Cyber Security at UNGA's First Committee 2021 – An appearance of harmony

The cyber security issue at this fall's session of the UN General Assembly's First Committee (Disarmament & International Security) was marked by an effort to patch up differences between leading cyber powers and present a common front. The chief product of this *rapprochement* was the tabling of a joint resolution co-sponsored by the United States and the Russian Federation. Its title "Developments in the field of information and communications in the context of international security, and advancing responsible state behaviour in the use of information and communications technologies" is admittedly quite a mouthful, but it literally reflects a merging of the two competing resolutions that had prevented a consensus approach to the issue since 2018. The resolution was adopted without a vote on November 3.

On the surface it suggests an acceptance of the new Open-Ended Working Group (OEWG) which was established at the First Committee at its 2020 session and which is to operate in the 2021-2025 framework, as *the* vehicle for the Committee's work on cyber security. The restoration of a single forum for cyber security deliberations (after two years of the initial OEWG and a GGE running in parallel) was an aim of many states and makes sense for considerations of coherence and efficiency.

At the same time, L.13 leaves out some elements that civil society has considered important in the UN's work. Notably the resolution makes no reference to the future role of civil society, the private sector and other stakeholders in the OEWG's work. There is also no explicit reference to a "human-centric" approach to cyber security that acknowledges the risks irresponsible state behaviour can pose for human security. The need to sustain peace in cyberspace has also been diluted in comparison with previous agreed texts and reference is made to ICT use "inconsistent with the objectives of maintaining international stability and security…" in which "stability" has been substituted for the standard "peace" in the usual UN formula of the need to maintain "international peace and security". "Stability" is a mercurial term and lacks the concepts of cooperation and non-use of force inherent in the word "peace".

The resolution also rather oddly treats the products of the two prior processes (OEWG and GGE) differently. "Welcoming" the final report of the GGE, but only "Recognizing" the OEWG report, even though the latter process was the more inclusive and transparent one and therefore represents greater legitimacy. The final operative paragraph soliciting member states views makes reference to "national efforts to strengthen information security", a term which has the disquieting connotation that information itself can pose a "security" threat and one that Western states have avoided in the past.

Among the most promising proposals to emerge from the OEWG proceedings was that for a "Programme of Action" which sought to establish a "permanent forum" for the UN's cyber security work and acknowledged the importance of the involvement of other stakeholders.
With 53 co-sponsors the "Programme of Action" had considerable support, but it did not make it into the agreed section of the OEWG 's report. There was some speculation that these supporters would not wish to leave further development of the proposal to the new OEWG process with its five year time horizon, but would seek to establish a separate process to elaborate the "Programme of Action". This would have required submitting a resolution in the First Committee, and this was not done. Instead the supporters made a joint statement (delivered by France) during the thematic debate portion of the session. Why the supporters opted for a statement versus a resolution is not clear, but it may reflect a calculation that they could not muster enough votes in First Committee at this junction to have a resolution adopted.

The supporters' statement that was delivered, while useful in sustaining attention to the proposal, suffered from some ambiguity as to what exactly was being envisaged. Different terms – "instrument", "mechanism", "forum" "framework" were used by various supporters of the proposal to describe the product that was to be created. The 2001 Programme of Action on Small Arms and Light Weapons (SALW) that to some degree is the model for the current proposal was both a politically binding document and a regular process that entailed biennial meetings of states parties as well as review meetings. It did not however create a dedicated, permanent forum distinct from the First Committee sessions. Further clarification is in order as to what the "Programme of Action" would represent, in terms of content, process and institutional persona, if it is to gain greater adherence.

The statement of the 53 co-sponsors signalled that the "Programme of Action" proposal would be elaborated in the context of the new OEWG. Such a context provides no guarantees that the views of non-governmental stakeholders will be taken into account. Indeed, the statement makes a distinction between the "open and inclusive" consultations among states that is envisaged for the OEWG and the "informal consultations in other venues and forums which could provide opportunities to hear the views of NGOs". Once again it seems that the inter-governmental forum discussing cyber security may not provide means for an equitable input by NGOs into the official proceedings of the new OEWG.

In part due to this concern over future access, it was disappointing for civil society observers that the "Programme of Action" supporters were not prepared to operationalize the proposal at this stage. Leaving the proposal to an uncertain fate as one of many issues to be taken up by the new OEWG is not in keeping with the sense of urgency and emphasis on concrete and actionable results that most stakeholders expressed during the initial OEWG's proceedings. The "Programme of Action" was endorsed by several non-governmental stakeholders exactly because it promised to take the UN out of the rut of circular discussion and towards something of operational significance.

ICT4Peace, for its part, believes that establishing a permanent UN institutional body to deal with cyber security issues is long overdue. Specifically, ICT4Peace has called for the creation of a

standing committee of the General Assembly as the venue for future UN work and the provision of an associated secretariat in the form of a UN Office of Cyber Affairs. Twenty-three years after the UN General Assembly first put cyber security on its agenda the establishment of an on-going body devoted to this subject of ever-growing importance is an imperative.

Paul Meyer, Senior Advisor
ICT4Peace Foundation

November, 2021