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.8

7 March 2021

Photo: Lance Gradahl | Unsplash

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

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

www.wilpf.org

GETTING BACK ON TRACK TO CROSS THE FINISH LINE

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

A great deal has changed since delegates met in New York a little over one year ago for the second session of the UN's Open-ended working group (OEWG) on developments in the field of information and telecommunications (ICTs) in the context of international security. When this Monitor published its report of the OEWG's second substantive session in February 2020 in a pre-pandemic world, it spoke of cyber security as a team sport, a metaphor that had emerged and become popular in the course of the in-person OEWG sessions:

> "If member states can "play" together as a team through the final stretch and agree on a consensus report with good substance, then everyone wins, because there will be benefits for the international community. If members of the team start missing passes from their teammates, running the other way, or incurring penalties for bad behaviour—then we all lose out."[1]

The costs of losing out have come more sharply into focus during the pandemic. Our dependence on ICTs has never been higher, underscoring the ubiquity and the importance of meaningful access to them. Yet the misuse of technology, whether for criminal, personal, or political reasons, has risen at pace with this reliance, as civil society outlined in a joint statement to the UN First Committee in 2020. Cyber crime has soared. Multiple digital operations targeting medical facilities worldwide have sought to undermine responses to the health crisis, spread misinformation, or exploit our current increased reliance on digital connectivity. Some governments have instituted digital contact tracing applications or other approaches that raise concerns about privacy, surveillance, and human rights, while internet shutdowns have impeded access to updates on health measures and other relevant safety information. Online gender-based violence, including surveillance, increased significantly in this time. A greater number of states have or are exploring offensive cyber strategies and doctrines, while diverse actors are increasingly incorporating ICT use into their strategies for sowing disruption.

Indeed, throughout the UN General Assembly's (UNGA) 75th high-level debate in 2020, a record number of leaders highlighted digital insecurity and hostile cyber activity as among the key threats facing our world today.[2]

All of which makes the work of the OEWG in its final session more urgent than ever.

Know where you're going

The primary expected output of this third session is the consensus adoption of a final report. In theory, a substantive report from a significant UNGA-mandated body could be a catalyst for a good many things that would further cyber peace and security by addressing the challenges enumerated above. It could call for the establishment of new processes or research; speak out for or against specific behaviours; initiate accountability mechanisms, etc. And certainly, throughout the OEWG process there has been no shortage of substantive ideas and suggestions, as evidenced by the significant number of working papers, guidance documents, and proposals submitted to the OEWG by states and civil society in the hope that the Group would be in a position to action them. The willingness and interest of participating states to really dig into and discuss the OEWG's thematic topics, supplemented by the contributions and attention of other stakeholders, has been a noticeable characteristic of many OEWG meetings that WILPF has been able to observe.

The "first draft" of the final report that is before states to consider now is the product of several rounds of virtual consultations that took place over the last eight months. Like everything else, the pandemic has thrown many hurdles into the OEWG's path, not least the possibility of convening an in-person third session. The virtual consultations were an effective way for the OEWG chairperson to advance discussions while awaiting a final formal session to be possible and use the time to refine views to a place where a final report might be that much closer to being adoptable.

The first draft of the final report is currently structured in four parts: a) an introduction that provides context; b) agreed conclusions and recommendations, from across the six thematic areas the OEWG has discussed; c) a reflection of the discussions on these subjects; d) and final observations. The section of conclusions and recommendations is what will mainly be negotiated, although "nothing is agreed until everything is agreed," as is often said in negotiating rooms.

The draft includes rich content, much of which is found in the "discussions" component of the draft and demonstrates the complex nature of the subject and of OEWG sessions. The Chair has been careful that the report reflects not only areas of convergence but also where other views have been expressed, an approach that has been called for by some states to ensure that their views are captured, even if they do not trigger a recommendation.

However, the draft report could be stronger and more action-oriented. Quite a lot of the conclusions, and some recommendations, relate to the upholding, continuation, or acknowledgement of existing obligations, or recommend engaging in practice that has largely already been recommended by other relevant bodies (although perhaps these reminders and re-affirmations bear repeating!).

