CYBER PEACE & SECURITY MONITOR

Civil society perspectives on the Open-ended working group on security of and in the use of information and communications technologies

VOL.2 NO.2

10 December 2021

Photo: Jose Antonio Gallego Vázquez | Unsplash

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

WILPF
WOMEN'S INTERNATIONAL LEAGUE FOR PEACE & FREEDOM

www.wilpf.org

RESTART OR RESET? OEWG II GETS UNDERWAY

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

There is a noticeable sense of momentum within the United Nations (UN) around cyber peace and security these days. The UN Secretary-General (UNSG) prioritised the issue and identified cyber warfare as a key strategic risk in his recently released *Our Common Agenda*. He suggested a ban on cyberattacks against critical infrastructure and de-escalating cyber-related risks and tensions as possible elements of a new peace agenda. The UN's Working Group on Mercenaries released a report in which it assesses the role and impact of cyber mercenaries on human rights and makes some very specific recommendations to other UN bodies dealing with these issues. Other UN human rights experts have called for a moratorium on the sale of spyware. References to cyber threats and online networks are cropping up more frequently within UN frameworks on nuclear and autonomous weapons, as well as on small arms, alongside a growing number of relevant research initiatives. Despite misgivings from many states and stakeholders about a new initiative to develop a cybercrime treaty via the UN General Assembly (UNGA) Third Committee, preparations are underway for a January meeting of that process's Ad Hoc Committee.

Meanwhile, the two processes established in 2018 by the UNGA's First Committee both adopted substantive reports earlier this year, thus bringing to a close their respective work as well as a bifurcated process on cyber peace and security. This was followed by the adoption of a single resolution on cyber and information and communication technologies (ICTs) during the 2021 First Committee session, after two years of the so-called duelling resolutions from Russia and the United States.

Considering how long the topic of ICTs, a.k.a. cyber, has been on the UN's agenda, the current surge in attention and priority is not only welcome but overdue, not least considering the pace of technological development and the explosion of cyber threats we are facing. This surge should give impetus to the UN's second open-ended working group (OEWG II) as it has its first substantive session this month. The group's predecessor, OEWG I, began its work in a politically hostile climate but eventually cultivated a strong sense of constructive energy and trust among its participants, enabling the consensus adoption of a final report—hailed as a win for multilateralism and diplomacy, but certainly involving concessions from many states. The OEWG I final report was complemented by a substantive report and compendium of views from its counterpart, the sixth Group of Governmental Experts (GGE), released just two months later.

Despite the current goodwill and constructive spirit, many of the underlying issues that divided states during OEWG I and in the GGEs haven't disappeared. Moreover, it cannot be overlooked that in parallel to the momentum in the UN there is also undeniable momentum in the severity and scale of malicious cyber operations occurring in real time, which demand meaningful and effective response.

At the outset of OEWG I in 2019, a common remark was to "not start from scratch," meaning that states should not overlook or seek to undo the existing acquis of agreements and affirmations from past UN processes. This continues to be a relevant message for the restarting of OEWG sessions, as the new group seeks to build on the work of its predecessors. But that shouldn't hinder the potential for evolution either; and in a few areas, it may just be time for a factory reset.

Scratch lines

The OEWG II's provisional programme of work is guided by the resolution that established the group. It will mainly follow the same six topics as did OEWG I—threats; rules, norms, and principles; international law; confidence-building measures (CBMs); capacity building; and regular institutional dialogue. These topics are deeply interconnected. One of the balancing acts facing the new group will be respond to the issues that require urgent attention while not giving short shrift to the others.

At the conclusion of OEWG I, the stickiest issues were moved into a Chair's summary of the process, which is a non-negotiated document issued by a conference or meeting chairperson to accompany a negotiated report. It is a way to reflect points that were made but did not enjoy sufficient support or consensus to be included in the adopted report. The adopted OEWG I report was ultimately structured in a way that focuses on conclusions and recommendations.

Important among the items that did not survive into the adopted report was a reflection of the high degree of support from most—but not all—states on the applicability of international humanitarian law to cyber space.

