Statement by ICT4Peace to Second OEWG session  
February 10-14, 2020, UN HQ

Dear Chairman, members of the Secretariat and distinguished delegates,

We are grateful to address again this important Open Ended Working Group. The Chairman through his working paper has provided us with a helpful framework for focusing the work of this second substantive session.

In describing the existing and potential threats posed by irresponsible state behaviour in cyberspace, we consider that the threat to international peace and security should be preeminent. In the context of its First Committee origins, the OEWG’s efforts should focus on steps to maintain the “cyber peace” at a time of rising geopolitical tensions and an expansion of offensive cyber capabilities on the part of several states.

When it comes to offensive cyber operations, there is considerable debate as to how existing international law applies to specific state uses of ICTs. While we would welcome the negotiation of legally binding prohibitions on some offensive cyber actions, we recognize that in the near term, adherence to politically binding measures,
such as those generated by the 2015 GGE, is probably a more feasible goal.

The Chair has posed the question as to whether member states should “..unilaterally declare to refrain from militarization/offensive use of ICTs?”.

We answer in the affirmative and remind delegates of ICT4Peace’s “Call on Governments” to publicly confirm that they will refrain from offensive cyber operations targeting critical infrastructure. This would be a proactive means for states to demonstrate their commitment in policy and practice to this agreed UN GGE norm.

We also believe it is time for sophisticated cyber/Al surveillance systems to be brought more fully into export controls as a means of preventing human rights abuses.

The Chair has flagged “attribution” as one of the issues which might require additional norms for responsible state behaviour. We believe attribution is a critical precondition for achieving accountability for state conduct in cyberspace. Capacity for objective, well-documented attribution for malicious cyber activity should be developed as a matter of urgency.
ICT4Peace has circulated a paper and launched a pilot "peer-review" process, describing one mechanism for collecting this information, drawing upon the expertise residing in the private and civil sectors. We consider that such a solid information base would complement an eventual "Peer Review Mechanism" that could serve as an inter-governmental forum for holding states to account over their cyber actions. The Human Rights Council and its Universal Periodic Review remains a relevant model in this regard.

We support the goal of the Mexican proposal to encourage reporting by states on their implementation of norms, but believe this should be but one input to a "peer review mechanism" that would provide for interactive discussion of state conduct.

In addition, in our view, the current and future importance of cyberspace for international peace and prosperity warrants a dedicated forum under UN auspices to enable on-going consideration of international cyber security-related issues. Suitable secretariat support would be required for such a forum.
Perhaps the time has come for the UN to establish an “Office of Cyber Affairs” as a manifestation of the importance the UN Secretary General has assigned to these issues through the HLP on Digital Cooperation and the preparations for the upcoming 75th Anniversary of the founding of the United Nations.

In conclusion, ICT4Peace has high expectations for this WG’s output which it believes can only be enriched by the continued input from industry, academia and civil society as evidenced in the productive inter-session meeting of last December. ICT4Peace stands ready to support this group through its capacity building and other work as it has done over the past 15 Years.

Thank you for your attention