Interventions at the Open Ended Working Group (OEWG) Intersessional Meeting
December 2-3, 2019, New York

By Ambassador (ret) Paul Meyer, Senior Advisor, ICT4Peace

December 2 (morning session)

In the spirit of promoting an interactive discussion I refer to the earlier interventions of colleagues from FIRST and the Cyber Peace Institute to ask if there is a trend with respect to the degree of discrimination occurring in state -conducted cyber operations. The world was shocked by the damage inflicted by the "Not Petya" attack in 2017 that had effects far removed from the original target in Ukraine to cause multi-million dollar damage to a global shipping company, disrupted hospitals in the UK and destroyed data at many small and medium enterprises across the globe.
Whether these indiscriminate effects were accidental or intended is not clear, but it underlines how state cyber operations seem have paid scant attention to protecting the rights of citizens.

In order that the civilian owners and users of cyberspace do not end up as mere "collateral damage" we need to act to reinforce the norm of a "secure and peaceful ICT environment".
To this end, ICT4Peace has issued a *Call to Governments: Critical Infrastructure and Offensive Cyber Operations* (the text of which is available on our website) that seeks to have states proactively confirm that they will abide by the agreed prohibition on targeting critical infrastructure in policy and practice.

December 2 (afternoon session)

In the context of the OEWG, we are building on the *acquis* of earlier multilateral diplomacy, notably the consensus results of the three UN GGEs. While all eleven of the norms agreed by the 2015 GGE are worthy of implementation, ICT4Peace puts special emphasis on the prohibition on damaging cyber operations targeting critical infrastructure. Given the increasing dependence on such infrastructure and the dependence of that infrastructure on the proper functioning of computer systems, attacks that damage or disable the normal operations of this infrastructure could have an enormous impact on human security and societal well-being.

Despite the fact that the norms on protecting critical infrastructure were agreed four years ago, there still have been disturbing reports on state-conducted operations that have targeted such infrastructure, electricity grids in particular. In this light, ICT4Peace has in October issued a *Call*

to Governments: Critical Infrastructure and Offensive Cyber Operations urging states, especially those possessing offensive cyber capabilities, to publicly confirm that will respect the norm prohibiting cyber operations directed at critical infrastructure *at all times.* Not only will this action help reinforce the standing of the norm but will provide a proactive means of assuring the international community that these states are committed to acting in a responsible manner in cyberspace.

We believe that this prohibition should be respected *at all times*, given the continued debate over the threshold of an "armed conflict" in the cyber realm (triggering IHL) and the fact that damaging cyber operations are being carried out in peacetime. The 2015 GGE also did not condition their recommended prohibition on cyber operations against critical infrastructure in this way.

ICT4Peace agrees that the focus of the OEWG should be on *operationalizing* the existing norms agreed through the UN GGE process, rather than engaging in a proliferation of norms. There is one additional prohibition however that may merit consideration – a ban on cyber operations directed at nuclear facilities. While the critical infrastructure prohibition would cover operations against civilian nuclear facilities, nuclear weapon complexes should also be protected. As think tanks such as Chatham House and the Nuclear Threat Initiative have produced papers addressing this threat and eminent experts are now calling for a specific prohibition on any cyber operation targeting a nuclear weapon complexes, it would be appropriate for this further norm to be considered by this First Committee body.

December 3 (morning session)

We recognize the *Paris Call on Trust and Stability in Cyberspace* as an impressive effort to provide a broad-based endorsement of core principles to govern behaviour in cyberspace. Although there are a large number of supporters from international and civil society organizations (over 300) and from the private sector (over 600), to date the *Paris Call* has only been endorsed by 74 states. This is less than half of the UN membership and notably several leading states are conspicuous by their absence: US, Russia, China, India, Brazil, South Africa, Indonesia and Iran to name a few. If our aim is to ensure responsible state behaviour in cyberspace, it is evident that we will need to bring these states on board.

The resolution establishing this OEWG flagged the necessity for substantiation of "accusations of organizing and implementing wrongful acts brought against States". If this objective is to be realized, it will require a reliable attribution mechanism. The Secretary General in his *Agenda for Disarmament* has also stressed the need to foster a culture of accountability for cyber activity. ICT4Peace sees merit in developing a neutral, international cyber attribution mechanism, which could take the form of a public-private partnership drawing upon expertise in the technical security community, ICT firms, academia and civil society.

Last year ICT4Peace published a paper on this subject *Trust and Attribution in Cyberspace.* It foresees a network of contributors providing a "fact finding function" and a type of "peer

review" that could consider attribution judgments and provide a forum for accountability. Reference was made yesterday to the "Universal Peer Review" mechanism established by the Human Rights Council and this could provide a possible model for a cyber security equivalent. The ICT4Peace paper is designed to stimulate more detailed consideration of how to develop such an accountability/attribution mechanism under UN auspices. Devising a mechanism could even be a "deliverable" for this OEWG process.

We have made major collective progress in identifying key norms via the UN GGE reports and through other inputs such as those proposed by the Global Commission on Stability in Cyberspace. At the same time, we must recognize that a list of norms for responsible state behaviour without some complementary accountability mechanism could end up as a "to do" list that is never really acted upon.