Other of the recommendations, such as around information-sharing activities for confidence- and capacity-building, or to survey practice and understanding, are valuable but couched in a lot of qualifying language (i.e. "on a voluntary basis" or "as appropriate") which takes away from the strength of the recommendation. In some instances where the recommendation is less controversial, the report could take the tone of "encouraging" or "calling on states to" follow through on the recommendation. Some recommendations do not have a clearly identified follow-up measure attached to them, which makes their next steps unclear. WILPF would also wish to see stronger calls against aggressive cyber behaviour and clear provisions for accountability mechanisms.

Fair play

If the costs of losing out are urgent, then so too is the impetus for states to work as a team and move this process over the finish line.

Consensus in the UN context has over time been interpreted to mean unanimity. This often means that if even one state objects to something, then consensus is seen to be broken—even if all the other member states are in agreement. This usually has the effect of watering down final reports and outcome documents as an effort to find compromise. Moving to a vote is avoided at great cost. If consensus would be applied as it is actually meant—a general agreement—then there would be a greater potential for stronger or more ambitious outcomes in most UN processes.

In the search for OEWG consensus, pre-existing political dynamics will make this challenging. As just one example, the manner in which the establishment of a second OEWG was pushed through the UNGA before this first OEWG can conclude its work did no favours for the country that did the pushing. If anything, its tactics in October 2020—along with other recent manoeuvres in the OEWG—has further contributed to the needless politicisation of this issue in that way that could have blowback.

A reading of written governmental submissions to the zero-draft of the final report may give some indication of what other obstacles are. They also contain a peppering of technical suggestions that would render the language of the report more precise. There appears to still be divergent views about how the applicability of international humanitarian law (IHL) is framed, including how that applicability is seen by some states as serving to militarise cyberspace. There are some differing points in relation to the section on international law. There seems to also still be different understandings or approaches to the norms, and/or their status, established by past UN Groups of Governmental Experts (GGEs)—for instance, a few states would like to more strongly emphasise the potential to develop new norms even as existing ones are being implemented; others are quite firm in their support for the GGE norms as constituting an important shared baseline; and there also

diverse points made about whether and how to account for the eleven GGE norms, versus the thirteen that are contained in the UNGA resolution which established he OEWG but not otherwise adopted or agreed to.

It appears that calls from some states and groups of states for the report to include language about offensive capabilities and the weaponisation of cyber space have not been included. There are some specific proposals, such as on practical guidance for norms implementation and a standardised survey of existing implementation, that sound as though they enjoy wide support but have been noted as not integrated into the text, and rather will be annexed to it. A balance may need to be struck between acknowledging the vulnerability of the health sector—as highlighted by cyber operations during the COVID-19 pandemic—but not overlooking other vital critical infrastructure. A few states feel that human rights and gender perspectives do not have a place in the OEWG's consideration of "international cyber security". Finally, there is a division as to if, and how, the forthcoming OEWG is referenced in the text vis-à-vis a proposed cyber programme of action.

It is difficult, however, to assess with great accuracy what the tensions and red lines are going into this third and final session, because all of the virtual consultations held in recent months were closed to civil society. We've worked successfully with supportive member states and one another to find ways to contribute our views and expertise, as is described elsewhere in this edition. While this has led to some innovative and ultimately positive experiences and collaborations, civil society should not have to continue cultivating alternative methods and meetings in order to be included. The discourse on stakeholder participation must change from "if" to "how" we are involved.

Defining a "win"

Since the OEWG was first convened, there have been a series of what some might describe as "smaller" wins that deserve recognition.

That there has finally been a UN process on international cyber security open to all member states has made critical exchange and open discussion possible; in earlier meetings, several states noted that the OEWG is a confidence-building measure in itself. Even if divergent views remain, the process of needing to formulate more detailed and nuanced cyber-related positions and engaging with others has helped to sharpen understandings and build awareness of not only national and regional priorities, but also existing practice and of needs. As such, the OEWG may also enable better streamlining between existing initiatives and has highlighted gaps. The varied roles played by the diverse civil society groups engaging in the OEWG has been more fully articulated and outlined. Understandings about the gendered impacts of cyber operations have evolved throughout the OEWG, as described elsewhere in this edition. The discourse overall feels somewhat less securitised than it has been, in that concern or acknowledgement about the human costs of cyber operations are more prevalent, although much more needs to be done on this front.

