**Statement by Anne-Marie Buzatu, ICT4Peace Executive Director at OEWG Stakeholder Meeting, 26 July 2023**

Ambassador Gafoor and esteemed colleagues,

I am delighted to be part of this meeting and appreciate the opportunity to contribute to the dialogue today. Our remarks today will focus on the application of international law, institutional dialogue, and the effective implementation of the normative framework of responsible state behavior in cyberspace.

**International Law**

We echo the sentiments of many states and stakeholders in this meeting that the application of international law to the use of ICTs by states, and importantly understanding *how* international law applies to cyberspace, is a crucial step towards developing common understandings on this issue. The principles of the United Nations Charter are not only applicable but also essential in maintaining peace, security, and stability in the ICT environment.

In particular, we would like to draw attention to the following areas under international law that need to be further developed in terms of how they apply to ICTs and cyberspace:

- The Charter of the United Nations
- The application of IHL
- Peaceful Settlement of Disputes
- Protecting human rights online, including privacy, freedom of expression and rights of gender and other marginalized groups - State responsibility
- State response options

Numerous states have spoken about the need more effectively translate these areas of international law such that their spirit and intent can be faithfully applied to activities and incidents in cyberspace, and this is an undertaking that will hopefully be further addressed in future OEWG-related events, and could eventually be coordinated by, for example, a permanent platform hosted within the UN, with the inclusion of diverse expert stakeholders including academia, civil society and the commercial private sector.

**Institutional Dialogue**

We reiterate our support for the establishment of a Cyber Programme of Action (PoA) as a permanent, inclusive, consensus-based, and action-oriented international instrument to advance the implementation of the acquis on responsible behavior in the use of ICTs in the context of international security.

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.

For instance, the implementation of Norm 13 (j) regarding responsible reporting of ICT vulnerabilities, which is of the utmost importance to the security and stability of ICTs, requires the active participation of various stakeholders, including states, commercial entities, civil society, academic, technical, and other relevant communities.

To further progress on the PoA, we support an intersessional dialog dedicated to this topic, and request that the stakeholder community continue to be included in such discussions.

**Capacity Building**

Capacity building in the context of cyberspace safety and security can promote the development of skills, knowledge, and institutional structures needed to effectively address cyber threats. It is important for several reasons, many of which have been discussed over these past few days:

1. **Enhancing Technical Skills**: Cyber threats are evolving rapidly, and the technical skills needed to counter these threats need to keep pace. Capacity building programs can provide training in areas such as secure coding practices, network security, and effective incident response, helping to ensure that individuals and organizations have the skills needed to protect against and respond to cyber threats.
**2. Strengthening Policy and Legal Frameworks**: Capacity building also involves sharing the know-how with policy and lawmakers so that they can develop effective policy and legal frameworks for information technologies. This includes laws and regulations that define cyber crimes, establish accountability, protect human rights and provide the legal basis for cooperation and information sharing between different jurisdictions. From the stakeholder perspective, It also includes policies and procedures for organizations to manage cyber risks.
**3. Reducing Inequalities:** There is a significant disparity in cyber capabilities between different countries, and even between different sectors within countries. Capacity building can help to reduce these inequalities, ensuring that all countries and sectors have the ability to protect themselves against cyber threats.
**5. Building Trust:** Effective cooperation requires trust between different stakeholders, including governments, private sector organizations, and civil society. Capacity building can help to build this trust, by demonstrating that all stakeholders have the necessary skills and structures in place to manage cyber risks and opportunities effectively.

Capacity building is an activity in which many stakeholders including ICT4Peace quite active. So, this is another area in which stakeholders can contribute to the OEWG mandate, mission and aspirations.

**Points of Contact (PoC) Directory**

We acknowledge the importance of the PoC directory as a Confidence-Building Measure (CBM) in itself. The PoC directory can play an operational role if it is used as a communication platform for implementing practical, useful, and effective CBMs and promoting responsible state behavior in cyberspace.

Information-sharing, particularly in the event of cyber incidents, can vastly improve security online. The PoC directory should facilitate information-sharing between its member States, increasing transparency and strengthening common understandings of threats in cyberspace as well as ways of working effectively together to respond to cyber incidents. We also support holding regular and voluntary tabletop exercises to increase trust and predictability among States and at the same time strengthen cyber resilience at the national, regional, and global levels. Given their important responsibilities and areas of expertise, stakeholder involvement in these tabletop exercises can further increase their utility and effectiveness.

As an organization dedicated to promoting peace and security in the digital age, ICT4Peace is committed to supporting the OEWG's work. We look forward to continue working with other Member States and stakeholders in the areas of digital policy, cybersecurity, and internet governance. Together, we have the power to shape the future of cyberspace, to help ensure it remains a force for good, a tool for progress, and a shared space that benefits us all.

Thank you.