ICT for peace foundation

POLICY BRIEF

INCREMENTAL PROGRESS OR CIRCULAR MOTION? THE UN GROUP OF GOVERNMENTAL EXPERTS REPORT 2021

Paul Meyer

GENEVA 2021

ICT4Peace Foundation

ICT4Peace Publishing, Geneva. July 2021
Copies available from www.ict4peace.org

INCREMENTAL PROGRESS OR CIRCULAR MOTION? THE UN GROUP OF GOVERNMENTAL EXPERTS REPORT 2021

Paul Meyer

ICT for peace foundation

INCREMENTAL PROGRESS OR CIRCULAR MOTION? THE UN GROUP OF GOVERNMENTAL EXPERTS REPORT 2021

Making progress on complex issues in a forum like the United Nations with 193 state parties and a consensus decision-making procedure is always going to be a challenge. It becomes even more difficult when the subject matter, in this case international cyber security policy, is contested by influential states. It is understandable that when a forum can actually arrive at a consensus outcome, with no state opposing, it is often celebrated as a victory in and of itself.

Such a "victory" however can ring hollow, if the progress achieved appears more of a circular than linear nature.

This situation is evident in the final report of the UN Group of Governmental Experts (GGE) on "Advancing responsible State behaviour in cyberspace in the context of international security" adopted at the group's fourth and final meeting May 28, 2021.[1] The GGE which operated in the 2019-2021 timeframe with 25 nationally appointed "experts" was the most recent in a series of six such GGEs that have been organized by the UN since the turn of the century.[2] Two of these (2003-2004 and 2016-2017) failed to achieve consensus and didn't produce a substantive report. Four were able to agree on consensus reports in 2010, 2013, 2015 and the most recent in 2021. The chief aim of all these GGEs was to develop "norms of responsible state behaviour in cyberspace" as part of the effort to determine how the potent technology of the Internet and related computer networks could be managed in light of the UN's goal of maintaining international peace and security.

1 Final Report (Advance copy) of GGE on "Advancing responsible State behaviour in cyberspace in the context of international security" UN, May 2021 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

2 The states participating in the present GGE were: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russia, Singapore, South Africa, Switzerland, UK, United States and Uruguay.

One of the most difficult problems that the GGEs faced was the question of how the conduct of states in cyberspace related to international law, including international humanitarian law. A major accomplishment of the 2013 GGE was the affirmation that international law, including the UN Charter, applied to cyberspace. It was soon apparent however that this affirmation had not resolved underlying differences over the interpretation of how international law applied to the cyber conduct of states, particularly in the context of international security. Disagreement over this question had been the proximate reason for the failure of the previous GGE to reach a consensus outcome in 2017. The place of international humanitarian law (aka the law of armed conflict) in this new realm of military operations was especially contentious. Some states sought a confirmation that international humanitarian law would cover state cyber operations, whereas others resisted the notion arguing that this could sanction treating cyberspace as a legitimate domain for armed conflict.

This dispute surfaced in the proceedings of the UN Open-Ended Working Group (OEWG) on "Developments in the field of Information and Telecommunication in the context of International Security" which ran in parallel with the GGE in the 2019-2021 timeframe and was able to arrive at a consensus report at its final meeting in March 2021.[3] This result was only achieved by dividing the report into two sections: a section that had consensus approval and a "Chairman's Summary" which contained elements that were not able to command consensus agreement and had to be issued in a non-binding manner under the Chairman's own authority.

The international humanitarian law issue fell victim to this cut being relegated to the Chairman's Summary despite the support of many states and an energetic plea by the International Committee of the Red Cross to preserve a positive reference to it in the main report. The ICRC argued that acknowledging that international humanitarian law would apply to an armed conflict occurring in cyberspace should in no way be construed as condoning the militarization of cyberspace or legitimizing cyber warfare. In the event this construction was not sufficient to persuade skeptical states to accept the ICRC's proposed text in the consensus report.

