Report on the 2023 Cyber Security Debate in the UN First Committee on Disarmament and International Security.

Paul Meyer | ICT4Peace

Published first in "First Committee Monitor" Vol 21 No 5 (4 November 2023)

After a relatively low profile during the general debate segment the cyber security theme witnessed extensive participation during the thematic debate portion, taking up much of the Committee's proceedings on Tuesday, 24 October.

Ambassador Gafoor of Singapore, the Chair of the Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies 2021–2025, gave a brie ng in which he stressed the progress that has been made to date—embodied in the adoption of the second annual progress report— while highlighting the continued necessity for careful efforts to enlarge consensus. He suggested that the OEWG participants were coalescing around a concept of regular institutional dialogue that would be "a single-track state-led permanent mechanism under UN auspices." Referring to his **draft decision L.13**, he looked forward to the operationalisation of the Points of Contact directory, which should be functioning in 2024.

While most speakers were broadly congratulatory on the progress registered by the OEWG, there was an undercurrent of unease over what the Indonesian delegate referred to as "competing resolutions". The resolutions in question are **L.11, "Developments in the eld of information and communication technology in the context of international security,"** sponsored by Russia and China plus 17 other states, and **L.60/Rev.1,**

“Programme of action to advance responsible state behaviours in the use of information and communication technologies in the context of international security,” with 48 co-sponsors.

This of course is not the first time that the First Committee has been faced with competing resolutions on its cyber security subject. A similar situation occurred in 2018 when the initial OEWG and a further Group of Governmental Experts (GGE) were established, launching parallel processes within the same time frame. Although these processes were both able to agree on consensus reports in the spring of 2021, there was some relief expressed that the second iteration of the OEWG was authorised for the period of 2021–2025 without a competing process and a return to a consolidated forum for considering the cyber security issue.

The fact that the 2021–2025 OEWG was established by a resolution adopted in the fall of 2020 before the initial OEWG had finished its work was upsetting to some states that felt it had prematurely closed off certain options. Prominent among these was consideration of the proposal to agree a programme of work (PoA), understood as a “permanent mechanism” for dealing with the cyber security topic at the UN.

Russia and some of its allies have criticized proponents of a PoA as trying to set up an alternative format that would undermine the OEWG. No mention is made of the PoA in L.11. The US delegation responded to the Russian intervention by accusing it of seeking to steer the OEWG to further an “authoritarian agenda”.

France, as the lead on L.60, explained that while it and other proponents are prepared to continue to elaborate the PoA concept within the OEWG, they wish to move promptly after the termination of the OEWG in 2025 to develop the PoA by 2026. As operational paragraph (OP)4 of L.60 read, the Committee “Decides to convene a UN conference, upon the conclusion of the 2021–2025 OEWG and no later than 2026, with the mandate to deliberate on and finalize the scope, structure and contents of the PoA and the modalities for its establishment.”

This direction was diluted in a subsequent revision to L.60 that dropped the reference to convening a UN conference, substituting a “mechanism” with a more constrained mandate stipulating that decisions on the scope, etc. of the “mechanism” (no explicit reference to a PoA was retained in the operative paragraphs of L.60/Rev.1) “shall be based on consensus outcomes of the 2021–2025 OEWG.”

It appears that Brazil in particular influenced the sponsor’s decision to revise the resolution, as the delegation in its subsequent explanation of vote (EOV) said the original text would “prejudice the outcomes of the discussions in the OEWG regarding regular institutional dialogue.” This result further constrains the elaboration of a PoA within the OEWG, but evidently was considered a necessary concession by the resolution’s sponsors in order to gain support.

The spectre of parallel and competitive resolutions on the cyber security issue has shadowed the Committee proceedings. The Brazilian delegate expressed the frustration of many when he stated:

These common objectives [to promote an open, secure, stable, accessible and peaceful cyberspace] are under the risk of being sidelined by the current geopolitical circumstances. Unfortunately, once again we are dealing with competing draft resolutions related to the same issue. This situation borders on the divisive and might lead to a harmful duplication of efforts, as we witness in other areas.

As it happened, division and duplication were still the order of the day. **When action was taken 2 November on the competing resolutions, L.11 was adopted with a vote of 112-52-11 and L.60/Rev.1 was adopted with a vote of 158-10-12.**

In a joint **EOV by Australia, Canada, and Aotearoa New Zealand**, there was criticism of the “minimal opportunities to engage on resolution L.11” and the fact that the language of the resolution did not reflect consensus text or took such text out of its proper context. The EOV stressed that such “cherry picking creates division and discord.”

Switzerland, Japan, and the Philippines called L.11 “redundant” given the support for the decision L.13 on the OEWG.

China stated that it was not against the PoA but rather “fragmentation” of work on cyber security. **Malaysia,** in contrast, chose to characterise both resolutions as “mutually reinforcing”.

The Brazilian delegation in its concluding EOV on both resolutions “reiterates its call for all delegations to exercise restraint and refrain from tabling proposals on this topic until the end of the current OEWG mandate.”

On a more positive note, the draft decision L.13 introduced by Singapore on behalf of the OEWG Chair was adopted without a vote.

Nonetheless the divisions evident in this session’s treatment of the cyber security subject does not augur well for continued progress and substantive results from the two remaining years of the OEWG’s mandate.

Geneva 6 November 2023