The Plot Thickens: the UN Open-Ended Working Group on ICTs – Fourth Session

The UN's Open-Ended Working Group (OEWG) on the security and use of ICTs concluded its fourth session (March 6-10) at UN HQs in New York. The meeting was marked by a growing engagement by member states and a rich discussion of various aspects of international cyber security ranging from threat assessments, legal issues, confidence building measures, capacity building and institutionalized dialogue.

The able and indefatigable Chair, Ambassador Burhan Gafoor of Singapore, constantly sought to identify points of convergence *en route* to "concrete results" in this wide-ranging exchange of views. If nothing else the OEWG has clearly helped raise the profile of cyber security in the UN context and its crucial connection to global security and well-being.

Similar to a good detective mystery however, the plot thickens as the story progresses and as the cyber body count increases how the international community will escape the ravages of malign actors is difficult to predict. An annual progress report (APR) to UNGA will need to be agreed by the time of the group's fifth session in July and some major divergences remain in the positions of states and stakeholders not to mention the continued shadow that Russia's aggression in Ukraine casts over the proceedings.

Russian Cyber Operations

States did not mince their words in condemning the use of malicious cyber activity in violation of the "normative framework" for responsible state behaviour agreed in 2015 (which *inter alia* prohibited cyber attacks against critical infrastructure on which the public depends).

As the EU emphasized in its statement: "It is increasingly difficult to demarcate civilian and military dimensions of cyberspace as seen in the recent attacks on energy networks, transport infrastructure and space assets that also have a military function….The fact that there are countries that are willing to act in violation of the normative framework constitutes a threat in itself,". Several states condemned Russian action in Ukraine while noting that spill-over effects from offensive cyber operations could impact anyone, anywhere. The Russian representative attempted to deflect criticism of its actions, by characterizing these as a counter-productive "politicization" of the group's work.

A further manifestation of the Russian-Ukraine war was the vetoing of accreditation of many NGOs even though the overall number of stakeholders permitted to attend this session increased. As Canada stated: "we are disappointed that nearly 30 organizations were vetoed by five states. These vetoes are most unfortunate, as they deprive the OEWG

of benefitting from the full participation of reputable organizations such as Microsoft, the Cyber Peace Institute and the Australian Strategic Policy Institute".

The damage wrought by ransomware received much attention with many developing countries stressing that this attack vector now was a national security threat and not just a criminal concern. Kenya called for the creation of a repository of cyber threat information which would be a help to those struggling to enhance their cyber defences.

Legal Issues

The search for a common understanding of how international law and specifically international humanitarian law (IHL) applies in cyberspace continues to animate many delegations. There were calls for the OEWG having an inter-sessional meeting, perhaps virtually, devoted to this theme although this was contested by others. China suggested that invocations of IHL provides "a veneer of legitimacy" to offensive cyber operations, blaming "a certain country's wish to dominate [in cyberspace]". The perennial debate between those favouring a legally binding instrument to govern cyber security activity and those arguing that the existing legal framework complemented by the "normative framework" sufficed featured at various points during the proceedings.

The ICRC usefully submitted four position papers elucidating its views on the applicability of IHL to cyber operations in situations of armed conflict while recognizing that no legal consensus existed on some questions. The ICRC noted the special challenge cyber operations pose for IHL and its core distinction between combatants and civilians in a situation where an individual is "only one click away from the digital battlefield".

Points of Contact Directory

One item which the Chair would like to have the OEWG agree by its July session is the establishment of a directory for Points of Contact. He described such a Directory as constituting a Confidence Building Measure in and of itself and he conducted two informal consultations on the topic prior to the fourth session. A revised non-paper by the Chair was circulated laying out the modalities of the planned directory. Despite calls by some stakeholders (including ICT4Peace) to provide a directory that would also be accessible to non-governmental stakeholders, the plan indicates a State-controlled product that would be restricted to participating states and hosted on a password-protected website to be maintained by ODA.

The provision of national contact information (ideally both a diplomatic and a technical contact) would be solely on a voluntary basis and any interchange between participating points of contact would remain confidential unless there was mutual consent to share with a third party. Although agreement on a directory would be a "concrete result" it is difficult at this stage to judge its ultimate utility. This would be highly dependent on the level of participation and "value-added" of this directory relative to existing ones based in regional organizations. The non-paper indicates several actions over the next year that seemed aimed at facilitating participation by developing states in part by suggesting that the directory could be a tool for supporting capacity building activity.

