Statement by Anne-Marie Buzatu, ICT4Peace Executive Director to the OEWG Informal Stakeholder Consultations, 6 December 2023

Thank you to the chair and secretariat for this opportunity to present in the Informal OEWG Stakeholder Consultations, an opportunity that we very much appreciate.

Today, my brief remarks will address three critical areas: First, the necessity of addressing mis/disinformation within the OEWG's focus on Emerging Threats. Second, the crucial need to enhance meaningful stakeholder participation in Institutional Dialogue. And third, the imperative of consistently expanding the knowledge base of law and policymakers, as well as of other stakeholders, through Capacity and Confidence Building Measures to enable informed decisions and effective regulation in the realm of ICTs, with a special emphasis on AI.

Existing and Potential Threats

We wish to highlight our deep concern regarding the evolving narratives around misinformation and disinformation in cyberspace. At the substantive meeting of the OEWG in July, Ambassador Gafoor did a masterful job of achieving consensus on the second Annual Progress Report. However, we would like to note that the threat of misinformation, previously acknowledged in the Zero Drafts of the 2nd APR, was substituted with a narrower focus on State-led "information campaigns" in the adopted APR. This shift overlooks the multifaceted nature of mis/disinformation threats, which extend beyond state actions and permeate non-state action and impact and public discourse. This overall minimizes the extremely important threat of mis and disinformation in a multitude of areas, from national elections to armed conflict, which we have seen extensively in the Ukraine conflict, and now more recently in the conflict between Israel and Hamas. Recognizing the complex dynamics of mis/disinformation, particularly when turbocharged by AI, as a highly impactful and potentially devastating Existing and Potential Threat is crucial in formulating comprehensive and effective strategies to combat it. Furthermore, we must have the terms and tools to deal with it on an international level among states and other stakeholders, which brings me to the comments regarding Institutional Dialogue.

Institutional Dialogue

In this context, we reiterate our strong support for the establishment of a Cyber Programme of Action (PoA), which aligns with our goals for a safer, more inclusive, and equitable cyberspace.

Given that cyberspace is inherently multistakeholder, and that many non-state actors have "effective control" over certain elements of cyberspace, any institutional dialogue platform, coordination, or other governance mechanism also needs to be multistakeholder in nature.

This requires meaningful participation of the different stakeholders. Not only does meaningful participation mean inclusion of stakeholders in relevant discussions that influence decision-making, it also means that stakeholders such as civil society organizations—*who are often competing against each other for a sliver of the same funding pie*—have the financial means to meaningfully participate, while retaining the civil society perspective and independent voice that makes our contributions pertinent. Therefore, we would like to propose that a fund be established and financially supported by States, and other stakeholders with financial means such as ICT companies in the private sector, in order to enable the meaningful participation by relevant civil society organizations. This is even more important given the suggestion by Ambassador at the beginning of today's session that the civil society sector self-organize and work together.

Capacity-Building

Finally, we emphasize the critical need for capacity building among policy-makers and state participants, particularly in the realm of emerging technologies such as AI. In light of the complexities and rapid advancements in artificial intelligence, a significant concern arises from the current lack of understanding and expertise among many lawmakers and policymakers in this domain. As underscored by recent discussions and reports, including an article in the New York Times on December 6, 2023, there is a growing gap between the pace of AI development and the evolution of regulatory frameworks. This disconnect not only hinders the formulation of effective and timely policies but also poses risks of unintended consequences, such as stifling innovation, infringing on privacy and civil liberties, and failing to address ethical concerns. It is imperative that we bridge this knowledge gap and foster a deeper, more nuanced understanding of AI technologies among those responsible for governing and shaping policies. Doing so will enable us to craft regulations that not only protect citizens and uphold democratic values but also encourage responsible innovation and harness the transformative potential of AI for societal benefit.

We welcome the Dedicated Global Roundtablemeeting On ICT Security Capacity building scheduled for 10 May 2024, and hope to participate in order to share our viewpoints and expertise on requisite capacity-building needs for State and other stakeholder.

In conclusion, as we navigate these emerging threats and opportunities, let us remain committed to a collaborative, inclusive, and forward-thinking approach to cybersecurity and responsible behavior online. Together, we can ensure that technological advancements serve the greater good and contribute positively to our shared future.

Thank you.