Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security"

Summary

This paper outlines the issues that Canada would like to see addressed at the 2021-25 Open-Ended Working Group (OEWG), in a manner that builds on the acquis of the 2013, 2015 and 2021 consensus reports of the UN Groups of Governmental Experts (GGEs), as well as on the 2021 consensus OEWG report. First, Canada proposes that the 2021-25 OEWG focus firstly on practical measures to apply and implement the voluntary norms of State behaviour adopted in the 2015 GGE report and reaffirmed in the 2021 consensus OEWG and GGE reports. The OEWG could also aim to provide additional guidance on the implementation of the 2015 GGE norms, building on the guidance in the 2021 GGE report. Second, we hope that the OEWG can further build common understandings of the application of international law to state behaviour in cyberspace. Third, given the broader scope of the OEWG, and the participation of a wide variety of actors in this process, Canada hopes that the OEWG will be as inclusive as possible when it comes to stakeholder modalities. Fourth, we hope that an eventual OEWG report will address the gender dimensions of cyber security. The rationale for this proposed approach and more specific examples of what could be included in the OEWG report are outlined below.

Background

The 2013 GGE report affirmed the applicability of international law to State behaviour in cyberspace. The 2015 report affirmed the 2013 report, with further elaboration on applicable international law, as did the 2021 GGE and OEWG reports. With the new OEWG slated to work for the next four years, and with multiple initiatives for dialogue and capacity building underway, there is an opportunity and a need to expand common understandings and the consensus on how international law applies in cyberspace.

The 2015 GGE report included eleven voluntary, non-binding norms of State behaviour in cyberspace. The 2015 report of the GGE was adopted by consensus in resolution 70/237, which "calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts." These norms were reaffirmed by the international community in the 2021 consensus GGE and OEWG reports. The 2021 GGE report also provides guidance on the implementation of these eleven non-binding norms.

Canada sees the applicability of existing international law to State behaviour in cyberspace, together with the implementation of these agreed voluntary norms, as the foundation for sustaining international peace and security through the promotion of responsible State behaviour in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement and implementation in various forums (including the G7, G20, NATO, ASEAN Regional Forum and OSCE). Canada reaffirms the conclusions of the 2013, 2015 and 2021 GGE reports, as well as those of the 2021 OEWG report. We hope that the 2021-25 OEWG reaffirms the conclusions of those reports and builds on them, in a way that focuses on practical implementation of this acquis.

Issues that Canada will focus on at the 2021-25 OEWG

In order to consolidate and build on the achievements of the last two consensus GGE reports and the recent OEWG report, Canada will focus on the following issues, among others:

- *Norm implementation*: Developing an additional layer of guidance on the implementation of the 2015 GGE norms could better enable more Member States to implement them. The additional guidance could build on the norms guidance in the 2021 GGE report and could address topics such as the role of non-governmental stakeholders and human rights, including gender-focused considerations. If there is appetite among Member States, Canada may update and retable its 2021 OEWG norms guidance text, in order to advance the conversation on norms guidance and implementation. If most States feel that no new norms guidance is needed, Canada will focus on promoting the implementation of the 2015 GGE norms. This could be done by providing examples of how Canada has implemented these norms, by identifying barriers to norms implementation and by helping other States develop their capacity to implement the norms in a human-centric manner, for example.

- *International law*: In the first OEWG, Canada reaffirmed the applicability of international law to cyberspace and championed capacity building on international law. This led to a consensus recommendation for additional capacity building efforts, "in order for all States to contribute to building common understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community." To advance this objective, Canada will fund training courses on international law's applicability in cyberspace for the next two years. Canada will also work across regions to build common understandings and to have these reflected in OEWG consensus outcomes through 2025.

- *Gender*: At the 2019-21 OEWG, Canada advocated for the importance of mainstreaming gender considerations in the OEWG's work. Canada funded research on the gender dimensions of cyber security[1] and joined four other states in creating the Women in International Peace and Security in Cyberspace Fellowship program. This program funded the travel and participation of over 30 women diplomats to attend UN OEWG meetings, before the program went virtual because of the COVID crisis. This program allowed gender parity for the first time in a First Committee process, a fact that was noted by the 2019-21 UN OEWG chair. Donors are working on a revamped and expanded program that will be rolled out to promote the participation of women diplomats at the 2021-25 OEWG. Finally, at the 2019-21 OEWG, we proposed specific text on gender mainstreaming, some of which was included in the 2021 OEWG report. We hope to build on these efforts and have several proposals to advance this conversation at the OEWG. See Annex 1 for more on these ideas and other possible ways that gender can be further mainstreamed in the OEWG's work.

