ICT for peace foundation

The OEWG Final Report: Some Progress, Much Remains Unresolved

On Friday March 12, 2021, after one and half years of proceedings the UN Open Ended Working Group (OEWG) on Information and Telecommunications (ICT) in the context of international security, adopted a report. Given the varied perspectives of the member states engaged in the OEWG it is not surprising that agreement was only achieved on a final report by dividing the text developed over several months into two parts: a consensus section and a Chairman's Summary. The latter document was described as containing "diverse perspectives" , "new ideas" and "important proposals"(para 80) which preserved them for future reference even though they lacked universal support. As the consensus text, however, is the only part of the final report that states will accept as binding (in a political sense), this will be the focus of the present analysis.

To judge the merits of the report one has to situate it in the context of what has preceded it in the UN's work on international cyber security policy and what is to follow on in future. Since 1998 the UN General Assembly has had on its agenda an item on "Developments in the field of Information and Telecommunications in the context of International Security". Since 2003 the UN has created a series of Groups of Governmental Experts (GGEs) to consider this issue and in the years 2010, 2013 and 2015 these groups produced consensus reports on the task of identifying "norms of responsible state behaviour" in cyberspace. The zenith of these efforts came with the 2015 GGE report and its enumeration of eleven voluntary norms for states to observe in their cyber conduct. These norms covered such important elements of restraint as the non-targeting of critical infrastructure on which the public depends, the non-targeting of so-called Computer Emergency Response Teams (CERTS) which act as the "first responders" to cyber incidents and the prohibition on states employing proxies. Significantly, the UN General Assembly in 2015 adopted by consensus a resolution (70/237) which stipulated that states should be guided in their use of ICTs by the agreed norms of the 2015 GGE.

Unfortunately, rising tensions between leading cyber powers resulted in the 2016-17 GGE failing to agree on a report. The next year witnessed a bifurcation of the UN efforts with the establishment of the OEWG (open to all member states) and the authorization of a further GGE (with a restricted membership of 25 representatives).

A primordial question for many was whether the OEWG, despite the deteriorating atmosphere of emerging "great power rivalry" and the growth of "offensive cyber operations", would be able to build on the 2015 outcome and make real progress. Now that the results are in concerned observers are better placed to render an assessment on this key question. This analysis will be structured along the six themes the report is built around plus considering the fate of two of the most "action-oriented" proposals submitted to the OEWG (namely the National Surveys of Implementation and a Programme of Action) and providing some conclusions on multi-stakeholder involvement and the future course of action.

Section A Introduction:

The introduction provided a summary of the UN action that preceded the initiation of the OEWG and tried to capture some of the positive spirit that has informed it. In this light the report notes in para 6 "the international community's shared aspiration and collective interest in a peaceful and secure ICT environment for all and their resolve to cooperate to achieve it".

Section B Conclusions and Recommendations:

Existing and Potential Threats:

The report tries to characterize the current threat landscape, but the language here generally has been muted as several states opposed the more direct calls by some to condemn the growing "militarization" of cyberspace and the increasing trend of states to acquire "offensive cyber capabilities". The argument was made that it wasn't the existence of such capabilities that should be of concern, but only how they were employed. Thus in para 15 , it is blandly noted that "Harmful ICT incidents are increasing in frequency and sophistication" and in para 16 states "recall" that "several states are developing ICT capabilities for military purposes" and that the "use of ICTs in future conflicts between states is becoming more likely" without relating these two phenomena to each other. Para 18 echoes the 2015 prohibition norm regarding critical infrastructure in concluding that "there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities" on such infrastructure. This section concludes (in para 22) that "In light of the increasingly concerning digital threat landscape…States underscored the urgency of implementing and further developing cooperative measures to address such threats". While expressing a sense of urgency is appropriate this section doesn't reflect it and stipulates no new measures of restraint on state cyber operations beyond their borders.

Rules, Norms and Principles of Responsible State Behaviour:

This core section is largely a reaffirmation of what states have already pledged to do some six years earlier. There are references back to past resolutions, but little in the way of any advance on the past agreed norms. Characteristic of the 'treading water' nature of this section is the para 27 statement "States affirmed the importance of supporting and furthering efforts to implement norms by which states have committed to be guided at the global, regional and national level". Similarly, para 32 of the recommendations is a verbatim reiteration of the 2015 agreed norm against targeting critical infrastructure. Is sheer repetition of a norm likely to make it any more respected in practice, especially when the last few years have been marked by a disturbing rise in reports of state conducted offensive cyber operations doing just that?

