March 31 – CBMs

• Thank you Chair.
• Will discuss the work of a cross regional group on CBMs, then answer some of your guiding questions.

Cross regional group on CBMs

• On the first point, thanks Germany for convening an open, cross-regional group to advance CBMs at the OEWG.
• Canada proud to be part of this group, which has come up with lots of good ideas.
• These ideas will be presented by others in the group here today, and in a working paper to be posted on the OEWG portal between now and the July session.
• Canada championing gender and a transparency measure within this group.
• Gender: the paper will encourage States to share national policies on gender perspectives in cyber security.
• Transparency measure: Canada proposed at 2016-17 GGE that States be encouraged to share information on their active cyber capabilities and conditions surrounding their use.
• Proposal did not enjoy consensus, as some States felt that this might force them to share sensitive information. This was not the intent of our proposal.
• Rather, idea is simply for States who have active cyber capabilities to say so, and ideally to pledge that they will
use these capabilities in a manner that respects the norms and law.

- Canada and many others have already done this.
- This issue was raised again at the 2019-21 GGE, which Canada was not part of. We understand that this issue was proposed again, debated at length, and that the final GGE report includes a little bit of language on this.
- We applaud this progress at the last GGE, but we also think that more progress can be made at this OEWG.
- That is why Canada raised this issue within the cross-regional group convened by Germany.
- The idea enjoyed support within that group, and will be included in its working paper that you will all get to see in the coming weeks.
- We hope that this proposal will receive support among wider membership as it did within the cross regional group.
- This would be a simple, non-binding way to increase transparency about States cyber capability and conditions surrounding their possible use.

*Answers to your questions*

How can the OEWG substantively engage with regional organizations?
• Regional organisations are ideal venues for sharing best practices and raising the bar of cyber security amongst all the members.
• The OAS has also done useful work on CBM implementation that Canada has contributed to. For example, it has built a list of points of contact, and it has established a repository of cyber related policy and legislation.
• This is only one example of the great work that regional organizations have done on CBM implementation.
• Canada looks forward to continuing to take part in this important work.

How can the OEWG facilitate cross regional exchange of ideas, experiences and best practices?

• Canada has been proud to support the great work of regional organizations in implementing CBMs.
• For example, at the OSCE, we are championing CBM 4, along with Kazakhstan. It aims to promote information sharing on national approaches to ensure an open, secure, interoperable internet.
• This work will hopefully help protect the general availability and integrity of the internet, an objective shared by The Netherlands and others who have mentioned it this week.
• Despite this progress made within regional organizations, some States and regional organizations have indicated that they face challenges and barriers in the implementation of the CBMs recommended by the 2013 and 2015 GGEs.
• While previous reports laid out CBMs, they provided limited guidance on how the CBMs that were developed by the GGE could be translated into concrete State action.
• Rather than attempting to develop new CBMs, Canada hopes that the OEWG will focus on practical measures to apply and implement the voluntary CBMs and transparency measures adopted in the last two consensus GGE reports and in the 2021 GGE report.
• We look forward to working with you, Chair, and other member States, in order to move forward on this issue.
• Thank you.