CYBER PEACE & SECURITY MONITOR

Civil society perspectives on the Open-ended working group on developments in the field of information and telecommunications in the context of international security

VOL.01 NO.06

10 February 2020

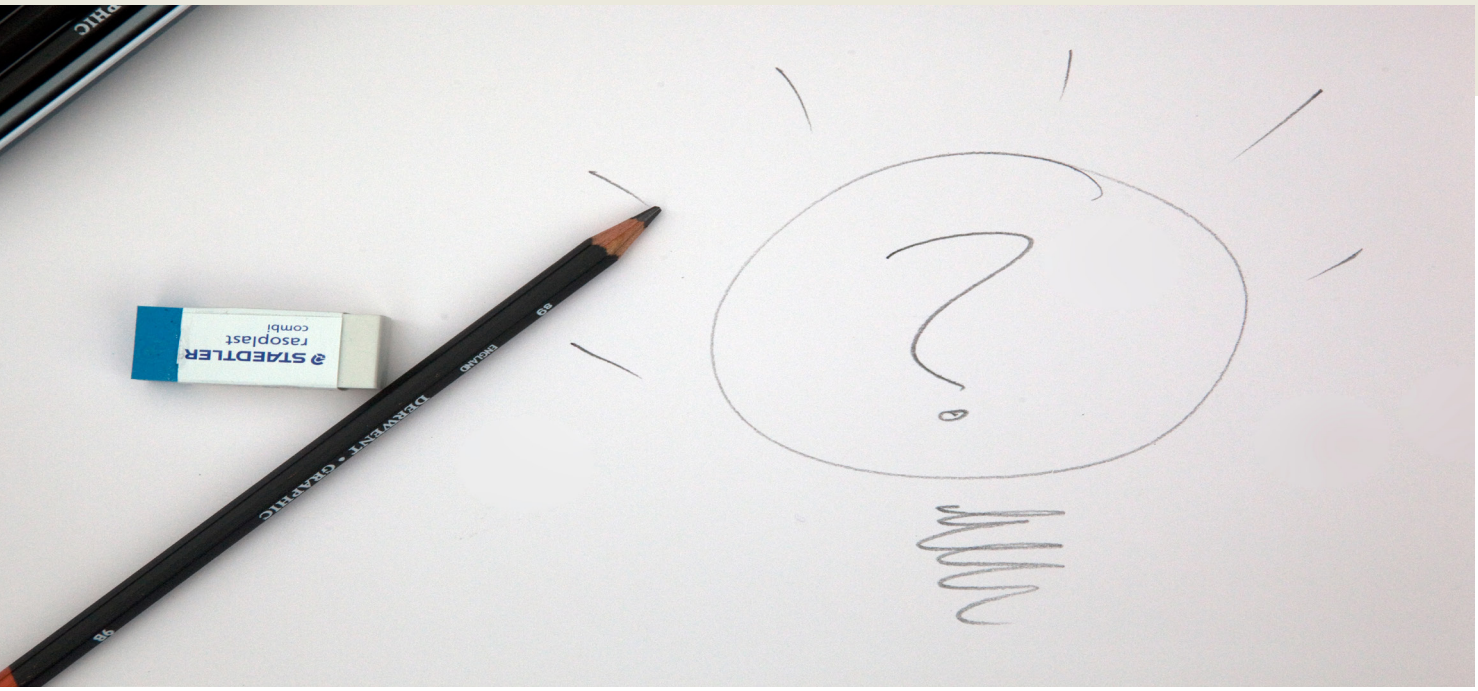

Photo by Mark Fletcher-Brown, Unsplash

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

A PROGRAMME OF THE WOMEN'S INTERNATIONAL LEAGUE FOR PEACE & FREEDOM

www.wilpf.org

EDITORIAL: FINDING PURPOSE

Allison Pytlak | Women's International League for Peace and Freedom

The constructive atmosphere of the first substantive session of the United Nation's Open-ended working group (OEWG) "on developments in the field of information and telecommunications in the context of international security" set a necessary and important tone for its future work. The OEWG is the first open and inclusive UN forum to discuss digital technologies in the context of international security. It emerged, unfortunately, in a situation of intense politicisation, deadlock, and grandstanding—which is why the positive spirit and quality exchanges during its first session were an encouraging sign that states are committed to moving past the polarisation and tension surrounding the OEWG's establishment and are eager to engage in this area of work.

This is a good basis on which to begin the second session. Few items on the UN agenda feel as pervasive and rapidly evolving as information and communications technologies (ICTs), and their misuse, making it all the more urgent that meaningful and effective outcomes be reached.