Multilateral and especially UN processes put a high premium on the adoption of final reports by consensus. Certainly, achieving agreement and building shared understanding is important for international cooperation, and the agreement of the report is part of the Group's mandate. But it's important to not lose of sight of the bigger picture—we should not prioritise the achievement of the document over action.

We encourage states to be bold as they move into this final round of OEWG talks and go for gold as they cross the finish line.

NOTES

1. Allison Pytlak, "Cyber security—a team sport", *Cyber Peace & Security Monitor*, Vol.1, No. 7, 18 February 2020.

2. View our UNGA Disarmament Index to learn more: https://reachingcriticalwill.org/disarmament-fora/unga/2020/index.

"REGULAR INSTITUTIONAL DIALOGUE"—FROM CONCEPT TO COMMITTEE

Paul Meyer | ICT4Peace

The call for a "regular institutional dialogue" to continue consideration, under UN auspices, of the subject of information and telecommunication technologies (ICTs) in the context of international security has been a refrain in all three reports adopted by the UN's Groups of Governmental Experts (GGEs) on responsible state behaviour in cyberspace. That said, this common recommendation of successive GGEs has not progressed much beyond a slogan in the work of the Open-ended Working Group (OEWG) on ICTs. There has been surprisingly little input from states as to the specific form this dialogue should take and how in particular it should be "institutionalised".

The zero-draft of the final report before the OEWG at its final March session does not provide much in the way of actionable guidance on how this "regular institutional dialogue" is to be manifested in future. The draft report suggests in paragraph 109 that it should be "inclusive, transparent, consensus driven and results based"—all desirable qualities, but ones divorced from any specific institutional form. After five years of GGE consensus reports and over two years of OEWG discussions, it is time for the UN to establish an on-going inter-governmental body to work on international cyber security issues.

At a time when the magnitude of malicious cyber activity, including state sponsored offensive cyber operations is increasing exponentially, with concomitant damage to the interests of "netizens" everywhere, it is imperative that the "institutional deficit" in the UN's work on cyber security issues is remedied. Certainly, non-governmental stakeholders have voiced this concern during the OEWG proceedings, and it was a noticeable theme in the dedicated informal consultations with stakeholders that were held on the topic in December 2020.

The tabling of a proposal for a programme of action in the OEWG by a group of 47 states has finally contributed a substantial answer to the question of what form should the institutional home for future UN work take. The proposal envisages the establishment of a permanent forum open to all member states that would provide for biennial meetings and periodic review conferences as well as working level thematic sessions. It would be allotted secretarial support via the UN Office for Disarmament Affairs (ODA) and/or the UN Institute for Disarmament Research (UNIDIR). The proposal suggests that by creating this permanent forum the UN could consolidate the twin processes of the OEWG and the GGE into a single venue and focus for the UN's cyber security work.

The programme of action proposal is a welcome initiative in imparting institutional content to the more nebulous ideas of a regular dialogue, but it too could be rendered more precise in its prescription. In submissions to the OEWG by ICT4Peace it has been suggested that the time has come for the UN to embrace the reality of major on-going work on international cyber security policy by creating a "Cyber Security Committee" of the UN General Assembly (along the lines of the Committee on the Peaceful Uses of Outer Space). It would also be appropriate to provide such a committee with a dedicated secretariat in the form of an "Office of Cyber Affairs". One could argue that the cyberspace realm is of equal or even greater importance than outer space for global security and prosperity and will continue to be of major significance for advancing UN goals for the foreseeable future.

Whatever emerges as the final report of the OEWG, one can only hope that it will go beyond the reiteration of the need for a "regular institutional dialogue" and actually provide an institutional blueprint to make this happen.

