UN OEWG – Walking the Talk:
For a new UN Program of Action (PoA) for Responsible State Behaviour in Cyberspace

The UN General Assembly has had on its agenda since 1998 an item entitled Developments in the field of information and telecommunication technology (ICT) in the context of international security". Soon we will be marking a quarter of a century that discussions of how ICTs or cyber technology can impact the security of states and societies have been ongoing at the UN. Progress has occurred in terms of several reports produced by a series of **Groups of Governmental Experts (GGE)** a mechanism by which a limited number of government-appointed experts (ranging from 15 to 25) study an issue over two years and issue a report with recommendations if they can all agree to it (these bodies work on consensus decision-making). The GGEs in 2010, 2013 and 2015 managed to produce such reports and they have offered up a menu of norms, principles and confidence building measures relevant to responsible state behaviour in cyberspace.

The 2015 report in particular represented a high-water mark of sorts for agreed guidance to states. It contained eleven voluntary norms of behaviour that covered some crucial areas of cyber operations. Notably, it prohibited the targeting by cyber means of critical infrastructure on which the public depends. It also banned targeting Computer Emergency Response Teams (the "first-responders" to cyber incidents) or involving such teams in offensive cyber operations. The report also stipulated that states should not employ proxies in offensive cyber operations and reaffirmed that international law was applicable to cyberspace. The General Assembly subsequently adopted by consensus a resolution (A/RES/70/237) calling upon all states to be guided in their cyber activity by the GGE report.

A newer and more inclusive UN process has been in the forefront of work on cyber security in recent years. This is the **Open-Ended Working Group (OEWG)**, which as the name suggests, is open to all member states and the proceedings of which are transparent. An initial OEWG operated in the 2019-2021 time period and succeeded in producing a report in March 2021. In part this success was a function of the division of the final report in two parts: a section approved by consensus and a "Chairman's Summary" which included proposals that were raised during the meetings, but which were unable to obtain general agreement. Among these latter was a proposal for a **"Programme of Action" (PoA)** put forward initially by a group of some 45 states.

The PoA seemed to promise, for the first time, a certain "institutionalization" of the UN deliberations and an on-going venue for consideration of cyber security issues.

Lightly modeled on the 2001 UN Programme of Action on Small Arms and Light Weapons, the PoA aimed to consolidate the UN's work on cyber security in a permanent fashion complete with biennial meetings of states, periodic review conferences and provisions for meetings of technical working groups. The PoA seemed to promise, for the first time, a certain "institutionalization" of the UN deliberations and an on-going venue for consideration of cyber security issues.

The initial OEWG has now been supplanted by a successor OEWG with a five year remit (2021-2025). The sponsors of the PoA now number 60 states and their idea has attracted the support of many non-governmental "stakeholders" in civil society and the private sector. Although the sponsors submitted an updated paper on the PoA there is still some uncertainty as to its intended nature. The paper states that **a PoA "would be established as a permanent, action-oriented, inclusive, transparent and results-based mechanism,…".** Although heavy with positive sounding adjectives, the term "mechanism" is ambiguous, as is the formula used elsewhere in the paper that the PoA is "to function as an action-oriented instrument".

Clarity has also to date not been forthcoming as to how the PoA is to be realized and its relationship to the OEWG. The sponsors' paper refers to possible consultations in 2021 and 2022 on the proposal while noting that "At the end of these consultations, a resolution could be adopted at the First Committee of UNGA to establish the PoA". This implies that a resolution could be forthcoming shortly, without however any specific time commitment.

The third substantive session of the OEWG (held July 25-29,2022) has just concluded with the adoption of the first annual progress report which will be submitted to this fall's UNGA session. The progress report states that discussion of the scope, content and structure of the PoA and its relationship to the OEWG will be the subject of discussion in the **fourth and fifth sessions of the OEWG (in March and August of 2023**). Little clarity is provided as to how the PoA is to be managed in the near term and its sponsors have yet to articulate a position as to the way forward.

For those stakeholders who are eager to see the UN deliberations to move beyond the *declaratory* to produce more *operational* results the promise of a PoA is appealing, while at the same time the lack of clarity as to its nature and timing is worrisome. The **"talk"** generated by successive UN cyber processes needs to be supplemented by the **"walk"** that tangibly promotes responsible state behaviour in cyberspace in the context of international security. 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.

The PoA by putting some flesh on the skeletal concept of **"regular institutional dialogue under UN auspices" endorsed** in earlier consensus reports would help give some institutional form to what remains an essentially *ad hoc* process. As noted earlier, 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-both mentioned in the March 2021 OEWG report).

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. The NGO **ICT4Peace** with which the author is affiliated, during the initial OEWG put forward its own proposal for establishing a review mechanism called **"States Cyber Peer Review" Mechanism"** outlined **here**:

It is encouraging that some effort was made by a subset of PoA supporters during a May 2022 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 the Women's International League for Peace and Freedom (WILPF) merits attention and further action by the concerned parties. 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 realizing 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 current international 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 Burhan Gafoor of Singapore**, 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 cyberspace.

Paul Meyer, Senior Advisor, ICT4Peace

Geneva, August, 2022

This Article was first published in the Peace Magazine.