Statement by Anne-Marie Buzatu, Vice-President, ICT4Peace Foundation to the Open-Ended Working Group (OEWG) Stakeholder Session, 27 July 2022

We express our gratitude for the organization of this stakeholder session, and for providing an opportunity for non-state stakeholders to contribute to the discussions of the OEWG.

Considering the important expertise and areas of influence of the multistakeholder community, we consider it essential to achieve the OEWG's mandate that ALL relevant stakeholders are able to contribute to these discussions.

In that vein, we also express our concern that a considerable number of non-state organizations' requests to participate in next weeks' meetings were vetoed by Member States. We consider the contributions of many of these actors essential in crafting effective implementation frameworks for the work of the OEWG, and hope they will be included in future sessions.

In response to the question about the various ways in which we are currently involved in supporting and delivering capacity-building initiatives in the context of the current ICT security capacity-building landscape, for more than eight years, ICT4Peace has delivered numerous capacity-building courses on various areas related to cybersecurity. Last year we launched ICT4Peace Academy, which offers live custom-tailored courses on several topics related to cybersecurity, cyber diplomacy, application of international law to cyber and cyber norms.

Of particular relevance to the discussions this week, in cooperation with the Organization of American States, we have developed a 5-day interactive course on cyber diplomacy, law and norms in which we take a deep dive into how international law applies to cyberspace.

Through the mechanism of case studies, we analyze how international law would apply to cyber incidents according to the leading legal interpretations and through a comparative analysis of different State statements. We also take a close look at the normative framework for responsible State behavior in cyberspace, through the lens of how it would apply in realistic hypothetical situations, and consider the different roles and contributions of nonstate multistakeholder participation, as well as looking at cybercrime and cross-cutting issues such as gender in ICTs.

We consider capacity-building among states and other relevant stakeholders absolutely essential in order to more closely reach the goals of an open, peaceful and secure cyberspace. Our live, interactive courses bring together subject-matter experts and practitioners and are specifically tailored to meet the needs of the participants, including taking into account their particular national/regional and institutional contexts. The scenarios we use are realistic and inspired by real life events and help to prepare state representatives so that they are more able to effectively respond to cyber incidents when they do occur, because they do.

I will end there on this question and look forward to the next round of questions.

***

Regarding the question on how stakeholders can work with States to contribute to the implementation of concrete, action-oriented proposals made by States, we would highlight our team's extensive experience in developing effective multistakeholder approaches to governance. By including us in the room, and organizing this session, he OEWG has shown great understanding of the nature of the threats we are facing in the cybersecurity realm.

Each stakeholder, whether civil society, tech developer, subject matter expert such as in academia or States, has its important role to play in developing and implementing the frameworks that will support a safe, secure and peaceful cyberspace. Effective implementation of the normative framework will require approaches that recognize the different areas of effective control that each stakeholder brings to the table. This approach could, for example, help to inform the development of a dedicated platform for cybersecurity issues, such as under the proposal to develop a Programme of Action.

In addition, we would draw your attention to our proposal to improve transparency and accountability in cyberspace through the development of a peer-review mechanism on the order of the Human Rights Council. This would help to further develop what it means practically for States to behave responsibly in cyberspace and contribute to a growing body of good practices and standards to guide States in their behavour online. It would also provide a measure of oversight.

In closing, we thank you very much for this opportunity to speak today and contribute to the OEWG's discussions and look forward to working with all stakeholders towards practical, effective and action-oriented responses to the cyber challenges we are all facing.