The state of play

Ambassador Lauber, chairperson of the OEWG, states in his working paper that the objective of this second session will be to "deepen the discussion of the First substantive session and reflect on various aspects pertaining to the OEWG's mandate in more detail…". The working paper provides his observations and takeaways from the first session as well as some questions to focus the discussion. Afterward, a pre-draft of the final report will be prepared and states will come together for two informal consultations to discuss and negotiate, ahead of the third and final OEWG session in July—which is where the report will be put forward for adoption, which must be agreed by consensus.

The proposed outline for the final report is a good approach. It gives space under each of the six substantive OEWG topics to identify points of agreement and where more discussion is needed as well as to offer conclusions and recommendations, which would be negotiated. This could mean that there is less potential for obstruction as long as all views are (faithfully) represented—although "nothing is agreed until everything is agreed", as goes a familiar refrain at the UN.

This is a good basis on which to begin the second session. Few items on the UN agenda feel as pervasive and rapidly evolving as information and communications technologies (ICTs), and their misuse, making it all the more urgent that meaningful and effective outcomes be reached.

There are points of agreement in many of the discussion topics. Most participating states have expressed similar concerns on the threat landscape, albeit some with greater detail than others and it is important to acknowledge that countries prioritise threats in different ways. All recognise the benefits of technology for socio-economic development and are keen to preserve a technology neutral, and behaviour-focused, approach. There was also widespread recognition in September of the importance of capacity- and confidence-building measures, and to build on regional cooperation and initiatives. A point highlighted by many delegations was practicality, with urgings to avoid politically charged and possibly unproductive avenues of discussion in future OEWG sessions. Finally, another major takeaway was the recognition from virtually all participants to not "start from scratch" and take existing practice and normative agreements as a baseline of discussion.

Implicit in "not starting from scratch" is the understanding that international law applies in cyber space, and that this should not be undermined. Most states and many non-governmental actors support this view, although

many point out that this assertion needs further unpacking, such as by better explaining how international law applies. Some states assert that it may apply but appears insufficient to constrain state behaviour. Some of these states therefore support steps that would lead to new international law, possibly through binding norms or a treaty. There is also a small grouping of states that contest the applicability of international humanitarian law (IHL) to operations in cyber space on the grounds that doing so legimitises conflict in cyber space and contributes to its militarisation. This is different than the concern that has been expressed by some civil society organisations about militarisation, which comes from a place of contesting the weaponisation of technology and militarism more broadly. In fact, some of the states who do not accept the applicability of IHL for this reason are some of the most aggressive actors in cyber space.

Apart from these more easily identifiable areas of convergence and divergence are a multitude of other points where opinions may differ: should the OEWG account for the actions of non-state actors in cyber space, for example? How to apply a more human-centric approach to international cyber security and grapple with human rights dimensions? It is also important to remember that not all countries have been engaged in these discussions for as long as some others and are now developing positions and understand the dynamics and evolution of the UN dialogue on this subject. As that occurs and the conversation expands, there is the potential for other priorities to emerge.

The fate of the multi-stakeholder approach

A question from many in civil society is if the informal multi-stakeholder consultative meeting held in December 2019 will have any bearing on the process going forward. This was always a planned part of the OEWG's timeline yet took on new significance after many civil society groups were denied access to participate in the first substantive session. The meeting then became the only opportunity for representatives of non-governmental organisations, academia, and industry to meaningfully input and engage on the same six topics that states speak to during formal sessions.

Some hoped that the high turnout and expert inputs from the more than 100 organisations that attended the December meeting would have sufficiently demonstrated the added value and logic of having these stakeholders in the room. Yet, the 30 organisations without ECOSOC status that applied to attend this session have been denied accreditation. This includes reputable research institutes, advocacy networks, and private technology companies that together possess significant knowledge and expertise in this area. As we noted in September, such a broad and categorical denial of access is extremely rare in UN disarmament and arms control fora and sets a dangerous precedent, not least when those affected have credible background and expertise to the issue at hand.

There are credibility and practical risks to shutting out stakeholders.

There are credibility and practical risks to shutting out stakeholders, especially those with a role to play in implementing decisions taken by the OEWG and can provide subject matter expertise. At the same time, it is worth remembering that participation in a global meeting is only one kind of multi-stakeholdership; national dialogue processes and consultations between government representatives and a range of civil society actors are encouraged. A "stakeholder" is someone or something with an interest in, or will be impacted by, a decision or an action. A worthy question is, who then is going to be impacted, positively and negatively, by the decisions made in the OEWG? Conversely, how are the interests of those affected being represented in multilateral spaces?