Per our reporting, other areas that were also contentious at the end of OEWG I included:

- How exhaustively and prescriptively to name the different types of critical infrastructure
- Whether to affirm the applicability of the UN Charter "in its entirety"
- Whether and how to define which legal principles are or should be applied to state behaviour in cyber space
- The ordering of norms vis-a-vis law
- Whether to welcome or include reference to past UNGA resolutions that approved reports from earlier UN GGEs by vote, versus those adopted by consensus
- Tech neutrality
- Concerns about the development of ICT capabilities for purposes that undermine peace and security, and for military purposes
- If the call for states to submit views to the UNSG and to establish national points of contact in relation to capacity-building should be voluntary or not
- The possibility of developing legally binding obligations
- Reconciling very different views on if and how to reference OEWG II and the proposal for a programme of action (PoA) on cyber.

Any of the above could be a trigger for debate, some more than others. At the close of OEWG I, a few states even disassociated with parts of the final report while others expressed discomfort at certain concessions or raised points about the costs of consensus-based decision-making.

There is some residual skepticism about OEWG II as a forum, left over from how it was established in 2020 in a move at the UNGA First Committee by Russia that many states felt was premature. Given the growing support for creating a cyber programme of action (PoA)—intended to be a politically-binding and "action-oriented" instrument—OEWG II is under some pressure to demonstrate it can not only maintain the largely constructive spirit of OEWG I, but also have impact, lest it be eclipsed by the PoA.

One way for the OEWG II to not start from scratch would therefore be to advance on or survey progress made on some of the tangible recommendations contained in the OEWG I report or build on proposals made through working papers and other submissions. The guiding questions set out by OEWG II Chair Ambassador Burhan Gafoor of Singapore for the December session will be useful in this regard as well as for identifying priorities. Many of them ask what role the OEWG can play in facilitating national or regional actions such as norms implementation to information-sharing, matching needs, and clarifying or building policy. Others ask broader questions, such as about the potential development of new norms; most sections touch on the role on non-governmental actors.

Reset

Which brings us to a point where a reset is sorely needed. The standard UNGA modalities for non-governmental stakeholders to apply for accreditation and registration to formal sessions were exploited by a handful of states in OEWG I, who blocked the participation of multiple legitimate actors but who lack UN Economic and Social Council (ECOSOC) status. To garner wide input to the OEWG from some of these actors, many of whom play an active role in implementing the UN cyber norms, the OEWG I chairperson and supportive states facilitated several ad-hoc

informal dialogues and events, such as the Let's Talk Cyber initiative. While these were well-attended and successful, including for fostering a sense of community, they were not intended to become a permanent substitute for the meaningful inclusion of civil society in the formal meetings.

It was therefore widely hoped that OEWG II might bring about new modalities. During an organising meeting held in June, several states spoke to this issue and came with proposals for OEWG II, based on other relevant UN and multilateral processes. This issue was left as "outstanding" at the end of that meeting, with the understanding that more consultations would be held, and a proposal made. Subsequently, one of the Working Groups of the Paris Call for Trust and Security in Cyberspace put out a study on the need for greater inclusivity in the UN dialogues on cyber security, while representatives of other civil society organisations, including WILPF, co-authored a report to highlight good practice on civil society inclusion in other processes.

It was therefore disappointing to many when a letter from the Chair published in mid-November set out that he had taken a decision to use the same modalities as OEWG I. This means that accreditation requests to join formal meetings would go through the usual procedure in which states can object to an application, and that other informal consultative meetings can be arranged. The Chair does commit "to engaging with stakeholders in a systematic, sustained, and substantive manner" and sets out a plan to have, as of 2022, day-long informal consultations a few days in advance of planned formal OEWG sessions.

In December, however, there'll be only one 90-minute consultation held during a lunch break in which stakeholders can deliver remarks of two minutes in length.

In response, more than 40 member states and close to 150 non-governmental representatives sent a letter to the Chair, outlining their concerns.

It's possible that states won't object to formal accreditation requests this time around, but if so, a minimum ask would be that objections are accompanied by an explanation, particularly when the organisation in question has a credible track-record of work on cyber peace and security.

Excluding civil society from OEWG II or making it challenging to join will only be detrimental to the process—both its credibility and its impact. "The discussion of the OEWG agenda and the implementation of its outcomes cannot be done by governments alone," notes one of the aforementioned studies. The discourse on stakeholder participation must change from "if" to "how" we are involved.

Moving to action

Adopting or issuing reports and statements are important for multilateralism and awareness-raising, but what is necessary is that commitments are implemented and actioned outside the halls of the UN. "Ultimately, success depends not on the report but on our collective determination to implement the commitments made today," noted the representative of the Czech Republic in closing remarks to the OEWG I third substantive session.

