1 March 2023

To: Amb. Burhan Gafoor

Chair Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

CfMA STATEMENT DURING THE INFORMAL DIALOGUE BETWEEN THE CHAIR AND INTERESTED STAKEHOLDERS: OEWG ON ICT SECURITY

Mr Chair, thank you for the opportunity created to engage with stakeholders through this informal dialogue. The CfMA was looking forward to interacting with diverse colleagues, in this room and beyond next week for the 4th Substantive session of the OEWG II on ICTs in New York, United States. Unfortunately, our participation is constrained by the inability to receive a US Visa on time.

Moreover, this is the second time our request for NGO accreditation to engage in formal sessions are being vetoed. The CfMA is based in Kampala, Uganda and is one of the very few actors from developing countries advancing a global south perspective in discourses and processes like this one created by your office. Nevertheless, despite these setbacks, we are glad about your resolve to diversity and inclusion of perspectives and that you are still able to engage with stakeholders through this informal consultation.

Mr. Chair, regarding your questions as to what new and emerging technologies can potentially be exploited for malicious ICT activity? And Which are being used most extensively currently and which pose the greatest risks to international peace and Security, we take note of the following.

- Big data analytics and storage which has led to the use of offensive and defensive cloud security infrastructure.
- Artificial Intelligence and Machine Language that has seen the rise of robotics in production and now social interactions.
- Block chain technologies for smart societies and financial institutions

We note that some of the possible risks/threats that these technologies pose to international peace and security include but are not limited to.

- They exploit supply chain vulnerabilities in various hybrid products thus leading to the increased threats of ransomware and breach of privacy.
- Distributed Denial of Service is another form of malicious activity that may exploit the weakest link on cloud infrastructure.

And regarding your question on how stakeholders can work together with the international community to develop a deeper understanding of the potential risks to international peace and security posed by these new and emerging vectors and vulnerabilities, we suggest the following:

- That there is need to collect and share examples of impact of cyber incidents, including on critical infrastructure, and particularly the disproportionate impact for both countries in the global North and those of developing countries
- Continuous Research including from developing countries such as Africa, Asia, Latin America, the Caribbean etc. is critical.
- Information sharing and inter-agency coordination between states and other communities such as technical community and academia

On what concrete, specific initiatives can States and/or stakeholders undertake within the framework of the OEWG to mitigate the impact of these new and emerging vectors and vulnerabilities on international peace and security, we propose that.

- Investment in strong cybersecurity standards and practices is key and such investments doesn't have to be highly sophisticated
- There is need to collect and share lessons learned from ransomware attacks, make more countries resilient, expand existing coalitions/networks
- There is need for cyber capacity building of state institutions so that they can survive and remain resilient
- There is need to encourage developments of national-level research that feeds into the overarching framework at international level in respect to how ICTs can be used for peaceful purposes. For example, the CfMA has been raising awareness, building capacity and sensitizing stakeholders on the work of the OEWG II. The CfMA has also conducted research that informs about the relevance of normative frameworks for responsible state behavior in the cyberspace in Uganda and we believe such contributions are significant Mr. Chair.

Thank you very much for this opportunity, Mr. Chair