Permanent Mission of the United Republic of Tanzania
to the United Nations

Check Against Delivery
SUPPLEMENTARY SUBMISSION OF THE UNITED REPUBLIC OF TANZANIA TO THE
ADHOC COMMITTEE ON THE CHAPTER OF PREVENTIVE MEASURES
Madam Chair,

At the outset, my delegation wishes to state that, the Chapter on Preventive Measures is critical in the detection, prevention and control of the offences to be covered by the future Convention. The Convention should use permissible language encouraging State Parties to develop and maintain effective, coordinated policies and measures that focus on proactive activities such as public awareness and other educational programs. Equally important is the need to enhance enforcement measures through the criminal justice system to effectively deter and prevent cybercrime in accordance with the fundamental principles of domestic legal systems of State Parties. In Tanzania for instance, cyber-dependent offences have been designated as economic crimes attracting severe penalties including the issuance of ancillary orders such as forfeiture of tainted properties.

We further support and echo the recommendations of the Intergovernmental Expert Group on Cybercrime including the observation that prevention is not just the responsibility of Governments: it also requires the participation of all relevant stakeholders, including law enforcement authorities, the private sector, especially the Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general. We further reiterate our previous statement in the Technical Assistance Chapter that some developing countries have limited capacity and capability to prevent, detect and combat cybercrime. The Convention should therefore encourage various measures and programs including those offered by UNODC to continue providing technical assistance, upon request, to prevent and counter cybercrime.

Question 32 : my delegation puts forward the following key areas:

i. General Preventive Measures principles in line with existing international instruments on crime;

ii. Participation of all relevant stakeholders, including, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the general public;
iii. Development of long-term public policies on prevention, which should include the development of awareness-raising campaigns;

iv. Development or strengthening of support programmes for victims of cybercrime and other disadvantaged groups such as women, children and the elderly;

v. Development of specific and joint tailored efforts to foster international cooperation arrangements to enable reporting, detection, investigation, prosecution and deterrence of child sexual abuse and exploitation online; and

vi. Sharing of best practices on effective and successful preventive measures against cybercrime.

It is also our considered view that there are vulnerable groups, such as children, for whom preventive measures would need to be prioritized. My delegation recalls that during the general discussion on the criminalization chapter, there was consensus by State Parties on the criminalisation of child sexual exploitation which may include possession or online distribution or transmission of child sexual exploitation and abuse materials.

In particular, we proposed for the adoption of a wider overarching offence of online sexual abuse to encompass conducts of child sexual exploitation, which may include possession or online distribution or transmission of child sexual exploitation and abuse materials. We all spoke in one voice that the effects of online Child Sexual Exploitation and Abuse Materials can be devastating, ranging from significant distress to victims but also a wide range of short-and-long term psychological trauma. To this end, we submit that the future Convention should prioritize and provide specific measures aiming at protecting children from such abuses. State Parties may consider adopting joint mechanisms in collaboration with the private industry to detect and promptly remove CSEM online. All these measures should be carried out in consistent with State Parties domestic laws and legal systems.

On question number 33, we recognise that during the general discussion on the criminalization chapter, there was no consensus on the inclusion of an offence of unauthorised access to or interference with a Critical Information Infrastructure (CII).
We concur with other State Parties that the focus of this Convention is to prevent and combat cybercrimes and not cybersecurity, which is far beyond the mandate of the Adhoc Committee.

On question number 35, it is our view that authorities responsible for preventing the use of information and communications technologies for criminal purposes differ from one State to the other. In Tanzania for instance, while the mandate of the Central Authority for Mutual Legal Assistance in respect of criminal matters including cyber-dependent crimes is vested to the Director of Public Prosecutions, the mandate for acceding to the inbound extradition requests is vested to the Minister responsible for Legal Affairs. Furthermore, the mandates for the execution of MLA matters are equally shared by all law enforcement agencies depending on the matter in question. It is therefore our considered view that since State Parties have already designated such central and competent authorities under the existing international conventions and other bilateral treaties, it is not necessary for the Convention to require State Parties to make such a designation.

On questions 36 and 37, the future Convention should encourage State Parties to take measures to cooperate with civil society, the private sector and academia, to prevent the use of information and communications technologies for criminal purposes. We propose that the Convention should use permissible language without posing any mandatory requirements or obligations on the private sector, which may not be practicable. Furthermore, such cooperation must be consistent with the domestic laws of State Parties. The Convention should encourage cooperation in areas of raising awareness of cybercrime risks, capacity building and public education programmes.

I thank you Madam Chair.