“UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes”

Remarks by Dr. Daniel Stauffacher, Founder and President, ICT4Peace to Jeju Forum May 2019

As sometimes happens, an advertising jingle from the past sticks with you long after it has any commercial relevance. An American chewing gum manufacturer promoted its “Double Mint” product with the catchy tune: “Double your pleasure, double your fun with Double Mint, Double Mint Gum”. The phrase of course plays on the idea that if one thing is good, two of the same will be even better.

With respect to the protracted effort at the United Nations to develop a consensus agreement on fundamentals of international cyber security policy, doubling up has not accelerated progress to that goal.

Rather an already complex process has become more complicated and it will require some ingenious diplomacy on the part of concerned parties to obtain constructive results from the planned activity.

In order for you to appreciate what is at stake here, let me first provide some necessary background to the situation that the UN

and the wider stakeholder community concerned with cyber security currently faces.

It was back in 1998, that the UN was first asked to add the issue of “Developments in the field of information and telecommunication in the context of international security “to its agenda.

The request originated with the Russian Federation, which was evidently concerned that this potent new technology could be utilized, “..for purposes that are incompatible with the objectives of maintaining international stability and security and may adversely affect the security of states”.

This first step was influential at the UN in framing the issue of what has become known as cyber space and the activity conducted therein, although the original wording of “Information and Communication Technology” (ICT) is still favoured in UN documents.

The Russian initiative also contributed to situating state cyber conduct as constituting a “security” issue and thus the responsibility of the First Committee of the UN General Assembly which covers Disarmament and International Security matters.

Focusing on what became known as “cyber security” may have also contributed to an early adversarial attitude with respect to the new subject as the United States reacted coolly to what was

perceived as a Russian effort to constrain American development of so-called cyber weapons.

Early Russian proposals for an international treaty restricting military uses of cyber technology, ran up against the general opposition of the George W. Bush Administration towards multilateral arms control accords.

There was, however, enough support amid UN members for some examination of this new technology and its implications for international security that an initial Group of Governmental Experts (GGE) was established in the 2003-04 timeframe with 15 representatives of member states.

A GGE is a common mechanism employed at the UN to study a novel subject with a view to generating recommendations that could inform future negotiations of a multilateral agreement or other arrangement.

It is important to recall that UN GGEs operate on the basis of consensus, that is if one or more of the representatives involved disagree with the draft report prepared by the group, nothing is released.

This was the fate of the initial GGE which could not produce a consensus view on the significance, in terms of threat, to be attributed to state exploitation of ICTs for military and national security purposes.

There was also disagreement over whether information "content" as opposed to "infrastructure" should be subject to scrutiny from a security perspective. These two areas of disagreement have continued to mark (and complicate) UN efforts to develop common understandings regarding state conduct in cyberspace as I will return to later.

Despite this initial setback, the GGE process continued, reflecting the increasing recognition of the importance of the Internet in global affairs and rising concerns over malicious cyber activity, be it undertaken by cyber criminals or by states themselves.

A growing acknowledgement of the common interest that states and other stakeholders had in maintaining a peaceful cyberspace led to what now seems something of a golden period for interstate cooperation.

A series of GGEs succeeded in producing consensus reports in each of 2010, 2013 and 2015. Each of these reports yielded important findings and helped expand the area of common ground amongst the participating experts.

The 2010 report highlighted the growing use of ICTs by states as "instruments of warfare and intelligence" and the risk of misperception and escalation in the absence of shared norms of conduct. It recommended the development of "Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs,…".

The 2013 report built significantly upon the previous GGE introducing the significant conclusion that international law is applicable to the novel realm of cyberspace and that it was "essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".

This was the first time that the goal of a "peaceful cyberspace" was explicitly endorsed by the UN process. It also began to develop the "norms, rules and principles of responsible behaviour by states" that were characterized as "an essential measure to reduce risks to international peace, security and stability.".

Several specific confidence-building measures (CBMs) were enumerated by the GGE and the need for capacity-building as a complement to cooperative global efforts on cyber security was flagged.

The 2015 report represented the high-water mark for the GGE process and was the first to expand from the traditional 15 members to 20 representatives, thus responding to the growing demand by states for participation. The report notably raised the overall cyber threat perception by speaking of "a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors".

The report provided the most elaborated and specific listing of confidence-building measures that included ambitious undertakings for the international sharing of information on

vulnerabilities and mitigation strategies. The report also urged a norm of non-targeting of critical infrastructure providing public services.

The 2015 report also provided the first, albeit quite modest, opening to other stakeholders with interests in preserving cyberspace for peaceful purposes. In its concluding section the report noted that "While states have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.".

No sooner than the 2015 report was circulated that a UN General Assembly resolution authorizing a further GGE in the 2016-17 timeframe, this time with 25 members, was adopted.

The apparent positive momentum generated by the GGE process however was concealing several major problems that were to shortly manifest themselves in disruptive ways.

First, was the fact that the GGE had become essentially the only forum at the universal level for consideration of international cyber security policy.

This was a distortion of the normal function of a GGE in the UN context, which was to provide an initial expert study of a new topic with follow-up recommendations which would then be taken up by the General Assembly for action. After four almost

consecutive GGEs, three of which had produced substantive reports there had still been no take up by the wider body in terms of launching negotiation of a multilateral agreement or arrangement.