In this vein, it is vital that the OEWG not become just another talk shop. The 2021 joint statement from civil society to the UNGA First Committee described a range of cyber operations and threats which speak to the "the far-reaching impacts of aggressive action in cyberspace." The statement further underscores that, "Such actions demonstrate that the legal ambiguities surrounding the application of international law to state behaviour in cyber space are being exploited, and that relevant norms against such behaviour are not being respected."

Many in civil society had hoped that OEWG I would produce some form of accountability mechanism or framework. It did not, despite more than a few working papers and proposals to this end. Closing the cyber accountability gap and fostering transparency will continue to be a priority message for many, including WILPF.

More positively, however, OEWG I helped propel certain new issues to the international agenda that had not previously been well-accepted or often discussed. One example is growing acceptance of human-centric approaches to cyber peace and

security, and within that, an examination of the gendered impact of cyber operations as well as the value of women's participation in all aspects of the sector, which was further bolstered by the Women in Cyber fellowship programme.

Whether restarting or resetting, it's going to be important that states not let an approach of "not starting from scratch" limit the potential for evolution and growth. Whether it be new cyber norms, new concepts, or reacting to new threats, the time for urgent action for cyber peace is now.

ADDRESSING GENDER CONSIDERATIONS IN UPCOMING UN CYBER PROCESSES

Hana Salama | UN Institute for Disarmament Research

On the 30 November 2021, the United Nations Institute for Disarmament Research (UNIDIR) along with the Government of Canada and the Women's International League for Peace and Freedom (WILPF) co-hosted a briefing with the Women in Cyber Fellows (WiC)[1] on addressing gender considerations in the upcoming UN cyber processes. The aim was to take stock of how gender was addressed in past UN cyber discussions and identify ways of advancing the agenda both substantively and in terms of process at upcoming ones.

Speakers mentioned that gender matters in international cyber security, as it shapes and influences online behaviour; determines access and power; and is a factor in vulnerability, whether real or perceived. A gendered understanding of cybersecurity threats recognises that cyber threats—such as denial of service attacks on State services, data breaches, internet shutdowns—have gendered impacts. This understanding also recognises, as cybersecurity threats, issues such as cyber intimate partner violence, doxing, cyberstalking and non-consensual dissemination of intimate images, as well as online violent extremism and online sex trafficking. A gendered understanding of cyber threats will inevitably lead to the development of more inclusive, complete, and effective responses that consider the needs and vulnerabilities of all segments of society.

The discussion started by acknowledging that much progress has been made in the area of diverse participation and advancing gender considerations. The first cyber discussions at the UN were conducted among a small group of states (15-25 states who took part in UN Groups of Governmental Experts) and made little or no mention of gender issues. The 2019-21 UN Open-ended Working Group (OEWG) on information and communications technologies (ICTs), which concluded in March 2021, made some important progress on both gender and diversity, as it included a wider range of member states and increased civil society participation. Gender diverse representation was also stronger as compared to previous discussions and this was in part thanks to the WiC Fellowship programme.

The Fellowship was highly regarded by all participants and seen as a breakthrough innovation in the UN cyber process. It not only helped increase women's participation, but also encouraged collaboration and information sharing between states, something which had not been seen in previous disarmament processes and should be replicated elsewhere.

It was also noted that substantive issues around gender considerations were the focus of some delegations' contributions to the OEWG, and were therefore also included in the Chair's summary and final report of the OEWG. Participants acknowledged this progress, but also highlighted the need to keep this momentum going and advance this agenda further.

Proposals for taking the gender agenda forward

The following reflects a summary of proposals to advance gender considerations in the next OEWG, that arose from the discussions with experts in the field of gender and cyber and the WiC Fellows.

1. Build awareness by demonstrating that gender equality is relevant to the mandate of the OEWG.

It was noted that recommendations on gender are the focus of the discussion. However, insufficient explanations have been offered on why such recommendations are relevant to the mandate of the OEWG, or other cyber forums. It would be important to create opportunities to further discuss the relevance of gender perspectives in building a stable, peaceful, cyber environment.

2. Clarify concepts related to gender in cyber and create a shared understanding of how these fit into wider peace and security frameworks.