NOT QUITE SO "OPEN": REFLECTING ON STAKEHOLDER ENGAGEMENT IN THE OEWG ON ICTS

Sheetal Kumar | Global Partners Digital

As we head into the third and final session of the first Open-ended Working Group (OEWG) on information and communications technologies (ICTs), it's difficult to know what to expect. The OEWG is no exception within the United Nations when it comes to the impact of the COVID-19 pandemic on its process, including its calendar of meetings—and the general challenges it has faced in trying to reach consensus on the most contentious parts of its mandate. One area where it has managed to be unique though, unfortunately, is its lack of openness to civil society.

As mentioned in joint civil society statements to the first and second OEWG sessions and as addressed by a number of states in their remarks as well in relevant processes elsewhere (First Committee,[1] Arria formula meetings[2]), this is deeply regrettable. By shutting out civil society, the possibility of integrating valuable expertise and experience is lost, and moreover—there is a risk that discussions on state behaviour in cyberspace discount the impact of their behaviour on that which matters the most: people, their rights and the well-being of society as a whole. Considering the topic at hand—ICTs—are used on a daily basis by billions of people and which is almost exclusively developed and operated by non-governmental stakeholders, this lack of openness also risks making the discussions and their outcomes less effective in the long-run.

The pandemic and the world's increasing reliance on digital technologies had placed a concomitant emphasis on the importance of these discussions. Yet, as the UN attempted to grapple with the need for new working methods as the COVID-19 pandemic took hold, civil society struggled to find information on what was happening, how long meetings were going to be delayed for, and what would happen in place of in-person meetings. When informal intersessionals were held to discuss various iterations of the OEWG's final report, non-governmental organisations were not invited.

This greatly limited the ability of civil society to play any meaningful role in the dialogue. As a result, a group of member states, civil society, and industry stakeholders worked together at the end of last year to fill this gap and provide a space for stakeholders to share their perspectives on the OEWG's pre-draft text.

This event, dubbed "Let's Talk Cyber" was a success, with each session attracting around two hundred people from an average of twenty countries spanning regions across the world. The outcome report makes specific recommendations relating to each part of the OEWG's mandate, many noting the need for greater collaboration with all stakeholders, the need for a human-centric approach, and strong support for implementing agreed outcomes. These were overarching points; the report also includes concrete and actionable recommendations for how to take forward discussions across the OEWG mandate, from the less contentious sections on capacity building to the more challenging areas like international law.

Building on that success, some of those involved in the December event convened an event at the end of February 2021 to collect non-governmental stakeholders' views on the zero-draft of the OEWG report (then the latest version of the report). Much of what was said there echoed the key points from the longer December event, but the recommendations were more focused on the text of the zero-draft, noting omissions and areas where the text could be strengthened. Yet, these events should not be seen as a substitute for formal, and institutionalised engagement. They were organised because of a lack of formal opportunities to engage, and in the future should be regarded as complementary to and not a replacement for formal and institutionalised engagement.[3]

Non-governmental stakeholders are, like states, diverse and they vary widely in their expertise, interests, and mandates. These two multi-stakeholder events showed that. They also showed

that there is a huge appetite and interest among stakeholders in supporting the work of these discussions in the First Committee; in ensuring that they are effective, responsive to what is happening "on the ground" outside the well-pounded rooms of diplomats at the UN (whether virtual or otherwise); and that they work for everyone.

It's hoped that the third and final session will allow for meaningful engagement of civil society, and that whatever future dialogue unfolds (including the next OEWG) will learn from the lessons of this OEWG and institute inclusive mechanisms for the engagement of the wide range of people and groups who have a strong stake in these important discussions.

NOTES

1. For statements delivered during the UNGA First Committee, see https://reachingcriticalwill.org/disarmament-fora/unga/2020/statements.

2. "UN Security Council meeting highlights the cyber peace and security challenges wrought by the COVID-19 pandemic," 28 May 2020, https://www.reachingcriticalwill.org/news/latest-news/14706-unsc-meeting-highlights-cyber-peace-and-security-challenges-wrought-by-the-covid-19-pandemic.

3. This briefing paper outlines good practice examples on stakeholder engagement in multilateral and multistakeholder forums: https://www.gp-digital.org/wp-content/uploads/2020/06/ngo-participationgoodpractice_gpd.pdf.

