# ICT4Peace Submission to the UN Open Ended Working Group (OEWG) on ICT and International Security

We commend the OEWG's openness to input from civil society, academia and the private sector and ICT4Peace will look forward to contributing to its work through a sustained dialogue.

The 2015 report of the UN Group of Governmental Experts (GGE) noted that even as ICTs have grown in importance for the international community, "there are disturbing trends that create risks to international peace and security. Effective cooperation amongst states is essential to reduce these risks".

More recently, the Secretary General, in connection with his *Agenda for Disarmament,* has warned that malicious activity in cyberspace has already been directed at critical infrastructure with serious consequences for international peace and security. It is incumbent on the international community to work to counter such threats and to ensure the "secure and peaceful ICT environment" that your authorizing resolution (A/RES/73/27) stipulates.

The OEWG represents the latest installment of the 20-year UN endeavour to address developments in ICTs in the context of international security. This effort has yielded some important results, notably the consensus GGE reports of 2010, 2013, 2015. Yet these positive findings have not been adequately reflected in the actual conduct of states in pursuit of a "militarization" of cyberspace. With increasing reports of state-conducted offensive cyber operations including the targeting of critical infrastructure in other countries, promoting adherence in practice to UN identified norms of responsible state behaviour is vital. If the international community is to foster digital human security alongside cybersecurity for states it will need to keep pace with these developments and ideally steer them towards cooperative ends.

It is our hope and expectation that the OEWG will deliver results that tangibly contribute to conflict prevention and preserve cyberspace as a realm for peaceful purposes. In doing so it will need to build on the accomplishments of the past, while "further developing" these and promoting their implementation. ICT4Peace believes the following norms merit priority attention:

1. Non-targeting of critical infrastructure including devising common understandings as to what constitutes such infrastructure.
2. Non-targeting of Emergency Response Teams (e.g. Computer Emergency Response Teams and Cybersecurity Incident Response Teams).
3. Non-involvement of these Emergency Response Teams 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 and transparent policies for handling such vulnerabilities.
7. Transparency of policy and doctrine governing state offensive cyber operations.

In addition to developing these norms, which have already been generated by the UN GGE processes, we suggest that the OEWG also develop proposals for dealing with four other pressing problems:

*Attribution:* The necessity for substantiation of "accusations of organizing and implementing wrongful acts brought against States" is acknowledged in Resolution 73/27, but if this norm is to be implemented it will require a reliable attribution mechanism. ICT4Peace sees merit in developing a neutral, international cyber attribution agency which could take the form of a public-private partnership drawing upon capabilities in the private sector. ICT4Peace has published a paper on this theme: https://ict4peace.org/wp-content/uploads/2018/12/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf

*Disinformation, Hate Speech and political Interference*: These actions affect every means of expression at both national and international levels, but ICTs, including social media, substantially increase their impact. Any norm in this regard to be observed in practice will require definitional and operational elaboration. As these issues are somewhat distinct from the international security context of the OEWG and could complicate its efforts, ICT4Peace suggests that separate fora may be tasked with this work.

*Export Controls*: There has been increasingly concern expressed about sophisticated cyber surveillance equipment being misused by some states to monitor individuals and impinge on their civil and privacy rights. ICT4Peace would like to see the OEWG develop a recommendation that would require states to include such equipment and software in their national export control regimes.

*AI and Cyber Security*: The potential of Artificial Intelligence to amplify some of the problematic aspects of current state conducted cyber operations will require extension of the normative framework for responsible state behaviour in cyberspace to this potent new technology. The OEWG could draw upon the earlier work of the CCW's GGE on Lethal Autonomous Weapons (LAWS) in formulating initial guidance in this regard.

Finally, we would like to stress that the cumulative economic and financial cost of cyber incidents to national economies and in particular developing and emerging economies have become enormous. Therefore, it has become evident, that national cybersecurity building has become a necessary state function. However, many developing countries lack the necessary resources to build and maintain the required national cybersecurity institutions and technical and human capacities. Cybersecurity therefore must become a priority in national development strategies and cooperation agreements. The need for cybersecurity capacity building in developing countries has already been highlighted in the UN GGE 2015 report and should also be reflected in the OEWG outcomes.

Geneva, 4 August 2019

Contact:
Daniel Stauffacher, President, ICT4Peace
danielstauffacher@ict4peace.org