Cyber Security at the UN General Assembly First Committee – Déjà vu all over again

A Commentary by ICT4Peace prepared by Paul Meyer

On November 3rd the First Committee (Disarmament and International Security) of the UN General Assembly concluded its 2022 session by taking action on three draft resolutions before it. Regrettably, after four years of relatively harmonious handling of cyber security related issues by the Committee, a polemical tone and a divisive approach to future work resurfaced. To many observers it was a painful reminder of the situation pertaining at UNGA's 2018 session when competing resolutions led by Russia and the United States respectively were pushed through to a vote instead of cooperating on a compromise text that could have commanded universal support. As the sage Yogi Berra once remarked it was a case of "déjà vu all over again".

In 2018 the competing resolutions consisted of the US-backed one that authorized a continuation of the prevailing practice of creating restricted membership Groups of Governmental Experts (GGE) to continue work on norms to govern international cyber security policy. The Russian-led resolution countered with a new, more inclusive approach, the Open-Ended Working Group (OEWG) which enabled any interested member state to participate. Although this bifurcation of effort arguably was a drain on the UN's resources and potentially damaging as to policy coherence, in the event the two processes proceeded without conflict and succeeded in producing consensus reports in March and May 2021.

Much in these reports reiterated the work of earlier UN GGEs, notably the 2015 GGE which had recommended adoption of eleven voluntary norms of responsible state behaviour in cyberspace. Stakeholders were hopeful that the follow-up process would yield more operationally relevant recommendations. Troubling however was the fact that in the fall of 2020, before the initial OEWG had completed its work, Russia successfully introduced a resolution authorizing a second phase of the OEWG with a mandate lasting until 2025.

Already in the course of the first OEWG, several states saw the need to move beyond the realm of declaratory policy (which had largely been achieved in the 2015 normative framework for state conduct in cyberspace) to ensure a more practical and on-going process under UN auspices. This produced a proposal for a "Programme of Action" (PoA) that would serve "as a permanent, inclusive action-oriented mechanism" advance cooperation and facilitate the implementation of the agreed norms. Although sponsored by some 60 states the PoA was not supported by all OEWG members and was treated in its final report as a proposal that merited further discussion and elaboration as part of any follow-up work.

In the progress report adopted by the new OEWG after its initial year of work the PoA proposal is identified for further elaboration during the two sessions of the group to be held in March and July 2023. At this year's First Committee, the Chair of the OEWG (Ambassador Gafoor of Singapore) put forward a draft decision (L.54) that simply noted that a progress report had been endorsed and secured consideration of the cyber security issue on next year's First Committee session. Some participants might have preferred that this decision would suffice. In the event however, Russia introduced a resolution (L23) that provided direction as to the future discussions within the OEWG that appeared to usurp the Chair's authority in seeking First Committee support for the OEWG's work so far and in prejudging the focus of future sessions. It didn't help that the resolution drew in its preambular section on problematic phraseology such as "international information security" and "community of shared future for humankind" linked to the rhetoric of particular states and not commonly subscribed to.

In this context, France introduced a resolution (L73) highlighting the PoA proposal that sought to advance consideration of this idea without directly challenging the primacy of the OEWG that many member states appear to favour. The original ambitions for the resolution were likely higher, but the extensive consultations France engaged in during the session resulted in something of a diluted document. While on one hand "Stressing the urgent need to assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats…" the resolution did not attempt to force the pace of a PoA's elaboration which was tied to the existing schedule of the OEWG and the resolution specifically committed "to take into account the consensus outcomes adopted by the OEWG 2021-2025". The French Ambassador in her statement spoke of the resolution being "in synergy with the work of the OEWG" and "in keeping with the central role of the current OEWG in discussions on this proposal". The realization of a cyber PoA is now cast as "a concrete objective for the end of 2025".

The underlying tensions regarding future directions emerged in the, at times, sharp exchanges amongst the principal protagonists. The chief Russian delegate defended L.23 by claiming that "Any attempts to present our initiative as undermining the work of the OEWG and its chair are untenable and do not correspond to reality. A loving parent will not harm their child". He went on to blast "our Western colleagues, whose words are often at odds with their deeds. While publicly declaring their full support for the activities of the OEWG, in reality they are promoting an alternative document aimed at replacing the Group with a format that meets their interests".

In a joint statement explaining their vote on L.23, Canada, Australia and New Zealand decried that the "spirit of cooperation, which resulted in a consensus resolution in 2021, was not replicated this year" and led these states to "conclude that this resolution is deliberatively divisive and undermines the OEWG and the progress made by all member states in that context".

Malaysia spoke for many when it stated in its explanation of vote "My delegation would have preferred the consideration and adoption of a single document under this agenda item, so as to maintain the spirit of consensus, cohesion and common purpose evidenced during the last session of the First Committee".

In the end only the OEWG Chair's decision (L.54) was adopted without a vote, while L.23 was adopted with a vote of 112 yes, 52 no and 10 abstentions and L.73 was adopted with 157 in support, 6 opposed and 14 abstentions. Although avoiding the harmful bifurcation of effort created by the 2018 session, the machinations of the First Committee in addressing its cyber security item this year reflects the deep divides that still characterize the positions of leading powers and which are likely to continue to colour the proceedings of the OEWG. Russia has succeeded in its aim to ensure that the OEWG retains its monopoly over the UN's deliberations on cyber security affairs. Proponents of the PoA seem to have conceded that they will not be able to "fast track" its development outside of the OEWG which may mean that substantive action on the PoA will have to await the conclusion of the OEWG in 2025 (although there is no guarantee that it will be endorsed in any final report of this body).

For the stakeholders in civil society and the private sector, the return of division and rancour in the UN's discussion of cyber security will be a discouraging reminder of past polemics and contribute to a sense that significant international cooperation on state behaviour in cyberspace is not going to occur in the near term. We must be prepared to engage over the long haul in order to sustain the vision of a peaceful cyberspace.

Paul Meyer
Adjunct Professor of International Studies, Simon Fraser University
Senior Advisor, ICT4Peace