STAKEHOLDER RECOMMENDATIONS FOR THE ZERO-DRAFT OF THE OEWG FINAL REPORT

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

As outlined in the preceding article, non-governmental stakeholders presented their views on the zero-draft of the OEWG's final report during an informal virtual consultation held on 25 February. The four-hour event attracted around 200 participants from across the globe who actively participated in the discussions, and was organised by Global Affairs Canada, Global Partners Digital, Microsoft, Research ICT Africa, and WILPF.

The full summary report (forthcoming) offers an overview of each session, as well as items that stakeholders expressed wanting to retain, modify, or remove from the zero-draft. A video recording is available online.

This article has extracted the recommendations that emerged from each of the thematic sections. States and others are encouraged to read the full report for greater detail, which is being prepared by Global Partners Digital with inputs from other organisers and moderaors.

I) Existing and emerging threats:

- The report should put greater emphasis placed on the human and societal impact of malicious cyber operations, emphasising that it is humans who are impacted by cyberthreats and attacks.

- The report should maintain the focus on the abuse of ICTs, and the behaviour of both state and non-state actors, not the technology itself.

- In line with this point above, the report should put greater emphasis on the increased threats to critical infrastructure and to parts of the ICT infrastructure, including for example the public core and ICT supply chains, that require protection.

II) Rules, norms, and principles:

- Place more emphasis on a multi-stakeholder approach to norms implementation, which should be a fully inclusive process. At the

same time, highlight that there is a need also for disclosure of implementation and to monitor implementation of norms.

- Provide practical examples on multi-stakeholder cooperation, on how stakeholders are working on implementation of norms, or developing best practices on implementation of norms.
- Indicate that states, in consultation with other stakeholders should identify the relevant frameworks, such as national cybersecurity strategies and policies, where the norms can be operationalised at the national and regional levels.
- Encourage states to publish their position on how they interpret and how they want to operationalise norms. That would support monitoring and implementation.
- Actively encourage activities that help with norm dissemination.
- Annex the norms guidance described in paragraph 51 to the final report of the OEWG, to help diffuse the guidance contained therein, if it cannot be incorporated directly within the report.

III) International law

- There were numerous specific textual suggestions contained in the full report. Some are recommendations that would give precision and accuracy to the report, while others are calls for stronger language or in some cases, new conclusions or recommendations.
- A general recommendation shared by most participants is that states need to move beyond the general acknowledgement about the applicability of international law to their cyber behaviour and in using ICTs and really begin to describe and outline what this means practically, how they interpret the law, and on what legal basis relevant actions stand.

IV) Capacity-building

- Paragraph 83 should be part of the conclusions and recommendations.
- Gender should be mainstreamed in the design, implementation, and evaluation of capacity building programmes.
- Reference to engaging non-state actors should be included in the recommendation section.
- The need for greater resources to be made available for cyber capacity-building (CCB) efforts should be included in the recommendations section.
- The CCB agenda should be survey-based and agile so that CCB is tailored to the countries' needs.
- CCB should be part of the wider sustainable development agenda

V) Confidence-building measures (CBMs)

- Formalised regional exchange. Regional organisations play an important role in translating CBMs into practice, including through information exchange, capacity building, and gathering of best practices. At the same time, dialogue between different regional organisations, as well as complementary dialogue at the global level, can support CBM adoption. There is a further need for formalisation of the regional exchanges on a regular basis under the UN auspices to avoid leaving this exchange on an ad hoc basis.
- The role of non-state actors. In different national and regional initiatives, non-governmental stakeholders are actively involved in the discussions on how to implement CBMs. Non-governmental stakeholders can play key roles in capacity building, as well as in the design, implementation, monitoring and evaluation of CBMs. The report recognises that there is a variety of multi-stakeholder initiatives that exist to contribute to CBMs, but the text could be stronger on the need for greater transparency and information sharing on the implementation to assess their effectiveness in different contexts and this way contribute to more effective implementation. There is a role for other stakeholders including CSOs in supporting the understanding of their effectiveness and the report could include

this reference in stronger terms and in the recommendations.

- Actionable language. The desirability and viability of establishing a global repository of CBMs under the UN auspices included in the report were welcome, yet a more actionable language referencing that states should undertake concrete steps toward developing global CBMs would support progress and move the discussion beyond more general statements.