Building on the above point, it was highlighted that concepts around gender and cyber should be better defined, including what is meant by online gender-based violence, harassment, and other concepts. States and stakeholders should further discuss what the gender issues in international cyber security are, as distinct from a wholly human rights or interpersonal context. The gender differentiated impacts of offensive cyber operations should be further examined. There is also a need to better situate issues of gender-based violence and other "non-traditional" threats within the wider peace and security frameworks.

3. Increasing diverse participation in cyber discussions by including civil society and youth.

Multistakeholder participation was highlighted as an important way of ensuring better outcomes in the development of cyber-related measures or instruments. This includes ensuring that UN cyber processes remain open to the participation of both international and national level civil society, including women's rights groups, and having formal and informal spaces for states to meaningfully engage with civil society. Increased participation of women and civil society is not only important to advance gender considerations, but also to ensure diverse expertise, views and approaches to cyber discussions. It was also noted that youth is an important constituency to these discussions and that younger cyber fellows should be included going forward.

4. Increase the number and diversity of gender champions.

It was also recognised that gender is not a women's only issue. The exclusion of women and gender minorities and the failure to take into account gender considerations in cyber discussions would have a negative impact on society as a whole. Therefore, it was suggested that gender considerations should be championed by men and everyone regardless of their gender identity, and that a broader understanding of "gender" should be encouraged.

5. Connect gender in cyber to wider agendas by bringing human rights and WPS priority topics into the conversation.

Gender considerations could also be advanced in cyber discussions by connecting them to wider agendas such as Agenda 2030, human rights, or the Women, Peace and Security (WPS) Agenda, as a strategy going forward.

Participants noted that adopting a human rights and intersectional approach to cyber issues is essential. Thus, it is useful to connect gender considerations in cyber to existing commitments in human rights treaties such as Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and others. As highlighted by UNIDIR's recent publication *System Update: Towards a Women, Peace and Cyber Security Agenda*, and by several participants, advancing cybersecurity using the WPS agenda can help to promote a gender-inclusive cyberspace that protects the rights of women and girls. This would also help ensure that lessons learned from traditional peace and security processes are taken into account when trying to promote a sustainable open, free, and stable digital world.

6. Mainstream gender considerations into OWEG discussion topics.

It was recognised that current discussions on cyber are siloed and that gender considerations are often seen as an "add on". As such, gender issues are often not prioritised in statements delivered by member states during UN cyber discussions. It was also noted that this continues to be a sensitive

topic for some states and that there is opposition to addressing gender within security forums and processes, including on cyber. It is therefore important to move away from the idea that gender is a standalone topic. Instead, efforts should be directed at mainstreaming gender across all discussion topics. For example, at the OEWG, gender could be discussed in connection with core OEWG agenda items such as threats and response, international law, norms, technology development, and capacity-building.[2]

7. Share best practices on gender mainstreaming at an international and national level

There are important lessons learned about how gender mainstreaming has been done in other disarmament processes. It is useful to document and share those experiences, as they may be applicable to upcoming UN cyber processes, for example as in a paper produced by WILPF about lessons from the UN Programme of Action (UN PoA) on small arms and light weapons (SALW) which could be applied to the proposed UN PoA on cyber.[3] In addition, many participants highlighted the need to share national experiences of gender mainstreaming in cyber security policies. This could be done by assessing current practices, by doing gender audits, as well as by reporting on gender mainstreaming measures on UNIDIR's Cyber Policy Portal. Another best practice identified would be implementing the existing cyber norms in a gender sensitive way. It was also noted that the Association for Progressive Communications (APC) is developing practical guidance to support states in developing national cyber policies in a manner that mainstreams gender. It was agreed that this guidance will be a useful tool for civil society and national advocates.

8. Increase the evidence base for gender in cyber by furthering data collection through the creation of a research network

Increasing research and data collection on the gendered impacts of cyber operations and broader cyber related issues was highlighted as another important way to move the needle forward on this issue. It was noted that until 2019, there was little research on the gender aspects of cyber security. Organisations such as APC, WILPF, UNIDIR, and others have since published some studies on the issue however, it was suggested that additional research and more gender disaggregated data is needed at a national and regional levels on cyber professionals, access to ICTs, digital literacy, online misogyny, and gender-based violence, for example. It would also be useful to gather disaggregated data on similar issues as it relates to the LGBTQ communities and other sexual minorities. It was suggested that there should be more gender disaggregated data by region, such as data on the proportion of women who work for tech companies or as cyber diplomats in Africa.

