Reaching Critical Will

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

Women's International League for Peace and Freedom

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

December 2021

On the occasion of the first 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) wishes to highlight what it sees as key priorities for work of the Group. These are informed by some of the guiding questions that were put forward by OEWG Chairperson H.E. Gafoor in his November 2021 letter to member states for the December session. It includes points on the meaningful inclusion of civil society; human-centric and gendered perspectives; threats and concerns; and points in relation to law, norms, and accountability.

Meaningful inclusion of civil society

The value that civil society brings to multilateral forums on cyber peace and security cannot be underestimated. In the context of the OEWG II, formal participation of a range of civil society stakeholders is crucial for the transparency, credibility, and effectiveness of the process. The informal mechanisms developed during OEWG I are commendable and were productive but should not become a substitute for formal participation such as is common across the UN system.

A letter delivered to the OEWG Chair on 7 December[1] outlines five principles for more meaningful inclusion of civil society in OEWG II, following the blanket and anonymous rejection of several non-ECOSOC holding relevant stakeholders throughout the OEWG I process by a few member states. The letter was supported by more than 40 UN member states, and dozens of civil society groups and individuals, including WILPF. It builds on concrete proposals put forward in this regard by some governments during the OEWG II organising session in June 2021. It also considers ideas and examples put forward in relevant studies and informal publications from non-governmental stakeholders.[2]

[1] Available online at https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/letter-to-chair_9December.pdf.

[2] See: *Promoting stakeholder engagement at the Open-Ended Working Group on ICTs: Operationalising para.4 of the UNGA Resolution (A/RES/75/240),* November 2021, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/stakeholders-OEWG.pdf; and *Multistakeholder participation at the UN: the need for greater inclusivity in the UN dialogues on cybersecurity*, November 2021, https://pariscall.international/assets/files/10-11-WG3-Multistakeholder-participation-at-the-UN-The-need-for-greater-inclusivity-in-the-UN-dialogues-on-cybersecurity.pdf.

WILPF strongly supports the contents of the letter and principles and methods proposed. We see it as vital that the status quo of the first OEWG not be extended into this new process, not least considering its even longer duration.

Human-centric and gendered perspectives

WILPF advocates for the continued evolution and application of the human-centric approach to international cyber peace. This approach gained traction throughout the OEWG I and we encourage states and other stakeholders to continue to explore the meaning of the term and apply it to their work. We understand this concept as accounting for, among other things, human rights and fundamental freedoms in the context of international and state-sponsored cyber policies, operations ,and use of ICTs. WILPF believes that there is good inspiration to be found in the transformative concept of "humanitarian disarmament"[3] which is now commonly accepted and recognised as a people-first and inclusive approach to international disarmament, non-proliferation, and arms control.

In this vein, WILPF warmly welcomes that the OEWG I final report and Chair's summary included references to and support for women's participation in cyber security and in cyber capacity-building, and also the improved gender diversity in most OEWG I sessions.[4] This has established a new baseline which forms a foundation for further work and progress during OEWG II and was informed by the inputs of non-governmental experts as well as a diversity of member states.

We encourage states to consider gender diversity in the composition of their delegations to future meetings and for the OEWG II Chair to actively encourage this. We also encourage that space be made in the agenda for a deeper dialogue and action about the gender dimensions of international cyber security, and remind that "gender" encompasses more than considering women alone but also applies to men, boys, and people of diverse gender identities and expressions.

Deeper dialogue and action could include, for instance, more thorough exploration of the gendered impact of cyber operations and relevant responses; the application of other frameworks such as the Women, Peace and Security Agenda and human rights frameworks and resolutions; how to increase the evidence and research base; and integrating gender considerations into cyber capacity building. Gender should be mainstreamed across the OEWG agenda, and not siloed off into a separate working group, as had been suggested during the OEWG II organising meeting in June 2021. Additional ideas have put forward in a position paper from Canada[5] and outlined in report from an online meeting convened by WILPF, Canada, and the UN Institute for Disarmament Research on 30 November to consider how to advance gender consideration in upcoming UN processes.[6]

---

[3] See https://humanitariandisarmament.org/about/.

[4] For an analysis, see Veronica Ferrari, "Why should gender matter (more) for the OEWG?", Cyber Peace & Security Monitor, Vol. 1, No. 10, p.7, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf.

[5] Available at https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/canada-positionpaper-december2021.pdf.

[6] See p.4, *Cyber Peace & Security Monitor* Vol 2., No. 2, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor2.2.pdf.

