ICT4Peace Statement at Virtual, Informal Consultative Discussion with Chair of the Open-Ended Working Group (OEWG) on the Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025

Excellencies, Ladies and Gentlemen, Dear Colleagues

We appreciate this opportunity to speak today, but we would ask that in the future that there is additional time allocated for non-state stakeholders, many of whom have extensive expertise relative to the Information and Communications sector, to make meaningful contributions.

Furthermore, in line with the words of Ambassador Gafoor's opening remarks, we call on the OEWG to change gears from a talk shop to one that is focused **implementation** of the 11 norms elaborated in the 2015 GGE Report, and subsequently reaffirmed in the 2021 GGE and OEWG reports.

Along the theme of implementation:

- We call for the OEWG to develop a **robust and nimble institutional framework** that is able to respond in a timely manner to new and emerging challenges in information and communications technologies, including developing mechanisms to elaborate more norms to respond to additional, emerging and future challenges. The Programme of Action for advancing responsible State behaviour in cyberspace makes a promising start, however we have concerns that a body that only has working level meetings organized once a year and a Review conference organized every five years would not be nimble enough to respond effectively to the fast-moving challenges presented in the Information and Communications Technologies Space
- We also refer back to two previous submissions ICT4Peace has made to the OEWG to :
    1. Call on States to publicly commit to not cyber attack critical infrastructure installations
    2. To develop a framework and mechanism for robust accountability of States for their activities and actions in cyberspace. We have suggested to develop one modeled after the Human Rights Council's Universal Periodic Review (UPR) mechanism

- As a final note, we want to stress the **urgency** to respond in a coordinated and effective manner to the exponentially increasing number of threats online, including but not limited to, malware, particularly ransomware attacks, mis/disinformation online and attacks on our critical infrastructure installations. **The OEWG must act now in concert with the non-state stakeholder community** to develop the frameworks and mechanisms that will help to ensure a safe and secure cyberspace.

Thank you for your time and attention.

Anne-Marie Buzatu
VP and COO, ICT4Peace
16 December 2021

Pro Memoria see Compilation of all ICT4Peace Inputs to the OEWG 2019 - 2021