ICT for peace foundation

Comments by ICT4Peace on the "Zero Draft" report of the UN Open Ended Working Group

We appreciate the evident efforts made in this "Zero Draft" to produce a cogent and accessible report prior to the OEWG's final session this March. It is generally a well-balanced account of the discussions that have taken place in the OEWG across its major themes. ICT4Peace would like to see a greater focus in the report on the future course of action recommended for this subject matter within the UN context, rather than a record of discussions. We offer the following comments on the present text with the view to enhancing the report's ultimate utility to the international community including concerned non-governmental stakeholders.

Our principal concern remains with the absence of the concept of "accountability" in the report. Experience has shown that a set of norms without any accompanying accountability mechanisms regarding their implementation is unlikely to be respected in practice. Regrettably the only time in the current text that the word "accountability" even appears (para 36) is part of a six-line, opaque sentence in which better understanding of "sources of ICT incidents" is somehow to produce "greater accountability and transparency". We would suggest substituting here a concise sentence along the lines of "States agreed that greater transparency and accountability for their cyber operations would constitute a confidence-building and conflict prevention measure."

In terms of what form the desired accountability mechanism should take, we refer to our earlier proposal for a "Cyber Peer Review Mechanism". In the context of international cyber security, a state-led process of review that also provided for inputs from non-governmental stakeholders and publicly accessible results appears best suited to ensure a credible and effective procedure. The Universal Periodic Review mechanism of the UN Human Rights Council already provides a model and precedent for such a peer review process undertaken by states. We note that the call for accountability figured in several of the informal dialogues held in December and believe the OEWG report should acknowledge its importance for promoting responsible state behaviour in cyberspace.

We commend the priority accorded the protection of critical infrastructure in the report and its warning of the "potentially devastating humanitarian consequences" of any attack on this infrastructure. The report needs to demonstrate serious concern with the harm inflicted upon humans by irresponsible state cyber actions. While we appreciate that the singling out of "medical and healthcare facilities" (par 50) in this context is not meant to exclude other critical infrastructures, the report should include a specific statement to that effect along the lines suggested by Australia and five other states in the non-paper. ICT4Peace has earlier proposed the desirability of states possessing offensive cyber capabilities to publicly commit to respecting the prohibition on the targeting of critical infrastructure. We appreciate in this regard the report's encouragement (para 74) for states to "publicly reaffirm their commitment to be guided in their use of ICTs by the 2015 report of the GGE".

As a forward-looking report the language on how UN work on cyber security should proceed in future is of prime importance. The support expressed for "frequent and structured discussions under UN auspices of the use of ICTs" (para 96) is good but needs to be expressed in a more prescriptive manner. ICT4Peace welcomes the "Programme of Action" proposal (para 99) as providing the type of "institutionalized" follow-up that the UN urgently requires to adequately address the challenges posed by state sponsored cyber operations. ICT4Peace agrees that the "regular institutional dialogue" recommended by successive GGEs must be given practical, institutional expression. A permanent forum, with dedicated secretariat support and provision for regular and review meetings aligns with our call for the establishment of a "Cyber Security Committee" under the General Assembly to be supported by a UN "Office of Cyber Affairs". We would like to see the OEWG report provide practical guidance regarding the form on-going UN work should take and would hope that the sponsors of the "Programme of Action" proposals can move rapidly to obtain the General Assembly's mandate to initiate its negotiation as soon as possible.

The need to involve other stakeholders in the future inter-governmental dialogue on international cyber security, both as concerned entities and eventual partners from the private sector and civil society is acknowledged at several points in this report. We note in particular the concluding reference to the "importance of identifying appropriate mechanisms for engagement with other stakeholder groups in future processes" (para 106). It would be preferable however if the OEWG report could provide more guidance as to the nature of these "appropriate mechanisms for engagement". There are models of such stakeholder engagement in other areas of the UN and given the high stake non-governmental entities have in promoting responsible state behaviour in cyberspace, we would favour a more substantive recommendation in this regard. Affirming the need for inclusive, transparent processes with non-governmental stakeholders granted equitable terms of participation, such as real-time rights to intervene in discussion, would constitute more appropriate language on this crucial aspect of future arrangements.

The OEWG's sessions have permitted frank discussion of the challenges posed to the maintenance of international peace and security of malicious cyber operations. After more than two decades of UN discussion of the cyber security issue, there are high expectations riding on the outcome of the OEWG. If the labours of the OEWG are to yield results that will truly help sustain a "peaceful ICT environment", its final report should provide an actionable blueprint as to how future UN work on this subject matter should be conducted.

February 2021