- Greater transparency. States should be encouraged to take more measures to be transparent about their behaviour, whether by publishing policy documents on the cyber policy portal or otherwise. This would help to understand the motivations behind certain actions and developments and build among state and non-state actors.

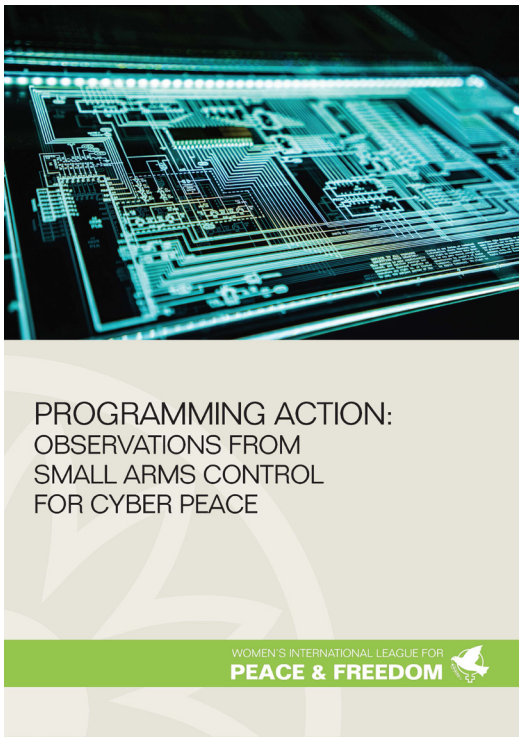
VI) Regular institutional dialogue

- Some participants made recommendations and observations during this segment that are broader than textual suggestions for the zero draft of the final report. Textual suggestions can be found in the full summary.

- There was discussion about the human element and role of individuals in cyber security decision-making, as well as about what basic standard or level of security should be expected. Even while these are technical discussions, the role of individuals within them should not be overlooked.

- One participant built on earlier discussion and comments about doing more to build in security at the outset of a product's development process but noted that there is little incentive to do so. This participant encouraged to "level the playing field" and asked everyone to engage in "secure by default" processes in order to allow everyone to innovate without sacrificing security. This approach could combine with building trust, confidence, capacity, and awareness to enable a new security cyber environment.

- Finally, and while not framed as a recommendation, there was some discussion in this segment about the new (second) OEWG that will begin work later in 2021, including the problematic way in which it was established and that the potential for non-governmental stakeholder participation is not yet determined.



A new briefing paper from the disarmamen programme of the Women's International League for Peace and Freedom (WILPF) explores observations from the UN Programme of Action on small arms and light weapons process that can be applied to the growing calls for a programme of action on state behaviour in cyberspace.

We have identified five observations from our experience in engaging with the small arms UNPoA that we deem relevant for the international cyber security community to consider as it moves forward. This briefing paper is informed by interviews with other civil society experts, as well as publicly available analysis and commentary.

Read the briefing paper.

BRINGING GENDER ANALYSIS INTO INTERNATIONAL CYBER SECURITY

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

> "Gender matters in international cyber security. It shapes and influences our online behaviour; determines access and power; and is a factor in vulnerability. As a result, malicious cyber operations can differently impact people based on their gender identity or expression."[1]

When the Open-ended working group (OEWG) held its first substantive session in September 2019, only a small handful of governments and civil society representatives touched on the gender dimensions of international cyber security in their statements.[2] These mainly pointed to the absence of gender diversity within international cyber security fora and capacity-building activities, specifically the lack of women's participation.

One and a half years later, as the OEWG moves to conclude its work, the gender dimensions of international cyber security are being more thoroughly explored, discussed, and hopefully will be meaningfully addressed within the Group's final report. However, references to gender are also being pushed back on by some, described in one instance as a "secondary" issue (alongside human rights and sustainable development). Even for supportive states, moving from acknowledgement of the issue into action will be necessary.

How it started

It was realised early on that while great strides have been made in recognising the applicability of human rights frameworks to gender-based threats and abuses in digital contexts, the gendered impact of international cyber operations and incidents, as well as gender inequality, has been a largely unexplored part of the discourse in more securitised cyber processes and fora.

