Reaching Critical Will

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

Women's International League for Peace and Freedom

Informal inputs to the informal intersessional meeting of the UN Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025)

December 2022

On the occasion of the informal intersessional meeting of the second Open-ended Working Group (OEWG II) on security of and in the use of information and communications technologies (2021-2025), the Women's International League for Peace and Freedom (WILPF) is submitting the following informal inputs.

THEMATIC SESSION: Confidence-building measures (CBMs) and Points of Contact Directory *(*Not delivered orally)*

Thank you, Chair.

In the context of discussions about CBMs, WILPF would like stress the importance of transparency, accountability, and implementation of the existing normative framework. Undoubtedly, in a time of heightened geopolitical tension and a deteriorating online environment, the need for effective CBMs feels greater than ever.

The often covert and destabilizing nature of cyber operations and incidents uniquely escalate tension and crisis or generate misperception or misunderstanding. Therefore, activities that foster dialogue, help to cultivate common understandings, or aid in predictability can be powerful correctives. As has been the case in other areas of international security, trust and confidence emerge over time through consistent behaviour, information sharing, and demonstrable implementation of agreed commitments—in this instance, the normative framework and existing law.

Positively, diverse CBMs exist at regional and other levels, including among non-governmental networks and forums, thus providing a good basis for the OEWG's efforts in this area. Several of these existing CBMs have been identified and discussed by states and stakeholders in statements and submissions to prior sessions and in meetings this week.

Points of contacts directories are one such CBM already in use in some, but not all, regions or professional sectors. It will be important that the proposed OEWG directory not duplicate but find ways to complement, or even strengthen, existing similar directories. In listening to presentations yesterday and reviewing written inputs, it seems there are diverse understandings amongst states about the purpose of the directory. It will therefore be important to be able to answer the question about what the added, or unique, value of a UN-established points of contact directory, in a busy landscape?

And, as was highlighted in UNIDIR's presentation yesterday, there is a lot to be learned in looking at similar directories and networks from other First Committee issues. From amongst those being studied, we would encourage considering the experience of networks developed in the context of biological and chemical weapons, given that the dual-use nature of those threats and the types of actors involved may be more similar to the cyber and ICT environment, than directories about SALW, for example. We would also encourage that the

directory be an “active” network as much as possible—again, lessons from other areas show that if networks like these are kept passive, they also become dormant. Finally, the directory should be made available states and non-governmental actors, and also eventually account for relevant existing non-governmental networks and contacts. Gender diversity must be a consideration in its composition.

And so, while welcoming the plans to advance on a directory, it is important that the OEWG look to additional activities beyond a PoC Directory to build confidence. WILPF remains concerned that national implementation of the UN cyber norms is not being regularly demonstrated, and there is insufficient transparency about relevant state action.

This week we have heard many solid examples of CBMs that are currently in practice or could be considered by the OEWG.

There are of course a few CBMs already in the OEWG’s toolbox. States should follow through on the encouragement to submit their views to the UN Secretary-General on this subject, as set out in the OEWG I final report and reaffirmed in more detail elsewhere, such as the 1C resolution on ICT and the Annual Progress Report. The OEWG could, as has been proposed in past, also seek to standardise what information states include in their reports such as through a questionnaire, key questions, or survey, or ensure that information in reports is reviewed and utilised beyond their collation into the UNSG’s report, so as to incentivise the reporting process and utilise the data provided.

We also encourage states to be more transparent about cyber capacity and the conditions surrounding their use, such as by publishing relevant policy and doctrine, including on the UNIDIR Cyber Policy Portal. Linking cyber incidents, when they happen, to specific of the norms would also bolster shared understanding of how the framework is being implemented. During the 2019-2021 OEWG several proposals were made in relation to accountability both by states as well as non-governmental stakeholders, ranging from surveys to peer review mechanisms. It is regrettable that a more solid outcome in this area did not emerge from the Group, and WILPF encourages that accountability frameworks—as a component of building trust and confidence—be given more airtime in future OEWG sessions. In all of this work, there is a need for cooperation with non-governmental stakeholders, given their active role in threat detection, response, norms promotion, capacity-building, and more.

THEMATIC SESSION: CAPACITY-BUILDING *(**Delivered orally on 8 December)*

Question: How can States raise awareness of the gender dimensions of security of and in the use of ICTs and promote gender-sensitive capacity-building at the policy level as well as in the selection and operationalization of relevant projects?

WILPF welcomes that this is a guiding question, and that today there have been interventions from some states and also other stakeholders on this point.

In its intervention, Canada mentioned the small but rapidly growing body of research, tools, and training resources about gender and cyber security more broadly. In addition to the UNIDIR research mentioned by Australia, there is other research underway from GPD and the Association for Progressive Communications about gender in national cyber security strategies; and inclusivity in cyber norm development and implementation. Just earlier this week, the Global Network of Women Peacebuilders, ICT4Peace, and the Government of Switzerland hosted a workshop considering how to better account for cyber security in the context of WPS Agenda. WILPF participates in a working group convened by the Centre for Feminist Foreign policy about feminist approaches to international cyber security challenges.

