Submission by ICT4Peace to the OEWG on ICT Inter-sessional meeting, December 6, 2022

The Chair has requested input on the topics of confidence-building and the creation of a directory of national Points of Contact. The following represents our contribution to the consideration of these two issues:

Confidence-building

We all recognize that confidence regarding compliance with agreed norms and measures is an essential component of sustaining any cooperative security regime. This is as relevant to state conduct in cyberspace and respect for the normative framework that has been endorsed by UN member states as it is in other areas of international security. Confidence doesn't emerge *ex nihilo* from a single act but is gradually built up through a pattern of consistent behaviour in implementing agreed norms.

Confidence building can take several forms and generate a variety of benefits. At a basic level conflict prevention and the control of escalation in a crisis are core objectives of confidence building. In a more indirect manner, the experience of jointly cooperating on confidence building activity can enhance trust amongst participants as it contributes to greater predictability and transparency. This process is as applicable to state activity in cyberspace as it is in other areas of international security.

Regrettably, the current situation with respect to offensive cyber operations by states does not inspire confidence as to implementation of agreed norms. Unrestrained cyber operations are degrading human security. Attacks against critical civilian infrastructure are in contradiction with the norm prohibiting the targeting of such infrastructure by cyber means. ICT4Peace reiterates its call on those states that possess offensive cyber capabilities to publicly commit to respecting the prohibition on targeting critical infrastructure on which the public depends.

If confidence in the conduct of other partners to our normative framework is to be developed over time, national implementation has to be regularly demonstrated. This in turn requires enhanced transparency regarding state conduct. Completing a National Survey of Implementation as recommended by the initial OEWG is one way of providing a degree of transparency as is making public relevant doctrines and policies regarding international cyber security activity. A state might also consider confidence building measures along the lines of those existing for conventional forces, by exchanging information about planned cyber security activity and inviting observation of cyber security exercises. If such confidence building

measures cannot be agreed upon at the global level, then regional and sub-regional organisations should consider adopting them. There is also scope for cyber security capacity building to increase the level of confidence that interested states can participate in an equitable manner in international policy development.

To be most effective in building confidence however, transparency should go hand in hand with accountability. States and stakeholders alike should have an opportunity to seek clarification of international cyber activity that appears at variance with our normative framework. Equally states should be provided with an inter-governmental platform to provide explanations as to their cyber security conduct. ICT4Peace has for some time put forward a proposal for a peer review mechanism as a means of providing some accountability for state action and one which would envisage appropriate involvement by non-governmental stakeholders. Confidence does not breed in the dark and sooner or later we will need to turn an institutional spotlight on the behaviour of states in the increasingly important realm of cyberspace if we want to see our agreed normative framework upheld in practice.

Directory of National Points of Contact

Having a directory of national points of contact responsible for international cyber security policy would seem to be a useful tool. Much would depend on the comprehensiveness of such a directory and how well it would function in practice. Although the OEWG report referred to contacts at the technical, policy and diplomatic level, it would be important not to duplicate existing contact points through networks of Computer Emergency Response Teams (CERTs) as well as cooperative networks run by the cyber security technical community (e.g FIRST.org). The directory once established should be maintained by a designated body (e.g. the UN Office of Disarmament Affairs) and made available to both participating states and stakeholders. Of course, participating states would be responsible for ensuring that the national listing for points of contact is maintained and regularly updated. Periodic testing of the communication links for the points of contact could be helpful and once mature this network could contribute to the aforementioned transparency and confidence building objectives.

ICT4Peace Foundation, Geneva
Geneva 15 November