"When the OEWG began, we were struck by the fact that gender considerations were simply absent from international cybersecurity policy discussions," said Sirine Hijal, Deputy Cyber Foreign Policy Coordinator of Canada. "This was surprising, given what we know about the positive impact that the meaningful participation of women and girls in other areas of international peace and security has had on those processes. Canada therefore sought to work with other States and with non-State actors to address this gap."

Specifically, Canada commissioned two research reports published in April 2020 that helped to fill this gap. *Why gender matters in international cyber security* and *Making Gender Visible in Digital ICTs and International Security* considered the gendered impacts of international cyber operations such as internet shutdowns, data breaches, and disinformation campaigns; while also identifying relevant touch points with other international frameworks and processes and feminist research in this area. The research reports were previewed and highlighted during a first-ever side event on gender and international cyber security that took place during the OEWG's informal multi-stakeholder meeting in December 2019.

Other research has followed. Most recently, the UN Institute for Disarmament Research (UNIDIR) released *Gender Approaches to Cybersecurity*, a report that explores from a more technical perspective how gender norms shape specific activities pertaining to cybersecurity design, defence, and response. There have also been more side events, webinars, and consideration given to gender diversity and awareness within specific capacity-building initiatives such as on cyber crime and during other cyber-related events.

Early in the OEWG process, a small group of states initiated the "Women in International Security and Cyberspace Fellowship". The fellowship supported the participation of more than 20 women from diverse global regions to participate to the second OEWG session in February 2020, all of whom work within their governments in either policy or technical roles related to cyber security. The fellowship programme has since included multiple

learning opportunities, both in-person and virtually since the start of the pandemic, and peer support.

"Thanks to the Women and International Security in Cyberspace Fellowship, women from around the world continue to meet virtually, build negotiations skills and discuss cyber issues," said the New Zealand Ministry of Foreign Affairs and Trade in a Tweet. "We are proud to support this Fellowship alongside Australia, Canada, the Netherlands and the UK.".

How it's going

At the close of the OEWG's second substantive session in February 2020, the Chair noted that something "fantastic" had happened, which elicited applause throughout the conference room—gender parity had been achieved. While an equal number of women and men participating in an international conference in the year 2020 shouldn't have seemed that farfetched or unusual, it unfortunately was—especially in the disarmament and arms control space.

"Based on my experience, it's absolutely crucial to take into account the perspectives of women and men, girls and boys," said Ambassador Jürg Lauber of Switzerland, the OEWG Chair during remarks to the Let's Talk Cyber side event in December 2020. "In order to develop the best solutions, to take best decisions, to make the UN's response to any problem that we face as humanity, we need to have these perspectives represented.".

Looking beyond participation, it was also noteworthy that by this second session a much wider and more cross-regional group of states were highlighting the importance of incorporating a gender perspective into OEWG discussions on international cyber security.[3]

These calls and the research underlying them have had impact, in that the most recent version the final OEWG report—as well as prior ones—contains multiple references to either gender, or to women. These are spread across most of its six thematic areas of focus. There is also a paragraph in the Introduction section (paragraph 11) which "welcomes the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions."

In this paragraph, "the OEWG underscores the importance of narrowing the "gender digital divide" and of promoting the effective and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security."

The majority of the other references are found in the section of the draft which outlines discussions that was had in earlier OEWG sessions. This means that while the report adequately reflects the discussion that was had on this issue, it only puts forward one gender-sensitive recommendation contained paragraph 55—that "capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory."

Whether this is owing to push-back from some states or other reasons, gender supporters within the OEWG should be bold and call for incorporating gendered aspects into conclusions and recommendations. Increased recognition and support for the gender dimensions of international cyber security in the OEWG comes at a time of heightened and growing recognition of the gender dimensions of security writ large—and specifically, how disarmament, arms control, and related processes and fora can incorporate gender analysis and perspectives into their work.