Mr. David Koh of Singapore chaired the multi-stakeholder meeting. His summary will be presented formally on the first day of this meeting. The summary has also been shared with all member states, who may choose to advance some of the content. It is comprehensive and wide-ranging, picking up on a lot of the specific proposals made in December. It also helps to identify where there are similar and different views among the stakeholders present–and between

some stakeholders and governments. There are also unofficial summaries available, such as from Global Partners Digital and Citizen Lab, alongside our reporting.

Identifying a common purpose

Questions about the OEWG's purpose and what it will produce have been central since its inception, not least because of the parallel process taking place in the form of the UN's sixth Group of Governmental Experts on ICTs. Each process puts pressure on the other to deliver a result, which should ideally be complementary and avoid duplication or redundancy. As noted above, suggestions from states so far on possible OEWG outputs—which would be captured as recommendations in the final report—are largely practical in nature. There is no shortage of ideas; around 10 states have prepared working papers in the last five months with suggestions in this regard.

Within topics where there is broad support, the next step will be to establish clarity on what a recommendation or a conclusion could look like, and if it will enjoy the support of all. For example, does recognition of the need for more capacity-building measures translate into a specific course of action? Does an acknowledgement that regular institutional dialogue would be positive mean that all states have a similar view on the form that dialogue could take? It is time to start moving toward this kind of specificity. The GGE and the OEWG are both under pressure to deliver results, which will be important to help the UN in preserving its role as a central forum for discussion on international cyber security. The emergence of other normative processes on international cyber security in the last few years shows that the global community takes this issue as a priority and will act through other channels to address threats there, if UN mechanisms are too slow or too deadlocked.

Purpose is also a question that sometimes arises in reference to the eleven voluntary norms of state behaviour developed by the UN's fourth GGE on ICTs, in 2015. This is not to say that that these norms are not underpinned by specific objectives—they each were carefully crafted and negotiated—but rather that as viability hangs on their implementation, which has been patchy, some question the purpose of the norms and where they fit in the landscape, five years after their adoption. Varied understandings of key terms contained within the norms, as well as differing levels of awareness about their existence has hindered implementation.

This may be due in part to the fact that they were developed and negotiated by a small group of states. That was no easy feat, but as the rest of the UN membership didn't participate closely in the process there may not be the same level of direct buy-in and ownership, or understanding about why and how they came to be. These problems have been coupled by other practical challenges, such as those of attributing responsibility for cyber operations, and no real way to monitor compliance, much less address non-compliance. If the OEWG's outputs could include practical steps that address some of these challenges while also cultivating wider ownership and involvement, we would take an important step forward in better assessing the on-going impact of the norms but also curtail aggressive behaviour in cyber space.

INTERVIEW WITH THE WORKING GROUP CHAIR

Allison Pytlak | Women's International League for Peace and Freedom

As the OEWG moves into its second session, WILPF wondered what its Chair is thinking about the process and its possibilities. We interviewed H.E. Mr. Jürg Lauber, Permanent Representative of Switzerland to the United Nations in New York, in his capacity as the Chairperson of the OEWG.

How do you feel about the OEWG process so far, both in terms of participation and content?

We have seen a very high level of participation throughout both the OEWG's first substantive session in September and the informal intersessional consultative meeting with stakeholders in December. More than 100 delegations participated in the first substantive session and more than 70 took the floor. At the informal intersessional consultative meeting with stakeholders, besides numerous representatives from governments, more than 100 organisations from industry, civil society, and academia participated. Delegations raised numerous issues that are of concern to them, such as artificial intelligence, internet of things, autonomous cyber attacks, or the need for a human-centred approach. The broad participation and high level of interactivity in our discussions shows that the issue is of relevance to all of us, and that governments and other stakeholders are willing to engage on these topics at the multilateral level.

What would be a productive or useful outcome from the OEWG?

The OEWG is the first opportunity for the whole UN membership to discuss this topic openly. I don't see it as the task of the Chair to decide what outcome would be most productive or useful, as this will have to be defined by the members of the Working Group. At the first substantive session, delegations emphasised that we do not start from scratch. Past Groups of Governmental Experts (GGEs) have delivered concrete results, including, among others, recommendations on confidence-building measures and creating a regime of norms for responsible state behaviour. We now have the opportunity to discuss how to go forward. Delegations have brought up many ideas, including for example a review mechanism for the implementation of the GGE's norms of responsible state behaviour, a matchmaking mechanism for capacity-building, or the universalisation of regional confidence-building measures. The next rounds of discussions will show what elements can potentially be part of a consensus and what areas need more time and efforts. Beyond this, it would certainly be a significant outcome if the Group could agree on ways to institutionalise future dialogue in this increasingly significant field.