Concerns were being voiced that the GGEs had become a way of deflecting attention from actual state conduct in cyberspace while providing major cyber powers with a convenient process to point to as a sign of their "responsible behaviour".

Second, was the failure/Inability of leading cyber powers to arrive at a common security concept regarding cyber operations. The Russian Federation and China had since 2011 been promoting at the UN a *Draft Code of Conduct for Information Security* that demonstrated a concern that information content itself could represent a threat to national security and set out a series of measures for maintaining sovereign control of their "information space".

This contrasted with a Western concept of "cyber security" that stressed the integrity of the inter-connected systems and was favourable to a free flow of content with only minimal controls to protect public welfare. This conceptual difference might have been managed over time with the right cooperative spirit, but the geopolitical environment had begun to deteriorate in a major manner.

Since the Russian action in the Crimea in 2014, relations among the great powers, specifically Russia, China and the US had again become competitive and even adversarial.

State conducted cyber operations for espionage or military purposes had also become more salient with several states following the US lead in developing both dedicated military cyber units and overt offensive capabilities.

These underlying tensions came to the surface with the failure of the 2016-2017 GGE to agree on a final report.

The ostensible reason for the failure was disagreement over how international law is to apply to state cyber activity. A divide emerged between the US and Western allies on one hand and China and Russia on the other over whether international humanitarian law should apply to inter-state cyber operations which was seen by the latter as tantamount to legitimizing armed conflict in cyberspace.

In better times, the representatives may have found a way to overcome this difference, but there was no longer the evident political will in key capitals to show flexibility in these discussions.

In other words, the failure of the 2017 GGE reflected a deeper rupture in the relations of major cyber powers that had allowed for a degree of cooperation in defining what responsible state behaviour in cyberspace should consist of. Developments at the

fall 2018 General Assembly session brought this out in dramatic fashion.

Despite the fact that previous resolutions establishing GGEs had all enjoyed consensus status, the 2018 First Committee session of the General Assembly was presented with two competing resolutions setting out markedly different future paths for UN work on cyber security.

After years of supporting reiterations of the GGE format, Russia put forward a more ambitious resolution that foresaw the establishment in 2019 of an open-ended working group (OEWG -a forum in which any interested UN member state could participate) to "further develop the rules, norms and principles of responsible State behaviour" and to render a report by the fall of 2020. The resolution also incorporated elements from earlier GGEs combined with selected measures from the Sino-Russian *Code of Conduct on Information Security*.

The US for its part, championed a resolution authorizing a standard GGE in 2019 with a mandate to study the issue of possible cooperative measures and to report back to the 2021 session of the General Assembly. [i]

After years of leading on GGEs, which remain opaque mechanisms limited to a few states, Russia was now stressing the "more democratic, inclusive and transparent" nature of its open-ended working group proposal. The US and its partners were left

to defend the traditional GGE formula which had become deficient in the eyes of many states.

Although duplication is normally anathema in multilateral diplomacy, the two proponents of these competitive processes did not seriously engage in an effort to find a compromise formulation that could restore the consensus status that previous UN cyber security work had enjoyed. In the end, states were obliged to vote on both resolutions and despite the obvious disconnects and inefficiencies between them, both resolutions were adopted by wide margins.

The international community is thus faced with two disconnected processes, running on separate tracks and timetables with different scope for participants.

The UN Secretariat and others are trying to maintain a brave face about it all, but unless some logical division of labour is created for the two processes it is hard to see how they could both produce useful results.

One possibility would be to have the GGE limit itself to considering the issue of the applicability of international law to state cyber operations.

The OEWG in contrast could, as its mandate permits, further develop the normative ideas and CBMs already generated by the earlier GGE process. It could also usefully complement these by

identifying procedures for reporting on implementation thorough peer review mechanisms for instance.

The mere fact of the OEWG activity at the UN level could help spur parallel measures being developed at the regional and national levels.

The OEWG's mandate also explicitly calls for consultations with the private sector and civil society, which is a positive signal, although these sessions would have to be funded by external contributions. It will be important for some donor states or concerned corporations to provide this funding to ensure that this wider consultation occurs.

Of the two processes, the OEWG will be the first out of the gate, with an organizational meeting June 3 and the first session mid-September, whereas the GGE will only hold its initial meeting in December.

If a positive synergy is to be established between the two processes, it will require conscious leadership to that end. Once the chairpersons of the two processes are identified, these individuals should consult each other, and provision could be made for the chair of the OEWG to brief the GGE and vice versa.

Both chair persons should ensure they brief the annual sessions of the UNGA First Committee, which established the two processes, as to the progress they are making.

To conclude, in my view, the OEWG with its wider participation and greater transparency is likely to prove the more important of the two UN processes.

It has the potential to generate the take up by states of actual norms and measures and produce multilateral accords to govern state behaviour.

It is also the vehicle most open to inputs from the private sector and civil society, which have become ever more active recently in suggesting specific steps for safeguarding a peaceful cyberspace.

All concerned stakeholders will need to be vigilant and vocal in ensuring that 'great power rivalry' does not "gum up the works" for those seeking an open, sustainable and peaceful cyberspace.

Thank you for your attention.