International Law:

Although the GGE reports established the principle that international law applies to cyberspace and the conduct of states within, how exactly the law applies to the activities of states remains an open question. Indeed, disagreements over this issue was the principal reason for the failure of the 2016-17 GGE and has continued to cast its shadow over the OEWG proceedings. The final report represents a simple reiteration of the *status quo* and its recommendation in para 40 consists of suggesting that "States continue to study and undertake discussions within future UN processes as how international law applies to the use of ICTs by States as a key step to clarify and further develop common understandings on this issue". This kicking the problem down the road was disappointing, if foreseeable given the views of influential states. The fact that IHL is only operable in a state of armed conflict has led some states to take the view that such a condition should not be allowed to occur in cyberspace. Even the ICRC's plea to insert text to affirm the applicability of international humanitarian law to the cyber realm, while asserting that this did not represent condoning the militarization of cyberspace or legitimizing cyber warfare, was rejected.

Confidence Building Measures:

Confidence Building Measures (CBMs) have been a mainstay of past GGE reports and the OEWG sings their praises without providing much in the way of new material or direction. A paean to the various benefits of CBMs is given in para 41, such as the statement "CBMs can also support implementation of norms of responsible behaviour, in that they foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States". No new CBMs however are put forward unless one counts a recommendation in para 51 that "States, which have not yet done so, consider nominating a Point of Contact, inter alia at technical, policy and diplomatic levels" and that "States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level". Continuing to consider rather than taking action, regrettably marks this section as it does several others in the OEWG report.

Capacity Building:

This subject which had already featured in earlier GGE outputs received further elaboration in the OEWG report, which flagged that capacity building was an important aspect of the international cooperation required to achieve the "open, secure, stable, accessible and peaceful ICT environment" that has been the established goal of the UN process. In para 56 a set of principles for guiding capacity building efforts is provided which could prove a useful reference in future. This section also contains an apparent endorsement of the "National Survey of the Implementation of UNGA Resolution 70/237", an Australian-Mexican proposal submitted to the OEWG for regular reporting on the national implementation of agreed norms. Although still appearing with the "on a voluntary basis" caveat, and uniquely in the context of sharing information on capacity building efforts, the report's suggestion that states may wish to employ

this model for exchanging information, represents the only endorsement of a substantive proposal previously presented to the OEWG in its final report.

Regular Institutional Dialogue:

Although earlier GGEs had called for the continuation of a "regular, institutional dialogue under UN auspices" there were high hopes that the OEWG would provide actionable guidance on what form such a dialogue would take. Matters were complicated however when the UN General Assembly adopted a resolution (75/240) in December 2020, well before the conclusion of the current OEWG, that created a new OEWG to operate from 2021 to 2025 with essentially the same mandate. To many observers this action seemed to be pre-judging the outcome of the current OEWG.
This issue of follow-on became all the more acute in light of the presentation by some 50 states of a proposal for a "Programme of Work" lightly modeled after the 2001 UN Programme of Work on Small Arms and Light Weapons. This Programme had as one of its principal features the consolidation of the UN's work on international cyber security into a single permanent forum which would hold regular meetings as well as review and ad hoc thematic sessions and which would be provided with secretariat support. This proposal was the most practical and results-oriented option submitted to the OEWG. It was in line with ICT4Peace's long-standing call to institutionalize the UN's work on cyber security by establishing under the General Assembly a "Committee on Cyber Security" and provide that committee with dedicated secretariat support via a UN "Office of Cyber Affairs".

The Programme, however, did not enjoy universal support which meant in the end it could only be acknowledged as one proposal among others. This lead to the final report's statement in para 77-"States note a variety of proposals for advancing norms of responsible state behaviour in ICTs, which *inter alia* support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action…In this regard the Programme of Action should be further elaborated including at the OEWG process established pursuant to General Assembly resolution 75/240"

In so far as the OEWG offers any guidance as to the nature of the body which would carry out the regular, institutional dialogue, it is contained in para 74: "States concluded that any future mechanism for regular institutional dialogue under the auspices of the UN should be an action-oriented process with specific objectives, and building on previous outcomes, and be inclusive, transparent, consensus-driven and results-based". Of course, the real challenge is devising a mechanism that meets these general criteria and which can finally demonstrate an on-going and substantive capacity at the UN to deal with the many issues relating to international cyber security.

