Informal Multi-stakeholder Cyber Dialogue

[SIDE EVENT] GENDER APPROACHES to CYBERSECURITY
09 December 2020
SIDE EVENT REPORT

GENERAL SUMMARY

As part of the Informal Multi-Stakeholder Cyber Dialogue, the *Gender Approaches to Cybersecurity* side event aimed to help shed light on the numerous initiatives relating to gender and cybersecurity. There were 185 participants who joined the event from Zoom and the Livecast including government representatives, non-governmental organisations, academia, and private sector stakeholders. The Livecast attracted viewers from 16 countries and 23 cities around the world.

SESSION OUTLINE

Allison Pytlak, Programme Manager at the Women's International League for Peace and Freedom (WILPF) moderated the session. Sirine Hijal, Deputy Cyber Foreign Policy Coordinator, Global Affairs Canada opened the event by highlighting three achievements related to incorporating gender approaches in international cybersecurity discussions. These include:

- Increasing support from many States for addressing gender issues at the UN Open Ended Working Group (OEWG).
- Research funded by Canada on gender and cyber (available on the OEWG portal here and here) which has led to more research efforts, providing better data and better analysis to inform the OEWG's work.
- Thanks to the *Women in Cyber Fellowship Program,* the OEWG achieved equal participation of women in its in-person meetings, which is a first for a First Committee-based process.

Collectively, these achievements have built a base of future experts who can mentor others and show the possibility those women have in contributing meaningfully to cybersecurity negotiations.

Ambassador Jürg Lauber, Permanent Representative of Switzerland to the United Nations, also shared his experience as OEWG Chair and involvement in other UN processes, including in his role as an International Gender Champion. Amb. Lauber drew two important lessons from these efforts:

- *The importance of diversity*: where diverse perspectives and experiences can enrich international discussions, and this can also ensure that we propose the best solutions to address the common challenges we face.
- *Representation of women*: women remain underrepresented in multilateral negotiations, even if there have been efforts to promote the participation of women through initiatives such as the International Gender Champions (IGC).

UN Institute for Disarmament Research (UNIDIR) Consultants Kate Millar and James Shires then presented their forthcoming research on the interconnections between gender norms and the field of cybersecurity. Dr Millar highlighted the difficulty in identifying the connections between gender norms and cybersecurity, as both are highly abstract concepts.

Dr. Millar also explained that gender informs cybersecurity in two ways: first, gender norms can construct individual roles, identities and expectations about behaviours in the cyberspace; second, we can also think about how gender operates as a hierarchical social structure. Dr. Shires further explained that there are three ways through which cybersecurity standards can become, first, more gender-sensitive and then ideally, more gender-responsive:

- Meaningful participation in the development and consultation around the creation of standards.
- The language and content of standards need to be examined from a gender perspective.
- Measuring the impacts of the standards based on disaggregated data collection.

Next, Paloma Herrera, researcher and coordinator of the gender and cybersecurity course at the University of Chile, also complemented UNIDIR's research findings, but from a cybersecurity policy level. She looked in particular at the main objectives of Chile's National Cybersecurity Policy, which strives to improve the security of standards in cyberspace and to ensure the full enjoyment of fundamental rights for people in equal conditions. She stressed that to achieve this objective, multilateral cooperation is essential.

Finally, there was a short presentation by Mila Francisco, diplomat at the International and Human Security Division in the Ministry of Foreign Affairs of Chile in Santiago and an active participant in the *Women in Cyber Fellowship Program*. She shared her personal experience as a fellow and discussed the impact of the programme on the OEWG process. She sees the fellowship programme as a driving force for encouraging female government representatives in the OEWG, and in building a strong peer network among its participants. After the moderated discussion amongst the speakers, the moderator opened to floor to questions and comments, including interventions from participants on the Zoom call and livestream chat. Some of the main themes of these discussions are captured below.

MAJOR THEMES / AREAS OF CONVERGENCE
The side event on *Gender Approaches to Cybersecurity* offered an opportunity for both State representatives and non-governmental stakeholders to further explore the inclusion of gender in cyber security and how this issue can be addressed at the OEWG and in other processes. As such, women's and gender diverse participation and representation was a major theme throughout. Some suggestions made in this regard by participants in the Q&A included: gender mainstreaming; the value of gender literacy and knowledge; and finally, it was noted that addressing gender equality and feminist concerns can and should become a regular feature of international cybersecurity discussions. One participant asked about how to increase gender diversity among non-governmental OEWG participants as well, and another highlighted that

there are also many regional and local groups of women that work in cyber whose perspectives could be leveraged to strengthen UN discussions.

The use of data was also highlighted as an important factor in supporting the work of promoting gender inclusion. It was stressed that by using data, we can improve interventions and support the practice that women are amplifying each other's voices in discussions. Even though current data available on this issue is limited, there may be data available about other processes which can be leveraged and supported in cyber processes. Finally, it was recognized that the participation of male allies and gender champions at the top of cyber organizations, the UN and foreign ministries is also necessary to make progress on these issues.

Beyond the above themes, the side event discussion highlighted areas for further work or research. This includes questions around how to broaden discussions of what constitutes 'expertise' and how to overcome gender-blindness within the technology sector and in government; and how to also improve awareness about potential gendered impacts of cyber operations, or gender biased algorithms. One participant noted that the term "gender" has become weaponised in online spaces and used as a mobilising tool by non-state actors, while another participant pointed to the importance of going beyond numbers alone, given that state representatives of any sex or gender are still bound by the instructions they receive from their governments, and that the formulation of security policy is often 'male-centred'.

NEXT STEPS

In terms of next steps, UNIDIR promised to share the research report authored by Dr. Millar and Dr. Shires on gender and cyber in January, when it is finalized. In the meantime, a commentary from them is available on the UNIDIR website. Canada will keep working with other States who are interested in addressing gender issues by promoting text to address gender in the OEWG report, including the gender text proposals that are included in Canada's broader OEWG text proposals. Dr. Herrera and other Chilean researchers will continue sharing their research on gender and cyber as well, building on the papers that were already uploaded to the gender section of the event series site.