The fate of this issue in the OEWG is relevant to that of the GGE as observers had hoped that the latter forum (operating under a very similar mandate to that of the OEWG) might be able to provide "value added" to the OEWG proceedings by clarifying

3 For an ICT4Peace assessment of the OEWG report see "Some Progress, Much Remains Unresolved" https://ict4peace.org/wp-content/uploads/2021/03/OEWG-FinalReportAnalysisMar212021PM.pdf

this crucial relationship between state conduct and international law. Part of this hope rested on the smaller grouping of the GGE and its more private deliberations. While the issue was addressed in the GGE report it was not resolved. Essentially the question was kicked down the road by the GGE. The key sentence reads: "The Group recognized the need for further study on how and when these principles [IHL] apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict".[4] As much in the way of offensive cyber operations conducted by states, which the GGE refers to as "malicious activity", happens below the threshold of armed conflict the international community is not really any further along in its understanding of what legal constraints apply to these operations.

This gap is all the more worrisome when one considers the major growth in damaging and disruptive offensive cyber operations carried out by states and/or non-state actors in the past couple of years that the GGE and the OEWG have been functioning. This increased level of threat is acknowledged by the GGE at several points in its report: "Incidents involving the malicious use of ICTs by States and non-state actors have increased in scope, scale, severity and sophistication"; "The Group underlines the assessment of the 2015 [GGE] report that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely"; "The Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of States."; "Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally… have become increasingly serious."; "The COVID-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain"; "New and emerging technologies expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity". After such a litany of rising threats the Group's conclusion that "Such activity can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals" comes across as understated and anticlimactic.[5]

In the face of these burgeoning threats what defences has the GGE to offer? It basically can only revert to the eleven norms of responsible state behaviour agreed as part of the 2015 GGE. A rather limp injunction is directed at those responsible: "States are

4 Final Report of GGE, pg 14

5 Ibid, pg 4

called upon to avoid and refrain from the use of ICTs not in line with the norms of responsible state behaviour".[6]

The impression left in reviewing the chief body of the report, which consists of reproducing the 11 norms of the 2015 GGE with some annotation, is that matters have not progressed much beyond the norms agreed six years ago. While the GGE claims that it has "developed additional layers of understanding to these norms" these layers seem rather thin and even threadbare.

Frequently, the report simply offers up a tentative recommendation for states to consider further action in realizing the normative goals. For example, in a section on the issue of attribution, the report "...recommends that future work at the UN could also consider how to foster common understandings and exchanges of practice on attribution".[7] The task is passed on to some unspecified body at some indeterminate future point in time.

Similarly, in a section devoted to cooperation to counter terrorist or criminal use, the report's advice is that "States may need to consider whether new measures need to be developed in this respect".[8] The report notes the utility of common templates to facilitate requests for assistance and the response to them, but then merely states: "Such templates could be developed at the bilateral, multilateral or regional level".[9] On the sensitive issue of vulnerability disclosures (and the unmentioned black market in "zero-day" cyber exploits in which government buyers have driven prices up exponentially) the report again manages only a convoluted and theoretical response: "At the national, regional and international level, States could consider putting in place impartial legal frameworks, policies and programmes to guide decision making on the handling of ICT vulnerabilities and curb their commercial distribution as a means of protecting against misuse that may pose a risk to international peace and security or human rights and fundamental freedoms".[10] Too often the report's recommendations have a diffuse, aspirational quality of the "somebody might consider doing something about this at some point" variety.

6 Ibid, pg 5

7 Ibid, pg 6

8 Ibid, pg 7

9 Ibid, pg 10

10 Ibid, pg 12

The GGE like the OEWG before it, gives only a brief, ritual nod to the contribution that other stakeholders ("the private sector, civil society, and the technical community") could make to inter-state dialogues.[11] The GGE in its consideration of the existing norms also fails to recognize the positive role that accountability mechanisms for implementation could play in incentivizing states to align their cyber practices with the "norms of responsible behaviour" they have endorsed. As with the OEWG, the GGE has not really advanced tangible action to curb malicious cyber activity. Regrettably, the GGE efforts seem to have yielded more circular motion than real progress. Translating the 2015 norms from the status of declaration to one of implementation remains, six years after they were agreed, largely unfinished business for the UN.

Paul Meyer, Senior Advisor, ICT4Peace
June 12, 2021

11 Ibid, pg 16

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peace-building, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organizations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with a book, published by the UN ICT Task Force in 2005 on the theory and practice of ICT in the conflict cycle and peace building[12] and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.[13]

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation

12 https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2005-Information-and-Communication-Technology-for-Peace.pdf

13 Para *36. We value the potential of ICTs to promote peace and to prevent conflict which, inter alia, negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction.*