Related to the directory was an initiative by India suggesting that a Global Cyber Security Cooperation Portal be established. Described as a "member state driven" portal, it would incorporate the directory in addition to serving as a document repository, an assistance mapping mechanism and a calendar of cyber security-related activity. India's move would seem to push aside the existing Cyber Portal maintained by UNIDIR which had received positive references in earlier OEWG reports. This appears as a further manifestation that some states wish to reassert state primacy in cyber security-related outcomes even though this is at variance with the multi-stakeholder approach to cyberspace governance.

Programme of Action Proposal and a Regular Institutional Dialogue

Proponents of the Programme of Action (PoA) proposal continued efforts during the session to promote this idea with several working papers submitted and calls for a dedicated meeting on the PoA to be held sometime in 2024 (the Chair commented that he would like to see this discussion occurring this year). The PoA while enjoying considerable support still suffers from a lack of clarity as to its nature, as illustrated by the fact that France and Egypt (the original co-sponsors of the idea when it was first put forward during the first OEWG in 2020) felt the need to table separate working papers describing their respective visions for the PoA.

The EU's own submission on the PoA avoided specifics and focused instead on the need to provide for the participation of stakeholders who will be important implementing partners. The aim of the PoA supporters now seems to be a consensus agreement emerging from the OEWG at its termination in 2025 that would inform a UNGA resolution that in turn would authorize a process to elaborate the PoA or enshrine a political declaration containing its essence. Rather murky indeed although the papers do reaffirm the original idea of creating some form of "regular institutional dialogue platform" (Egypt) or "permanent structure" (France) to deal with cyber security matters. Reflecting skepticism on the PoA proposal, China repeated its concerns that PoA supporters were preparing to circumvent the OEWG through some separate process which China would oppose. Iran stated that a PoA was no substitute for a legally binding instrument and stressed that any involvement by stakeholders would have to be of an informal and consultative nature with decision-making exclusively by states.

Interestingly the Russian Federation introduced a proposal for a "regular institutional dialogue (body)" that would operate on a consensus decision-making basis, exclusively by states and would limit non-governmental participation to a "strictly consultative and informal" format. According to the Russian proposal "the new body could exist under the UN General Assembly auspices as an open-ended working group/commission/committee/ review conference.".

The apparent flexibility as to what institutional form the new body could assume is noteworthy, if nothing more for the inclusion of the option of a General Assembly committee which happens to be the form ICT4Peace has recommended for some time as the most appropriate way of furnishing the UN with an on-going forum for considering cyber security matters. However, the sentiment was expressed by some PoA proponents

that the Russian proposal further muddied discussions, and would keep stakeholders at arms' length from deliberations in which their expertise was of critical importance.

Conclusion

There is a tendency in multilateral diplomacy to embrace a process in lieu of the production of a significant outcome as a way of ensuring that a problem is at least receiving attention and being discussed. The OEWG's Chair in his opening remarks to the session was frank in acknowledging that the landscape for ICT security has become more challenging: "The malicious use of ICTs has increased, not decreased". At the same time, he said that this situation has made the OEWG even more relevant and that "the work of the OEWG is critical because it is the only inclusive, open and transparent and democratic platform that we have today to discuss ICT security". He referenced the need for "the CBM nature of the OEWG process" and the effort "to rebuild levels of trust, and in some cases repair the levels of trust that might have shown some cracks".

Alas, while the sentiments of the Chair are laudable, we have to recognize that the edifice of trust in cyber space is more than merely cracked, but has suffered a catastrophic collapse. The restraint measures set out in the "normative framework" have been honoured more in the breach than in the observance by leading cyber powers. Lawyers can argue the particular challenges of applying IHL to offensive cyber operations, but this dimension pales in comparison to the brutal disregard of international law demonstrated by a permanent member of the Security Council in pursuit of its vile ends. In this context it will be difficult for the OEWG to make substantial progress towards the goal of a peaceful ICT environment, although there are other benefits to be derived from an expanding dialogue amongst states and stakeholders as to global cyber security governance. The OEWG is at present the chief vehicle within the UN context for sustaining this dialogue.

Amb. (ret.) Paul Meyer
Senior Advisor, ICT4Peace Foundation
16 March 2023