Women’s International League for Peace and Freedom

Inputs to the third substantive session of the UN Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025)

July 2022

On the occasion of the third substantive session 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 delivering the following remarks. These are informed by the guiding questions that were put forward by OEWG Chairperson H.E. Gafoor in his June 2022 letter to member states for the July session.

Re: Guiding questions on Capacity-building

The first set of the Chair’s guiding questions ask about the role played by non-governmental stakeholders in cyber capacity-building initiatives and projects. In this context, WILPF wishes to draw attention to the subject of gender-sensitive capacity-building, an approach endorsed by the final report of the 2019-2021 OEWG and which has subsequently been raised by governments as well as WILPF, the Association for Progressive Communications (APC), and other non-governmental organisations in contributions made during the first two substantive sessions of this OEWG.

In past meetings, we have suggested that the current OEWG could seek to elaborate guidance on what gender-sensitive capacity-building looks like practically. The guidance could take the form of, for example, a best practices document which the OEWG might develop; a list of key questions to consider or a checklist to facilitate gender-sensitive capacity-building; commissioning new research in this area; or in future meetings, the Chair could include more guiding questions on how states account for gender in their cyber-capacity building in order to help establish a baseline understanding of current practice in this area, and keep the topic on the agenda. We note that there is a recommended next step on gender reflected in the current draft progress report, although it is quite general and not specific to gender-sensitive capacity-building.¹

¹ Annex A Rev. 1, 20 July 2022 [DRAFT] 2022 Annual Progress Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, p.11, para 3 “States engage in focused discussions on the gender dimensions of ICT security and best practices on how to incorporate the gender dimension in ICT-related projects, for instance how gender-disaggregated participation records and other data can be effectively collected and utilized. Experts could be invited to make presentations on these topics to facilitate further discussion.”
Non-governmental stakeholders have a role to play in any 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 as the users of ICTs, as the builders of ICTs, or also, as individuals or communities that have been adversely affected by ICTs on the basis of their gender. It could also be in relation to expertise held on related subjects like human rights, or the Women, Peace and Security Agenda. Non-governmental stakeholders can partner with states in conducting a gender audit of existing cyber policies or laws in order to determine gaps where cyber capacity-building or knowledge-sharing is useful in non-technical fields while other actors may be useful in the provision of relevant gender-disaggregated data that could serve to identify gaps or needs.

Even generating awareness of gender issues in the context of international cyber security builds knowledge and capacity; and we take note of the small but rapidly growing body of research, tools, and training resources on this subject, much of which is civil society and academia-led.

WILPF would encourage states to continue approaching gender-sensitive capacity building by thinking on how to improve gender diverse participation, but to also think through what a gender-sensitive approach would look like in other aspects of cyber security: in the development of standards; in incident response; in legal measures., etc. We remind that gender is not synonymous with women, and while boosting women’s participation in cyber capacity-building is vital but approaching gender in such a binary way excludes people of more diverse gender expressions, and not necessarily taking an intersectional approach.

Re: Guiding questions on Implementing proposals contained in the draft annual progress report

Civil society has a significant role to play in working alongside member states and other non-governmental stakeholders to implement the concrete and action-oriented proposals contained in the draft annual progress report.

In the area of Threats, recommended next step #1 encourages the continued exchange on emerging and existing threats to security in the use of ICTs with the potential to impact international peace and security, and measures to address them. Civil society organisations are often on the front lines of experiencing ICT-related threats and can inform national governments of their impacts. This will enable responses that are rooted in real and lived experience and with an eye to their human rights implications. As one example, research undertaken by the Association for Progressive Communications, WILPF, UNIDIR and others has sparked an examination and discussion of the cyber threats that are experienced in relation to gender. Additionally, WILPF and other stakeholders are engaged in other areas of international peace and security, such as peacebuilding and disarmament, and have been active in raising awareness about the cyber-related threats facing existing weapon systems, or in connecting the dots between international peace and security forums through our research and policy analysis.
In the area of Rules, Norms, and Principles, as well as International Law, several of the recommended actions involve further exchange and elaboration on national understandings of the UN cyber framework. There are already examples of where civil society is contributing to activities like this; for instance, the Canadian norms guidance text received input from a diversity of non-governmental actors. Additionally, I would here like to mention a forthcoming project of the Stimson Center, which will seek to research and learn from how other areas of international risk—ranging from arms control to environmental standards—have been addressed by the international community through normative frameworks and existing law, and in particular, how aggressive or negative action has been deterred and accountability and effective implementation of the framework developed. In producing this research, Stimson intends to engage with other interested actors whether in government or civil society to cultivate and foster a sense of community around the subject of cyber accountability, while also continuing with its cyber accountability webinar series.

Finally, with respect to Regular Institutional Dialogue, and the recommended action on the cyber PoA proposal – earlier this year WILPF published an extensive research report at the request of the Government of Canada which considers possible options and key considerations for the further development of a global cyber PoA. Our research examined six existing UN PoAs, and through research and interviews, we tried to identify some of the major questions and concerns requiring deeper dialogue and consideration. I would also offer that the monitoring and reporting of UN OEWG meetings by WILPF’s disarmament programme, which follows on from our monitoring and reporting of other First Committee processes, aids in the overall effort of regular institutional dialogue by providing an informal but public record and accounting of OEWG meetings, thus also improving transparency.