July 11, 2023

OEWG ICTs 2021-2025: Virtual, informal dialogue with Chair

Mr. Chair, the CfMA is one of the Africa based organizations, that advances the views and perspectives of Africa and global south in processes like this one convened by you, Mr. Chair, we are based in Uganda. Our input draws from a document that was developed as an input into the Open-Ended Working Group on ICTs (OEWG) during a multistakeholder consultation held in Lilongwe, Malawi from 16th to 18th July 2022 immediately prior to the 11th African Internet Governance Forum.

The consultation, linked to the 10th African School on Internet Governance, was convened by the Association for Progressive Communications and Global Partners Digital, and was attended by a diverse group of individuals from African governments, law enforcement and security agencies, the African Union Commission, civil society organisations, digital rights and media groups, and cybersecurity experts – including our organization, the **Centre for Multilateral Affairs.**

Now in view of your request on how stakeholders can work together with States to contribute to the implementation of the concrete, action-oriented proposals made by States at the third and fourth substantive sessions across the various pillars of the OEWG's mandate, as captured in the Zero Draft of the second APR

And

How the stakeholder community can contribute most meaningfully and effectively to the implementation of the various proposals, given our unique expertise and resources.

Mr. Chair, we will focus our submission on the pillar of Capacity Building. We therefore, note that:

Non-state actors including civil society, business and the technical community, can contribute in a range of ways to capacity building. This includes: analysing policies and developing model laws; integrating a human centric and human rights approach into ICT security law, policy and regulation; developing and promoting standards for ICT security; developing skills and capacity - including

digital security and cyber hygiene capacity - in formal and non-formal contexts; developing training materials including for digital safety, security and literacy; designing programmes to achieve gender equality and equality in the cybersecurity sector – among others.

We recommend that stakeholders can collaborate to:

- Establish peer-to-peer knowledge transfer at innovation hubs and centres of excellence to encourage home grown expertise in Cyber and related areas.
- Prioritise cybersecurity in national budgets to ensure adequate resourcing for cybersecurity capacity development including through integrating cyber hygiene and digital safety and security into standard educational curricula at primary, secondary, tertiary levels and in vocational training programmes.
- Develop and implement mechanisms for national, sub-regional, regional and continental collaboration between Cybersecurity Incidents Response Team (CSIRT) or Computer Emergency Response Team (CERT).
- Establish CSIRTs and CERTs where they are not yet in place. Enhance coordination and collaboration at national, regional and international level between state and non-state actors, especially within the global South
- Enhance the capacity and capability of law enforcement agencies to tackle cybercrime and child online protection at national, regional and international levels.
- Enhancing resilience of national Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) by developing and operationalising national risk mitigation frameworks for identifying national critical assets and sectors.
- Develop a sustainable framework for cyber capacity enhancement. One approach is to build and give greater visibility to existing expert communities from within Africa - where they exist, and to create them where they do not - to take ownership and lead in sustaining cyber capacity building. A key example is the African Union Commission's Cybersecurity Expert Group.
- Work collaboratively to ensure a human centric approach which considers how cyber security affects peoples' well-being, rights, livelihood, environment, culture, belief systems and mindsets

Thank you, Mr. Chair.