Multi-stakeholder Participation:

The OEWG Final Report, as its proceedings throughout, suggest a mixed message with regard to participation of non-governmental stakeholders. Ambassador Lauber demonstrated a commitment to engaging such stakeholders and created the important enduring legacy of the dedicated OEWG website in which submissions from all categories of participants were treated in an equitable fashion. Regrettably however, many non-ECOSOC accredited civil society and private sector entities that sought accreditation to the OEWG were refused. While a successful session was held in December 2019 providing for a substantive exchange of views with non-governmental stakeholders and official delegations, this had to be conducted as an "informal" meeting separate from the OEWG and presided over by a chairperson from outside of the OEWG. In the final session of the OEWG, non-governmental stakeholders were excluded completely even though a few states took it upon themselves to organize informal virtual consultations on the report which probably strengthened the Chair's hand in issuing his summary. Lip service is paid at several points in the final report to the complementary role of non-governmental stakeholders, but no redeemable guarantees are issued regarding their rights to be meaningfully involved in any future process. The most on offer is an acknowledgment in para 71 that states affirm the importance "of identifying appropriate mechanism for engagement with other stakeholders in future processes".

Conclusions:

The OEWG in its work from September 2019 to March 2021 provided an important forum for discussing issues relating to international cyber security affairs and the role of the UN in dealing with this subject matter. On the basis of the Final Report, an observer can conclude that modest progress has been made with respect to this work and the group's mandate. Many in the stakeholder community would have wished for more concrete results emerging from the OEWG, along the lines of the "Programme of Action" proposal. The fate of this proposal will now be largely up to its sponsors and friends. Will they be content to continue its "elaboration" over the next five years of the new OEWG, or will they want to press for more rapid action, perhaps through a UN General Assembly resolution to initiate a dedicated process to develop its text and modalities. To be successful in such an endeavour would however require expanding the support base well beyond the original sponsors.

A fundamental deficiency in the OEWG Final Report is the total absence of the concept (and even the very word) of "accountability". ICT4Peace and many in civil society felt that agreement on norms of responsible state behaviour would have little real impact if they were not accompanied by some form of mechanism to hold states to account for their cyber security actions. This concern underpinned ICT4Peace's proposal for establishing a "Cyber Peer Review" mechanism which would have provided for a state-led review process coupled with input from the wider stakeholder community. The absence of the "accountability" theme in the Final Report of the accountability imperative was especially disappointing as throughout the period of the OEWG's

existence media reports were filled with alarming accounts of state offensive cyber operations, several of which were in direct contravention of the agreed 2015 norms.

After twenty plus years of UN discussions of ICT in the context of international security, we still seem some way off from creating an inter-governmental forum to be the "go to" institution for dealing with this subject matter on a regular basis. No one believes the challenges of international cyber security policy and practice are going away any time soon and these challenges are likely to take on ever greater significance for global security and well-being. The OEWG has provided a modest impetus to this endeavour, but much more is required of states and stakeholders alike if the goal of a "peaceful ICT environment" is ever to be attained.

Paul Meyer, Senior Advisor, ICT4Peace Foundation
Geneva, 21 March 2021

ICT4Peace Engagement in the OEWG:

ICT4Peace was an active participant in the OEWG from the start. The following is a compilation of official submissions to the OEWG plus various commentaries on its work:

ICT4Peace Submission to the UN Open Ended Working Group (OEWG) on ICT and International Security (4 August 2019)

Critical Infrastructure and Offensive Cyber Operations – A Call to Governments (21 October 2019)

ICT4Peace proposed "States Cyber Peer Review" Mechanism (1 March 2020)

Statement by ICT4Peace to Second OEWG session, February 10-14, 2020, UN HQ

Letter by ICT4Peace Foundation to Ambassador Lauber, Chair of the OEWG on the pre-draft of the OEWG report (27 March 2020)

Comments by ICT4Peace on the Chair's Revised Pre-draft Report – OEWG (December 2020)

Comments by ICT4Peace on the "Zero Draft" report of the UN Open Ended Working Group

Pro Memoria: The OEWG negotiations often referred to the Norms of responsible State behavior and CBMs agreed in the UN GGE Report 2015 (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) and endorsed by UN General Assembly.

An overview of the ICT4Peace activities since 2011 calling for and supporting the UN GGE and UN OEWG processes you find here.