Research topics such as investigating the gender impacts of large cyber operations or the barriers to entry for women to become cyber professionals were also suggested. It was suggested that the creation of a research network with academics, civil society, and think tanks on the topic of gender and cyber could be useful in this regard, in order to coordinate expertise and data collection efforts.

NOTES

1. The Women in Cyber Fellowship programme was established in 2020 to promote greater participation of women in discussions at the United Nations on international security issues related to responsible state behaviour in cyberspace. Thanks to the Fellowship, 35 women diplomats representing countries from ASEAN, Asia Pacific, South America and the Commonwealth participated in the meetings of the 2019-2021 UN OEWG on the use of ICTs in the context of international security, as well as joined training and mentorship opportunities. In 2019-21, the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom were donors. The United States has been added to the list of donors for the new iteration of the programme.

2. Linking gender perspectives on these issues was suggested by Canada and Ecuador in the 2019-2021 OEWG.

3. Allison Pytlak, WILPF, *Programming action: Observations from Small Arms control for cyber peace*, 2021.

LET'S TALK CYBER HOSTS A DISCUSSION ON UN CYBERSECURITY DIALOGUES

Sheetal Kumar and Kaja Ciglic | Global Partners Digital and Microsoft

Let's Talk Cyber, an initiative sponsored by the Australian and Canadian governments, EU Cyber Direct, Global Partners Digital, and Microsoft, seeks to build community amongst the stakeholders interested in issues related to international cybersecurity and in particular on responsible state behaviour in cyberspace. The initiative began in late 2020 as an attempt to broaden multistakeholder inclusion into the United Nations (UN) dialogues on cybersecurity, and in particular to the UN Open-Ended Working Group (OEWG) on information and communications technologies (ICTs) in the context of international security, via informal and structured discussions. Those initial meetings have gathered momentum since and we hope to continue to bring together governments, industry players, technical community, academia, and civil society from across the world to discuss the most pressing issues occurring in this space, as well as to keep them informed of the various governmental dialogues taking place on the subject.

With that in mind, on 3 November 2021, the Let's Talk Cyber initiative hosted a virtual session entitled "*Responsible state behavior in cyberspace at the United Nations: How can the multistakeholder community ensure that existing agreements become a reality?*". The webinar represented the start of a new discussion series that will take place over the next few months, as negotiations at the UN pick up again. This particular webinar sought to provide an overview of the deliberations that took place at the OEWG and at the UN Group of Governmental Experts (GGE) on the same subject over the past two years. Its goal was to thoroughly examine the two reports the OEWG and GGE respectively produced and to investigate how to ensure that these agreements are respected and implemented. All of course, with the role of the multistakeholder community in achieving those objectives foremost in our minds.

The webinar was moderated by Kaja Ciglic, Senior Director of Digital Diplomacy at Microsoft and brought together stakeholders that were instrumental in ensuring the two processes came to successful conclusions:

- H.E. Guilherme Patriota, former Chair of the UN GGE on Advancing responsible State behaviour in cyberspace in the context of international security, and Consul General of Brazil in Mumbai;
- H.E. Jürg Lauber Permanent, former Chair of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, and Representative of Switzerland to the United Nations in Geneva;
- Dr. Camino Kavanagh, Visiting Senior Fellow, Department of War Studies at King's College London and Senior advisor to United Nations Department of Political Affairs on Digital Risk in Armed Conflict and its Conflict Prevention/ Mediation & Digital Technologies; and
- Johanna Weaver, Director of the Tech Policy Design Centre and Special Adviser to Australia's Ambassador for Cyber Affairs.

Given the illustrious panel, the participants were able to hear firsthand what transpired in the two processes, including examples of how the two Chairs found innovative ways to ensure they were as transparent as possible in their deliberations and how they sought to gather feedback from states as well as the broader multistakeholder community. The challenges and potential lessons learnt that the COVID-19 pandemic introduced were also touched upon; with speakers highlighting virtual meetings as potentially not the most conducive to diplomatic negotiations, but certainly opening up the discussion to more stakeholder groups.

Dr. Kavanagh provided further background on the discussions and agreements that have preceded the latest GGE and OEWG. In particular, she highlighted the seminal 2015 GGE report, which

acknowledged that international law applies to cyberspace, as well as noted 11 norms of responsible state behavior. The two reports that were agreed in 2021 re-affirm those earlier conclusions and built on them, in particular when it comes to international law. Furthermore, the 2021 reports provide guidance on how to implement the norms and encourage states and other actors to focus on cyber security capacity-building.