- *Stakeholder participation*: Canada sees it as essential for a successful and credible outcome that the OEWG process allow non-State actors to participate meaningfully in the group's proceedings. We hope that all relevant stakeholders are able to participate in this OEWG through formal and informal mechanisms, not just ECOSOC-accredited organizations, as was the case at the last OEWG. This would allow the optimal range of pertinent civil society and private sector actors (NGOs, women's groups, human rights organizations, academics, industry groups, tech companies, etc.), to provide input into the OEWG process. We hope that their input is reflected meaningfully in an eventual OEWG report. The contributions of civil society and NGOs are especially valuable in addressing issues such as online freedoms and gender equality issues,

[1] See Making Gender Visible in Digital ICTs and International Security by Sarah Shoker and Why Gender Matters in International Security by Allison Pytlak and Deborah Brown.

as well as in ensuring that States' human rights obligations are taken into account. The inclusion of non-State stakeholders greatly enhances the quality of our First Committee discussions, and strengthens the prospects for publicising and implementing our outcomes. For example, it is critical that we coordinate with—and receive input from—the private sector, which develops, controls, and operates the majority of global ICTs. At the same time, we must hear from and speak with civil society actors—including academia—who bring to the table a wide range of insights, including local perspectives, technical know-how, legal understandings and a human-centred focus.

- *Future mechanism*: Canada will continue to advocate for the creation of an inclusive, action-oriented UN cyber Program of Action (PoA) that will help States implement the acquis, coordinate capacity building efforts and better integrate the voices of non-State actors. In line with our objectives for stakeholder participation in the OEWG process, Canada believes that constructive participation of non-State stakeholders in an eventual PoA could provide insightful and valuable input into that group's work. We also believe that non-State stakeholders could play a significant role in the practical work of national and regional implementation efforts when it comes to implementing the acquis of past UN cyber processes. Canada will therefore continue to advocate for the creation of the PoA at the OEWG and elsewhere.

These are only examples of possible issues that Canada will likely raise at the 2021-25 OEWG. We believe that these proposals would lay the groundwork for the development of further practical approaches to expanding and implementing the acquis of past GGEs and of the recent OEWG. It would allow the 2021-25 OEWG to take stock of existing work done by the international community in these areas, to identify gaps and to explore avenues for future cooperation. We hope that the 2021-25 OEWG can reach a consensus report that incorporates some of the proposals outlined above, in order to keep the momentum going and build on the achievements of the last two consensus GGE reports and of the recent OEWG.

Annex 1:

Options to Mainstream Gender Considerations at the 2021-25 OEWG

Objectives of this paper

Canada sees this annex to our position paper as an opportunity to present some options about how gender considerations could be mainstreamed and addressed by the OEWG. This paper will present a menu of options, some of which we hope might eventually get retained. Addressing gender considerations at the OEWG could be a means to reduce and prevent technology-facilitated and online gender-based violence. Doing so would add value to the OEWG's work, while building on the work of the 2019-21 OEWG on this issue. While this annex focuses on the OEWG, the options presented below might also be relevant as we seek to address gender issues at an eventual UN cyber Programme of Action (PoA).

Options for addressing gender considerations at the OEWG

Broadening the acquis of past UN cyber processes on gender

While gender has not featured prominently in UN cyber GGEs, this issue was raised by over 20 States at the 2019-21 OEWG. The 2021 OEWG report included several mentions of gender issues:

> The OEWG welcomes the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions. 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. (page 3)
>
> Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory. (page 8)

The Chair's summary that was attached to the 2021 OEWG report included several other proposals with regards to gender text, notably in summaries of discussions made by the Chair (pages 5 and 8), as well as in text proposals made by Canada (pages 11 and 13) and Ecuador (page 17). Canada had also made previous gender text proposals in November 2020 that were reflected in the final OEWG report or Chair's summary.

We hope that at the 2021-25 OEWG and at an eventual PoA, States will outline the importance of gender in their written submissions and verbal interventions and will explain why they think gender issues are important. States could indicate what they perceive as the most relevant ways to advance this issue, perhaps drawing from some of the options laid out in this paper. States may wish to make additional gender text proposals, or support gender text proposals made by others. Previous UN cyber reports offer limited views on the gender aspects of cyber security. Canada hopes that this acquis will grow as more and more States recognize the importance of this issue.

Extending the Women in International Peace and Security in Cyberspace Fellowship Program to maintain gender parity at OEWG meetings

The Women in International Peace and Security in Cyberspace Fellowship program funded the travel of 30-35 women diplomats to attend the UN OEWG meeting in February 2020, before the program went virtual because of the COVID crisis. This program allowed gender parity for the first time in a First Committee process, a fact that was noted by the UN OEWG chair. This program has been hailed as a major success that can be expanded on. Donors, which now include the US in addition to the initial five donors, are working on a revamped and expanded program, which we hope will build on the positive results achieved at the 2019-21 OEWG.