In short, there is really a great wealth of initiatives to harness, and synergize with in the work of the OEWG.

Turning back to capacity building, and something Canada hinted at, it's important to bear in mind that there is not a "one size fits all" approach to gender sensitive cyber capacity-building. The form it takes will depend on the recipients of the activity and their particular interests, needs, concerns, background, and experience. Second, in the context of building capacity, we must be mindful of the structural barriers that impede gender diversity within technological sector as well as in cyber diplomacy, barriers which also contribute to unique gender-related ICT vulnerabilities, or the, unique reasons for why and how people use or access ICT in relation to their gender.

In this vein, I want to share again some concrete ideas that we have presented before about how the OEWG could continue discussion about GS C CB:

- In future sessions, we encourage the Chair to include more guiding questions about how states presently account for gender in their cyber-capacity building in order to help establish a baseline understanding of current practice in this area.
- Based on this, and experience of stakeholders, the OEWG could elaborate guidance on what gender-sensitive cyber capacity-building looks like practically or articulate a good practices document;
- Or, it OEWG might also consider identifying some key principles, or key questions, to consider when conducting gender sensitive cyber capacity building and knowledge sharing;
- States could be encouraged to consider supporting new research or work in this area, or convening side events and workshops during OEWG sessions.

Looking beyond capacity-building gender can and should be mainstreamed into other aspects of the OEWG's work: what would a gender lens reveal about threats and/or cyber incident response; how to advance gender diversity in confidence building measures. In this context, we remind that gender is not synonymous with women, and while boosting women's participation in cyber capacity-building is vital, approaching gender in such a binary way excludes people of more diverse gender expressions and identities, and overlooks intersectionality.

Finally, Chair, non-governmental stakeholders have a role to play in all of the above suggested activities, as well as in other local, national, or regional initiatives. Civil society is often at the forefront of advancing feminist and gender-sensitive approaches and analysis to security issues and can offer firsthand and "on-the-ground" perspectives as well as contribute expertise. This may be from the perspective of being users of ICT, of being builders of ICT, or also, as individuals or communities that have been adversely affected by ICTs on the basis of their gender.

THEMATIC SESSION: REGULAR INSTITUTIONAL DIALOGUE *(**Not delivered orally)*
Question: In considering the proposal for a Programme of Action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, how do States understand its relationship with the OEWG? In what specific ways can the POA complement the ongoing work of the OEWG?

Earlier this year, WILPF drafted a research report commissioned by the Government of Canada, to consider "options and priorities" for the proposed cyber PoA, which has subsequently been submitted to the OEWG for consideration by all participants. At the time, the resolution adopted earlier this week had not even been drafted and while the proposal for a PoA was not new, there were many procedural variables ahead of us.

In reviewing that report in preparation for this session, it appears that several of the main recommendations are still pertinent. Additionally, another report that WIPF authored in 2021 also remains relevant—that report looked closely at lessons learned and observations from the PoA on SALW. While small arms pose a different threat than those posed by cyber, the SALW PoA is the only other instrument to emerge from the UNGA First Committee and does offer some important lessons learned.

WILPF wishes to mention few points for the OEWG's consideration in its future discussion about the cyber PoA, drawn from these two publications:

- It is important to achieve clarity about the instrument's goals, and scope, early on. A primary consideration that surfaced repeatedly in the research concerned the purpose and impact of the proposed new instrument.
    - Be ambitious and forward-looking now. Changes to agreed text are rare and difficult to achieve in future/later meetings.
    - Make space to discuss these questions openly, and early in the process.

- Prioritise national implementation over international meetings. A lesson learned from the PoA on small arms has been that political deadlock during biennial meetings and review conferences has overshadowed national implementation successes.
    - Prioritise developing the content of the instrument and translating the acquis into actions—and let the follow-up meeting structure and cycle flow from there.
    - Design future meetings in ways that enable meaningful exchange and assessment of progress toward implementation; building confidence and cooperation; matching needs.

- Be inclusive of the stakeholder community.
    - Reference the role of diverse non-governmental stakeholders within the text of the PoA, including in national and regional work. Root this in the real interactions and the roles they play, vis-à-vis government, within cyber security.
    - Interact and consult with your national non-governmental stakeholders to hear their views on different aspects of a future cyber PoA.

- A PoA can be an umbrella, and a springboard.
    - It can bring together diverse existing norms and commitments.
    - It can also be a springboard to further action. Future-proofing the instrument will be key.
    - Importantly, as a politically binding instrument, a PoA can help to close the current accountability gap.