

From Words to Deeds: A Programme of Action for Responsible State Behaviour in Cyberspace

Paul Meyer | ICT4Peace

The third substantive session of the OEWG

to be held July 25-29 will be an occasion for participants to consider how the process to promote responsible state behaviour in the use of information and communication technologies (ICTs) in the context of international security can be advanced. Given the external realities of a deteriorating international security environment in which agreed cyber security norms (such as the prohibition on targeting of critical infrastructure) are being honoured in the breach rather than the observance, the current tempo of the OEWG seems inadequate to the challenges being faced.

One potential vehicle for generating a more operational product in a shorter time frame is the proposed “Programme of Action” (PoA) sponsored by some 60 states. The PoA puts some flesh on the skeleton concept of “regular institutional dialogue under UN auspices” endorsed by earlier UN processes by proposing the establishment of “a permanent, action-oriented, inclusive, transparent and results-based mechanism” with a regular schedule of meetings. In my view the term “mechanism” is too ambiguous and I would favour “forum” as a more appropriate institutional manifestation of the evident desire to arrange for on-going consideration of cyber security issues.

The existence of a permanent UN forum for cyber security matters could also help incentivize states to undertake the reporting on national implementation of the agreed framework already encouraged (e.g. via the National Surveys of Implementation and the UNIDIR Cyber Portal). An open approach to the inclusion of stakeholders would also enrich this type of informational exchange. A dedicated forum alongside regular reporting would eventually provide a basis for creating the accountability mechanisms that have been absent to date from this ever increasingly important realm of the UN’s work. ICT4Peace’s own **proposal for establishing a review mechanism** has been outlined previously.

It is encouraging that some effort was made by a subset of PoA supporters during a May event to promote the further development of the PoA in order to ensure a clearer and more consistent content for the proposal. The positive contribution of the **paper prepared** by Allison Pytlak of WILPF merits attention and further action. The suggestion to put forward a “pre-draft” of a PoA text would be an excellent next step in refining the concept and providing a basis for wider consultation and eventual negotiation.

Greater clarity is also required as to the timelines for realising the PoA which need not wait the 2025 end of the OEWG’s mandate. Seeking authorisation for a negotiating process via an UNGA resolution as early as this fall would

allow for an agreement within a near term timeframe. Such a timing would be in keeping with the urgency the situation demands and help staunch the hemorrhaging of the UN's normative framework for cyber security.

Seeing the OEWG process transiting to more operationally relevant undertakings is a widely held aim of the stakeholder community. From his first days the OEWG Chair, Ambassador Gafoor, has been clear that he doesn't want to preside over a mere "talk shop". It is time for participants to rally around a PoA that has the potential to advance in practical ways the expressed commitment of states to responsible behaviour in cyber space.

Published in Cyber Peace & Security Monitor, Vol. 2, No. 6: Action, Accountability, and Ambition, dated 22 July 2022.