ICT for peace foundation

Comments by ICT4Peace on Chair's Revised Pre-draft Report – OEWG

This revision represents further progress in the effort to define an outcome of the OEWG in line with the importance of its subject matter. In our view, the OEWG's report must go beyond providing a "snapshot" of the current challenges facing global cyber security policy and chart a clear course for the UN to follow in managing these challenges going forward. In this regard we believe the following aspects of the revised pre-draft report need to be reinforced: i) restraint on offensive cyber operations; ii) accountability; iii) institutional support and iv) the role of non-governmental stakeholders. This submission will cover each of these themes in turn.

Restraint on Offensive Cyber Operations

The OEWG has recognized the pernicious effects of the "malicious use of ICTs carried out by State actors, including use of proxies" and that such use can have "significant and far-reaching negative impacts". The revised pre-draft report observes that "the use of ICTs in future conflict between States may become more likely", "absent a culture of restraint". It is correct that the report recognizes the crucial role of restraint on the offensive action of states in cyberspace, but "culture" is too amorphous a term to describe the degree of restraint required. To be effective and demonstrable, actual "measures" of restraint are needed. In other words, a framework of agreed measures and rules of restraint should be put in place to operationalize the existing norms that restrict the scope of state cyber operations that project power beyond their own borders.

Amongst the existing norms, ICT4Peace has long emphasized the primacy that should be shown the norm for the protection of critical infrastructure against cyber attacks. It is appropriate that the revised pre-draft report draws attention to "The potentially devastating human cost of attacks on critical infrastructure…"and proceeds to cite a few sectors, namely, "medical facilities, energy, water and sanitation". In our view the report should either enumerate a more comprehensive list of "critical infrastructure" or simply utilize that established term as there is a risk, in the context of protection, in specifying only a few sectors as it could leave the impression that those not named are legitimate targets. Given the importance of critical infrastructure to public well-being, ICT4Peace has advocated for governments to go beyond the tacit agreement of this norm and publicly confirm that it will be fully respected in state policy and practice (cf "Call to Governments" proposal).

Accountability

The concept of accountability for state action largely remains absent from the revised pre-draft report. Against the acknowledged backdrop of increasing "harmful ICT incidents" it could well prove futile to call for responsible state behaviour without a mechanism to hold states to account for their cyber conduct. The interests of the wide non-governmental stakeholder community demand no less. Such a mechanism is all the more important as states continue to engage in stealth offensive cyber operations, refusing to acknowledge their responsibility for interference with foreign computer systems. ICT4Peace favours a "peer review mechanism" as have been developed in other areas of UN activity, notably the

Human Rights Council's Universal Periodic Review mechanism, which allow states to take the lead in an equitable and collective process of a review of conduct while providing for inputs from concerned non-governmental entities. An endorsement of this or some similar accountability process should figure in the OEWG's outcome.

Institutional Support

The UN and specifically the First Committee of the General Assembly has been engaged with the subject of international cyber security policy for over twenty years. Frankly the time is overdue for this consideration to progress beyond *ad hoc* discussions and find an institutional home for on-going management of subject matter that has grown immensely in importance for global security and prosperity over the last two decades. As ICT4Peace noted in its March 2020 submission: "The time has come to signal that a dedicated inter-governmental forum with secretariat support is required by the UN".

We are encouraged that the "Programme of Action" proposal currently before the OEWG has recognized the need for a permanent body that would be the venue for annual meetings, quadrennial review conferences and occasional thematic sessions. ICT4Peace believes that it is time for the UN to establish a standalone "Committee on Cyber Security" under the authority of the General Assembly. Such a committee should also be supported by a dedicated secretariat fashioned as a UN "Office of Cyber Affairs". The existence of a permanent forum would also incentivize states to prepare the type of reports on implementation being advocated in the joint proposal before the OEWG as it would ensure such reports were subject to consideration at a diplomatic forum. The "Programme of Action" reflects the type of concrete result we would like to see the OEWG produce.

Role of Non-Governmental Stakeholders

To ensure the credibility of any eventual OEWG outcome it will need to integrate participation by other stakeholders in the future inter-governmental work. Enabling real-time participation by stakeholders in an observer capacity should be part of any institutionalized follow-up. Civil society and the private sector can bring much of benefit to the UN's future work on cyber security as well as being partners to governments in implementing programs that contribute to a productive and peaceful ICT environment.

December 2020