Ms. Weaver in her remarks touched upon how the multistakeholder community can play a role in shaping these norms and rules—a topic that came up in the questions from the audience repeatedly. She encouraged the community to engage with their individual governments, and to not solely focus on the UN processes but look to domestic transposition as well. She provided lessons learned from engaging in the processes so far, including the importance of working "in the margins": utilising informal channels for advocacy and diplomacy; the increasing importance of engaging media in reporting and raising awareness of state commitments to responsible state behaviour in cyberspace; the need for greater ministerial attention to the responsible state behaviour framework; and the need for more funding for implementation, which can be supported by developing and using metrics. Dr. Kavanagh echoed her comments, but also encouraged stakeholders to provide comments throughout the forthcoming negotiations and to work to ensure these are precise and on point.

In the final round of remarks, the speakers highlighted the upcoming OEWG, even though it was noted that the modalities and multistakeholder participation were not yet agreed and that therefore we will most likely have to wait until December before it will be clear how to proceed. They also touched on the proposed cyber Programme of Action, touching upon it with optimism and highlighting it as a potentially more flexible vehicle to move forward in this space. Ambassador Lauber also echoed Ms. Weaver's call for the multistakeholder community to continue engaging and pushing their positions at whatever level possible—a welcome and much needed invitation.

This Let's Talk Cyber webinar was certainly not the last. The next one will take place during the next OEWG meeting on 13 December, "The new Open-Ended Working Group on Cybersecurity: What can the multistakeholder community expect? Click here to register. For more information on the Let's Talk Cyber initiative, please check out the website, where you can sign up for the latest updates, as well as revisit our previous events.

Photo: Lucian Alexe | Unsplash

A CALL FOR ALL VOICES: HOW TO MOVE THE ACCOUNTABILITY CONVERSATION FORWARD

Juliana Crema | CyberPeace Institute

Actively following and engaging in the Open-ended Working Group (OEWG) I process has been a focus for the CyberPeace Institute since its creation in 2019. The inclusion of non-state actors and an overall multistakeholder approach in such critical discussions is of utmost importance. These communities can share knowledge and expertise with governments, and can encourage a more representative and comprehensive decision-making process. As such, the Institute has prioritised engagement and advocacy work in collaboration with other non-state actors to promote accountability and work towards a more peaceful cyberspace. The OEWG discussions provide a unique opportunity in that all UN member states are welcome to participate, unlike at the Group of Governmental Experts.[1] However, as the first OEWG II substantive session begins on 13 December 2021, there is the expectation that this process should be just as, if not more inclusive than OEWG I. OEWG II should ensure that countries can make meaningful contributions that build upon the previous discussions, final report, and multistakeholder input.

The importance of a multistakeholder approach

The systematic inclusion of non-governmental actors, specifically those without ECOSOC status, in substantive discussions regarding the application of international law to cyber space and the implementation of capacity building measures is critical. This inclusive approach needs to be integrated from the beginning of the OEWG II process in order to be effective.

The CyberPeace Institute is concerned that the documents shared ahead of the first substantive session of OEWG II do not specifically mention the inclusion of civil society, they do not provide enough information on how non-state actors can participate in the first substantive session, and there is an overall lack of transparency and visibility offered for multistakeholder contributions throughout the process. Non-governmental stakeholders have been invited to an informal discussion ahead of the first substantive session, however, one ad hoc discussion is not a systematic or substantive approach to multistakeholder inclusion.

Some states have voiced concern about the lack of inclusion of civil society, as they are strong proponents and advocates for the inclusion of the multistakeholder community in UN processes. Non-state actors are also active in this area and have published a letter through the Let's Talk Cyber initiative, which calls for "systematic, sustained and substantive" engagement through five points that call for greater transparency and inclusion in the process.[2]

Updates since OEWG I

Improved accountability in cyber space takes time, and needs to be based on an evidence-led perspective. A data-driven analysis underpins the Institute's advocacy work for a multistakeholder approach in the upcoming OEWG II discussions.