Threats and concerns

WILPF is concerned about the growing role of a range of actors that can be considered cyber mercenaries[7] and proxy actors and urges a greater focus on this in the OEWG II, building on past recognition of this problem by relevant UN Groups of Governmental Experts and some states during OEWG I. A recent report[8] from the UN Working Group on Mercenaries highlights that, "…some States, either by commission or omission, obscure their involvement in malicious cyberoperations, seeking to gain strategic military influence by evading their responsibilities under international law, including for violations and abuses committed by non-State actors recruited for this purpose. However, recruiting private actors to provide military and security services in cyberspace does not relieve States of their obligations under international law." We wish to bring to the OEWG's attention that the same report also recommends that this OEWG should further address human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations. However, any consideration of mercenaries or other private or non-state actors should not overlook the legal and ethical responsibilities of states such as in recruitment, deployment, and support of non-state actors, among other activities.

As a feminist organisation, WILPF challenges militarism and violence. We have expressed to this and other bodies our concern about the militarisation of cyber space, including through the growing development of offensive, or malicious cyber capabilities, and their growing role in formal military doctrines and strategy. The OEWG I report acknowledged that a number of states are developing ICT capabilities for military purposes, but merely recalling this fact will do little to stop states from developing such capabilities. In this context, we wish to point out that stability in cyberspace should not be taken as a substitute for cyber peace and urge the OEWG II to be driven in its work by a desire to protect the inherently peaceful character of cyberspace.

Finally, we encourage OEWG II, as a body established by the UNGA's First Committee on Disarmament and International Security, to not overlook issues relating to weapons security in its consideration of cyber threats. The vulnerabilities of nuclear facilities, the potential for network interferences, and growing illicit online arms trafficking are real challenges for global and regional peace and security. As relevant weapons fora are starting to consider these topics as well, it would be important for the OEWG to address them in tandem. WILPF views these new risks and vulnerabilities as a powerful rationale for disarmament and demilitarisation.

Law and norms; accountability and transparency

We agree that it is important and necessary for states to use the OEWG as a space to facilitate exchange on how they interpret international law as applying to state behaviour

[7] In its submission to the UN Working Group on Mercenaries, WILPF identified several types of actors that could be considered a cyber mercenary. These include APT groups; cyber militias; private companies; individual actors; PMSCs; among others. The lack of a clear definition of a cyber mercenary has been acknowledged by others. See https://reachingcriticalwill.org/images/documents/Publications/cyber-mercenaries.pdf.

[8] *Use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination,* A/76/151, 15 July 2021, https://undocs.org/A/76/151.

and use of ICTs, as set out by OEWG I. This includes both their own behaviour but also that of other states and actors, in order to build clarity and understanding around which norms and laws are being violated, when, and why it is seen as such. It is worth bearing in mind that if states already recognise and accept the rule of law, and the applicability of international law to state behaviour in cyber space, then the international community must guard against picking and choosing of which rules apply, and which do not, in an inequal manner. While the current combined approach of applying existing law and the voluntary normative framework is accepted by all states, the evidence shows that it is not enough to deter malicious cyber operations. In this context, WILPF underscores that the potential for a legal instrument should not be ruled out solely on the basis of past proposals in this area and lingering politicisation.

Given the current unlikelihood of a cyber legal instrument however, other avenues must be pursued to ensure norms adherence and compliance with existing law to close the existing accountability gap and end impunity. This particularly includes mechanisms that foster transparency and accountability, or help to harmonise cyber-relevant law, which WILPF views as necessary for cyber peace.

The proposal to create a cyber programme of action (PoA)[9] merits expedited consideration, and action. A politically binding cyber PoA could be become an umbrella for bringing together diverse normative frameworks—such as those negotiated inside the UN but also in external forums—and take into account existing regional frameworks and cooperation, while facilitating practical actions including capacity building. What will be crucial, however, is for PoA-supporting member states seek to use the opportunity of a politically binding instrument to meaningfully address and curb aggressive cyber behaviour, and not simply preserve the status quo. A new instrument, even if predicated on the existing *acquis*, is an opportunity to go further and make a difference in preventing cyber harm.

During OEWG I, several proposals were made in relation to accountability both by states and civil society. It is regrettable that a more solid outcome did not emerge from the Group, and WILPF encourages that it be a top priority moving forward. As a simple first step, states should follow through on submitting their views to the UN Secretary-General on this subject, as set out in the OEWG I final report and reaffirmed in more detail in First Committee resolution A/C.1/76/L.13. While the resolution offers more guidance to states on what to include in national reports than previous resolutions did, the OEWG could also seek to standardise what information states include in their reports such as through a questionnaire or survey, as was proposed during OEWG I, and ensure that information in reports is reviewed and utilised, so as to incentivise the reporting process. Acting on the recommendation to establish national contact points would also be an easy step to aid in transparency, confidence-building, and information-sharing. However, WILPF encourages states to use the opportunity of the OEWG II to go further toward establishing effective accountability mechanisms and practices that will foster cyber restraint, prevent cyber harm, and prevent conflict.

[9] Available online at https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/poa-workingpaper-december2021.pdf.