Advancing gender equality via cyber capacity building

In addition to the type of capacity building of diplomats outlined above, several States have suggested that the OEWG could play a useful role in identifying cyber capacity building gaps. States could then work with organizations such as the Global Forum on Cyber Expertise (GFCE) to coordinate existing and future capacity building efforts to address some of those gaps. One such gap could be implementing capacity building projects in a way that addresses the gender dimensions of cyber security. This could include specific elements such as assisting States in:

- mainstreaming gender considerations into cyber incident response and cyber legal framework regimes;
- designing responses to cyber incidents in a manner that takes into consideration the gendered impacts of these incidents;
- factoring in gender considerations into project design, including when it comes to cybersecurity standards and threat modelling;
- building cybersecurity skills and expertise beyond STEM, by expanding into areas such as communications, ethics and legal governance; and
- building a community of cyber incident responders that is more diverse, i.e. that includes a greater participation of women and members of the LGBTQ community.

Promoting gender-sensitive capacity building could thus become a key objective of the OEWG's discussions on cyber capacity building. Gender considerations could also be taken into account when determining which capacity building projects to fund in the context of the OEWG. This would serve as an incentive for implementing organizations to build in a gender component to their proposed projects.

OEWG session on gender

Rather than addressing the gender dimensions of cyber security via side events, as was done on the margins of the 2019-21 OEWG, the 2021-25 OEWG could have a session dedicated to this issue during one of the OEWG's regular substantive meetings. Experts on gender and cyber security from government, civil society and the private sector could be invited to provide insights and formulate concrete recommendations on this issue. Subtopics to discuss could include:

- gender-related threats, including how internet shutdowns and data breaches affect women and the LGBT community differently;

- gender mainstreaming in national cyber strategies;
- taking gender into account when implementing the 2015 GGE norms; and
- how to mainstream gender issues in the OEWG's work.

These topics could then also be discussed in subsequent OEWG meetings, with a view to assessing progress made to date and ways to further address gender considerations in the OEWG's work. As such, the OEWG could become a forum to exchange best practices on how to address gender issues in international cyber security work, whether at the UN, in States' domestic cyber security strategies, or elsewhere. States could also be encouraged to report back, during their regular statements at OEWG meetings, and through their responses to the annual survey, on how they are implementing the gender-relevant aspects of the acquis.

Gender inclusive stakeholder modalities

Canada hopes that the 2021-25 OEWG will adopt more open stakeholder modalities than those adopted at the 2019-21 OEWG, in order to ensure that women and other marginalised excluded constituencies' voice are heard. In Canada's view, adopting stakeholder modalities that allow the full participation of all relevant non-State actors (academia, civil society, the private sector and technical community) would result in richer discussions that are more reflective of the broader cyber security community's views. Many of these organizations have an important role to play in the implementation of the acquis of past GGEs and of the 2019-21 OEWG, including when it comes to the agreed norms of State behaviour in cyberspace. Allowing the full participation of non-State actors would also be helpful when it comes to the OEWG's discussions on gender issues. Most cyber diplomats are not gender experts. However, some stakeholders from the academic and NGO (especially human rights groups) communities are gender experts, or have relevant experience in this field. Their participation in OEWG deliberations would therefore enrich the OEWG's discussions on gender issues. It would likely result in the identification of concrete action items that could help address the gender dimensions of cyber security in the OEWG's work.

Collecting gender disaggregated data and undertaking additional research on gender and cyber

During the 2019-21 OEWG, Canada identified a research gap when it came to addressing the gender aspects of cyber security. We therefore funded two papers, one by an academic and one by civil society researchers. Since then, other research on this issue has been carried out, including by UNIDIR. Additional research in this area would be beneficial. Its authors could present their work during OEWG sessions or side events on gender issues and their papers could inform the OEWG's work on gender and cyber security.

There is also a need for more data disaggregated by gender, including baseline data. This was a recommendation made in the 2018 SALW PoA report in the small arms context. In the cyber context, the research paper drafted by Brown and Pytlak recommended that "all actors should maintain sex- or gender-disaggregated participation records for all cyber security related work (diplomacy, capacity building, incident response, etc.)." [2]

[2] Allison Pytlak and Deborah Brown, *Why Gender Matters in International Cyber Security*, April 2020, p. 22.

Similarly, UNIDIR's paper recommended that "international standards organizations, in cooperation with national standards bodies, should identify, and collect data on, the areas where cybersecurity standards have gender effects." [3] Collecting more such data would be useful to inform the OEWG's work on gender issues and help identify gender-related gaps in cyber capacity building and research, and shed more light on the gendered impacts of cyber operations.

Conclusion

The above is meant as an initial menu of options that lays out how the 2021-25 OEWG could address the gender aspects of cyber security. We welcome the views of other States on these options, as well as any other options that they may wish to add to the list. We hope that some of these options will inform the OEWG's work on gender issues.

[3] Katharine Millar, James Shires, *Tatiana Tropina, Gender Approaches to Cyber Security*, January 2021, p. 25.