For example, the Institute launched the Cyber Incident Tracer (CIT) #HEALTH to make data and facts about cyberattacks publicly accessible in one place. As this platform aggregates more and more data on disruptions, it can be an important reference for those seeking accountability in cyberspace and the quest for justice. With greater transparency about cyberattacks, the relevant laws can be more easily applied in practice to cases.

Based on the data collected in CIT #HEALTH, the Institute recently published an Addendum to complement the Strategic Analysis Report published in March 2021.

There are specific recommendations for governments throughout this work. The Report and Addendum can serve those engaged in the OEWG II process and other relevant fora to understand the true scale and impact of attacks against healthcare

and underscore that more must be done to protect this sector.

OEWG II: priorities and changes

The Institute has followed the developments ahead of OEWG II, set to run from 2021-2025, with great interest. So far, a change to note is the working group's name. OEWG I was titled "Open-ended working group on developments in the field of information and telecommunications in the context of international security" whereas through UNGA resolution 75/240, OEWG II has been changed to "Open-Ended Working Group on security of and in the use of information and communications technologies." Words count. This change in name is a signal that discussions could move away from responsible state behaviour and actions, to the security implications of information and communications technologies (ICTs). This could be a shift away from the political-legal considerations, such as how to build capacity and apply international law to cyberspace, to more military-centric considerations on the practical use of existing and emerging technology. It will be important to follow the first substantive session of OEWG II for clarity in this regard.

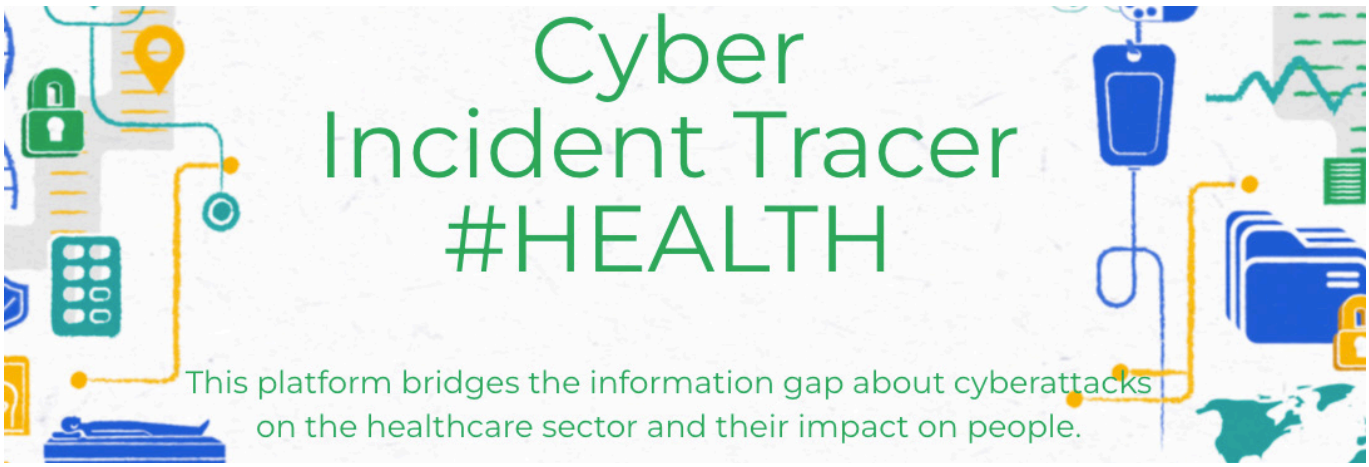
Additionally, there are several points that need to be discussed in OEWG II for the process to meet the priorities previously outlined by the Institute in an overview of OEWG I's final report. This includes concerns about the overall lack of a human-centric approach, specifically regarding the analysis of threats and the implementation of confidence building measures in cyberspace. Focusing efforts around people and their rights is necessary not only as a means to foster cooperation but also in terms of practical application of the agreed upon norms.

As underlined in the final OEWG I report, the lack of actionable steps towards greater accountability in cyberspace is a serious concern. These issues remain key for the CyberPeace Institute and are especially relevant for the proposed Programme of Action whose aim is to implement the recommendations outlined in OEWG I's Final Report. To be clear, states are not acting alone, and should include the non-state actor community to assist in creating solutions for these issues.

NOTES

1. The UN Group of Governmental Experts (GGE) is made up of a limited number of Member States and restricts their consultations to regional organisations. The UN Open Ended Working Group (OEWG) includes all interested Member States and historically consults the multistakeholder community. For more information on the differences between the UN OEWG and GGE processes, please see the Geneva Internet Platform's comparison.

