Statement by ICT4Peace to the OEWG on Cybersecurity, UN HQ, Sept 10, 2019,

Mr. Chairman, Excellencies, distinguished representatives, colleagues,

On behalf of ICT4Peace I am pleased to have this opportunity to address the inaugural session of the Open-Ended Working Group (OEWG) on "Developments in the field of information and telecommunications in the context of International Security".

After almost two decades of UN work on developing "norms for responsible state behaviour" in cyberspace, a new, inclusive process for advancing this goal has been established. We believe the need for such norms has become all the more pressing, as some state conduct in cyberspace threatens to transform this unique, human created environment into just another "war-fighting domain" in the eyes of some.

Fortunately, earlier UN processes have generated a significant body of norms which would serve the goal, as expressed in your authorizing resolution, of preserving a "secure and peaceful ICT environment". We urge states participating in this OEWG to lead by example in implementing the norms already identified in the 2010, 2013, 2015 GGEs. As indicated in our submission to the OEWG, we believe of the eleven, these seven norms merit priority attention:

1. Non-targeting of critical infrastructure including devising common understandings as to what constitutes such infrastructure
2. Non-targeting Computer Emergency Response Teams (CERTs)
3. Non involvement of these Computer Emergency Response Teams (CERTs) in offensive cyber operations
4. Non use of proxies by states in conducting offensive cyber operations
5. Responsibility of states to prevent or prosecute malicious cyber activity originating from their territory
6. Commitment to a responsible disclosure of vulnerabilities to help preserve the integrity of cyberspace
7. Transparency of policy and doctrine governing state offensive cyber operations.

We would like to see the OEWG further develop these existing measures with a view to *operationalizing* them as soon as possible. In the absence of an energetic assertion of these norms we risk leaving cyberspace vulnerable to whatever some cyber 'warrior' decides is advantageous.

ICT4Peace has already spoken out against the deployment of malware by states into foreign electricity grids threating the disruption of infrastructure critical for public use. If states are not going to abide by a key principle of conduct that their representatives have agreed to in the UN context, we will all

suffer. International experts convened at a meeting last year by the International Committee of the Red Cross have voiced their concern regarding the upswing in major cyber-attacks including those affecting the functioning of electricity networks, medical facilities and nuclear power plants. These findings are a stark reminder of the vulnerability of essential civilian infrastructure to cyber-attacks and of the significant humanitarian consequences that may ensue.

Be it in a state of armed conflict or not, ICT4Peace believes that the prohibition on targeting critical infrastructure by cyber operations should be publicly acknowledged by states and put into practice.

This should be a priority task for the OEWG to accomplish in line with its mandate to "further develop the rules, norms and principles of responsible behaviour of States". As the Secretary General noted in his *Agenda for Disarmament,* he foresees a personal role in the prevention and peaceful settlement of cyber conflict and in "fostering a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace". It is the current lacking of accountability for "irresponsible state behaviour" that has frustrated many of us in civil society who wish to preserve this hugely important cyberspace as a zone of peace.

In this exercise of accountability, we think the "attribution" issue requires considerable work with a view to devising mechanisms of impartial attribution of internationally wrongful acts.

ICT4Peace has put forward one possible model which could lay the basis for such an attribution capacity and I refer you to our submission for further details.

The challenges posed by offensive cyber operations are not solely the concern of states and companies. Individuals and communities have been harmed through mass campaigns of disinformation and the propagation of hate speech. Ethnic cleansing and sectarian violence have been promoted through nefarious cyber operations. These abuses must be countered with determination. A human-centered security approach should also be considered by the OEWG.

Effectively addressing the myriad of challenges posed by offensive cyber operations will require the engagement of the private sector and civil society as well. We have been encouraged by the provisions the OEWG have made for receiving input from these non-governmental stakeholders. However, we hope that all NGOs, that wish to participate in OEWG process will be allowed to do so.

ICT4Peace will continue to contribute, via its programs, to the OEWG goals of confidence building and capacity building, crucial components of a sustainable cyber peace. With regards to capacity building, ICT4Peace has implemented since 2014 numerous Cybersecurity Policy and Diplomacy Courses in close cooperation with the OAS, ASEAN, AU, OSCE and the UN.

It’s great that a large number of delegations are underlining the importance of cybersecurity capacity building. But I am not sure that the need for cybersecurity capacity building has sunk in as a true development priority in the international development debate as yet. ICT4Peace has tried in the past, to raise the awareness and recognition of the emerging cyber security divide, but we are not sure this priority has been accepted by the Development Cooperation Agencies and Finance and Development Ministers of this world.

More work of convincing is needed.

I thank you for your attention and wish all participants a productive initial session.