What are some of the challenges or obstacles to that?

Consensus is always a challenge, especially in an area where there is a significant need to establish more trust in each other. Another challenge lies in the relatively novel—and rapidly evolving—substance and the fact that many member states have to familiarise themselves with this field of work of the General Assembly. We will also have to manage the ambitious timeline foreseen in our mandate. We will have to find convergence on as many issues as possible in a limited amount of time. Our mandate foresees only three substantive sessions, of which we will soon start already the second. The first substantive session took place in a very constructive atmosphere and the members of the Working Group have touched

upon many areas where there seems to be a fair level of convergence, whereas in others a variety of different positions have been expressed. The remaining substantive sessions give us the opportunity for more interactive discussion, with the aim of going deeper into the substance and identifying concrete areas where common ground exists, but also trying to reflect on issues on which we cannot yet agree, which we might want to discuss further in the future.

Given the limitations to direct participation, what are other avenues for civil society to contribute to the process and/or its outcomes? What are your views on the informal multi-stakeholder session that was held in December?

Civil society can contribute in many waysThe different stakeholders have a unique understanding of many of the challenges and benefits of the use of ICTs in the context of international security. The multi-stakeholder session in December was proof of that and allowed governments and stakeholders to address many of the open questions in the room. In addition, we publish written contributions by non-governmental organisations to the process on the website of the OEWG. A number of member states have also held national cyber consultations to reflect the views of their national stakeholders in their positions.

Many delegations have stressed the importance of complementarity between the OEWG and GGE. How do you see this unfolding, practically?

This point was raised by many delegations. I attended many of the consultations of the GGE with regional organisations, among them the OSCE, OAS, ASEAN and African Union, and had the opportunity to get to know my colleague, Ambassador Patriota from Brazil, who is the Chair of the GGE. Ambassador Patriota and I are in close contact and I am happy that he has agreed to informally brief the OEWG at its second substantive session. The members of both groups also have a key role in ensuring this complementarity by shaping the content of the respective processes and their outcomes.

Do you have any final thoughts or observations?

I would like to encourage all readers to engage with the issue of cyber security and our process. The broad interest in the multi-stakeholder session in December has shown that cyber security in the wider context of international security is a topic which affects us all and in which many have a stake.

UNPACKING THE GGE'S FRAMEWORK ON RESPONSIBLE STATE BEHAVIOUR: CYBER NORMS

Sheetal Kumar | Global Partners Digital

Global Partners Digital and the Association for Progressive Communications have jointly published the third in a series of technical briefs, introduced in a previous edition of the *Cyber Peace & Security Monitor*, which looks at each component of the "responsible state behaviour framework": 1) norms, rules, and principles 2) confidence-building measures 3) capacity building and 4) the application of international law in cyberspace.

The latest entry focuses on cyber norms, and includes an analysis of each norm from a human rights perspective with examples of how human rights defenders can support the implementation of the norms. This accompanies two other briefs in the series which were previously published, on capacity-building and the second on confidence-building measures.

The cyber norms brief can be found here: https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/.

The other briefs can be found on GPD's dedicated information hub for the UNGA First Committee, which also includes a range of other resources: https://www.gp-digital.org/event/unga-first-committee-hub/.

CYBER PEACE & SECURITY MONITOR

Reaching Critical Will is the disarmament programme of the Women's International League for Peace and Freedom (WILPF), the oldest women's peace organisation in the world. Reaching Critical Will works for disarmament and the prohibition of many different weapon systems; confronting militarism and military spending; and exposing gendered aspects of the impact of weapons and disarmament processes with a feminist lens. Reaching Critical Will also monitors and analyses international disarmament processes, providing primary resources, reporting, and civil society coordination at various UN-related forums.

Reaching Critical Will

www.reachingcriticalwill.org

www.wilpf.org

The Cyber Peace & Security Monitor is produced by the Reaching Critical Will programme of the Women's International League for Peace and Freedom (WILPF) during relevant UN meetings.

CYBER PEACE & SECURITY MONITOR

Vol. 01, No. 06
10 February 2020

Editor: Allison Pytlak
disarm@wilpf.org

The views expressed in this publication are not necessarily those of WILPF or Reaching Critical Will.