2. Letter to the Chair of the UN OEWG, published 9 December 9 2021.



LETTER TO THE CHAIR OF OEWG II ON CIVIL SOCIETY PARTICIPATION

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

As outlined elsewhere in this edition, civil society participation to the first Open-ended working group (OEWG I) was a fraught issue and concerns remain over what this portends for the second OEWG (OEWG II).

In advance of the first session OEWG II, 44 UN member states, 72 non-governmetnal organisations, and 35 individuals submitted a letter to the OEWG II Chair, Ambassdor Burhan Gafoor of Singapore on 9 December 2021.

The letter proposes a set of principles that civil society participation modalities should embody, in line with the vision and commitment the Chair has set out.

Dear Chair,

The undersigned Member-States, regional organizations, and non-governmental stakeholders would like to thank you for your proposal for the modalities for the United Nation's second Open-Ended Working Group ("OEWG") on security of and in the use of information and communications technologies (ICTs) in your letter of 15 November. We appreciate receiving this information sufficiently in advance of the convening of the first session in December for us to consider it in detail and provide our views to you.

As the final report of the first OEWG on ICTs stated, "...the broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment"1. We are committed to your vision to build on the work already achieved by the first OEWG and to leverage their expertise by engaging stakeholders in a 'systematic, sustained and substantive' manner.

Rather than make proposals of specific measures we propose a set of principles that the modalities should embody which we see as fully in line with your vision and commitment to engaging with stakeholders:

1. The participation modalities should ensure that more non-governmental stakeholders are able to meaningfully participate in formal OEWG meetings than was the case for the previous working group. In particular there should be participants in addition to those already eligible due to their existing consultative status with the UN;

2. There should be a transparent process in place regarding any objection from a Member State to the accreditation request of a non-governmental stakeholder to participate in the formal substantive meetings, especially those who are already officially recognized by the UN in other contexts;

3. In the event that interested non-governmental stakeholders are denied accreditation to formal OEWG sessions there should be channels for such stakeholders to regularly express their views and for those views to be available to all accredited delegations. These channels can be convened through the good offices of the OEWG Chair as informal measures, and a facility that allows the official delegates to have access to them is essential;

4. Sufficient time should be made available to non-governmental stakeholders to meaningfully raise their views in both formal and informal meetings and for delegations to have sufficient time to meaningfully discuss those views.

5. A hybrid format should be utilized for formal and informal meetings to a sufficient extent to facilitate the participation of delegates and other stakeholders who cannot travel to New York in person. This is especially important during a global pandemic whilst so many countries do not have sufficient access to vaccines to facilitate travel and while vaccine regimes differ and given the potential for new variants to cut off travel for entire countries.

We are committed to a successful OEWG process and believe that it is likely to have a far-reaching impact on many stakeholders, including direct impacts on communities and individuals.

We also hope for an open, transparent and inclusive dialogue that would provide the basis for stakeholders to play a role in implementing the decisions and which would take into consideration their means and ability to participate and contribute to the outcome. Given the subject matter of the OEWG, this is doubly true: many of the measures agreed cannot be implemented effectively without the active participation, alongside governments, of non-governmental actors. Correspondingly, addressing threats emanating from cyberspace will require leveraging the experience, expertise and resources of all relevant stakeholders.

With this in mind, our proposal reflects what we believe is required to realize a minimum level of the systematic, sustained, and substantive participation by non-state actors in the work of the OEWG. We present this, therefore, as a compromise in the interest of consensus.

Finally, Excellency, we would like to emphasise our commitment to a successful outcome of the OEWG and to actively participate in our respective capacities, and the assurances of our highest consideration.

The letter and list of signatories is available online.

Want to follow the second UN cyber OEWG (2021-2025)?

You can find documents and other information as it becomes available at:

https://reachingcriticalwill.org/disarmament-fora/ict/oewg-ii.

Documents, statements, working papers, and materials submitted to the first UN cyber OEWG also remain available on our site.

Photo: UN Photo/Cia Pak

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 open meetings of the UN's OEWG on ICTs.

CYBER PEACE & SECURITY MONITOR
Vol. 2, No. 2
10 December 2021

Editor: Allison Pytlak

Contact: disarm@wilpf.org