For example, in 2020, the UNGA First Committee adopted an unprecedented 18 resolutions (25 per cent of total resolutions adopted) that include gender references, recognising the various close interlinkages between gender and disarmament.[4] This includes a biennial resolution on women and disarmament, non-proliferation and arms control. Every year, more states also endorse a joint statement on gender at the First Committee. This is in addition to a wide range of research, reports, side events, and other obligations being undertaken in the context of specific security processes, treaties, and issues ranging from nuclear weapons to the international arms trade.

Where next?

The OEWG is the first forum of its kind on

international cyber security. Its final report can set a baseline for future work in this area. It's regrettable that there are not more conclusions or recommendations relating to gender in the current draft. If this is the case with the final adopted report, then states and other stakeholders are encouraged to act on the report's observations and be ready to come to future OEWG or other relevant meetings with greater knowledge, experience, or data. There are also important learnings from other frameworks and research to draw from, including in the area of human rights, or feminist studies of technology.

"Canada is pleased to have worked with others to raise the profile of this issue, which is now squarely on the map in UN cyber negotiations and will remain on the agenda of future UN cyber processes," notes Sirine Hijal, Deputy Cyber Foreign Policy Coordinator with the Government of Canada.

There is scope to go further in other ways, too. "Women" and "gender" are not synonymous, and an over-emphasis on *women's participation* at the cost of *gender diversity* risks entrenching binary concepts of gender identity and expression. It's also tempting to focus on participation issues over the more challenging and sometimes technical work of providing gender-sensitive cyber incident response; investigation; or relevant capacity building programmes. Bolder yet would be to incorporate a feminist peace approach to international cyber security and challenge how existing patriarchal structures of violence and repression are being replicated and exacerbated by technology and within cyber space.

NOTES

1. Deborah Brown and Allison Pytlak, *Why gender matters in international cyber security*, April 2021.

2. This included Australia, Canada, Mexico, New Zealand, Sweden, and the United Kingdom, as well as the Association for Progressive Communications and the Women's International League for Peace and Freedom. See Reaching Critical Will, *Cyber Peace & Security Monitor*, Vol. 1, No. 2, 11 September 2019; and *Cyber Peace & Security Monitor*, Vol. 1, No. 3, 16 September 2019.

3. Per our reporting, Australia, New Zealand, the Netherlands, Canada, Chile, Ecuador, Argentina, Italy, Bangladesh, Thailand, Slovenia, the European Union, the United Kingdom, Cameroon, South Africa, Kenya, Nigeria, Switzerland, APC, and WILPF all referenced the importance of incorporating a gender perspective into OEWG discussions on international cyber security at different points throughout the second session.

4. Katrin Geyer, "Gender and disarmament," *First Committee Monitor*, No. 5, 13 November 2020, p. 13.

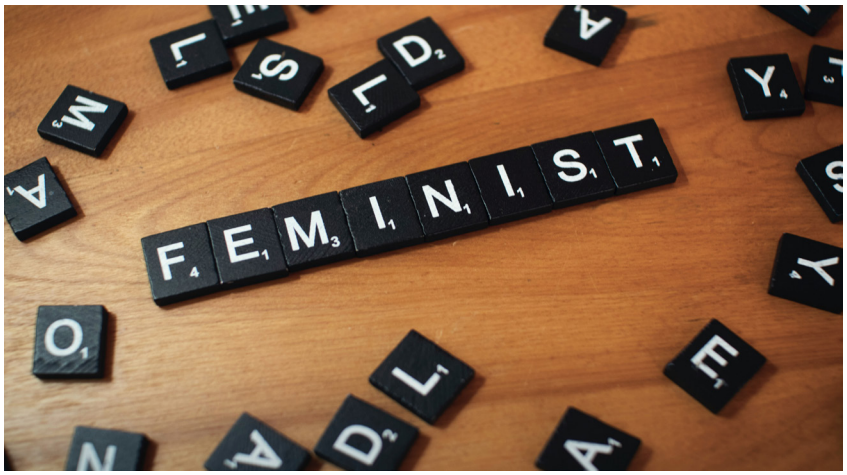


Photo: Jen Theodore | Unsplash

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. 01, No. 8
7 March 2021

Editor: Allison Pytlak

Contact: disarm@wilpf.org