial Support

There should be a provision under the convention that imposes an obligation to developed states as well as UN agencies to offer financial support to developing countries so as to implement strategies in detecting, preventing and combating cybercrimes.

7. Conclusion

The United Republic of Tanzania reaffirms its commitment to discharge its obligations under existing United Nations Conventions to prevent and suppress Cybercrimes. We further reaffirm our assurance to protect and safeguard the rights of victims of Cybercrimes. Also, we express our commitment to cooperate with other states and international community in preventing and suppressing cybercrimes.