Thank you Chair, as outlined in the suggested guiding questions you have shared, I would like to provide some detailed and specific initiatives on Canada’s cyber capacity building efforts. We hope this may offer some examples or lessons learned through which the UN could take on and support capacity building at the global level.

Since 2015, Canada, has committed $29M to cyber capacity building initiatives. These efforts seek to build an open, free and secure cyberspace around the world by helping states develop their technical and policy-level cybersecurity capacity.

As a direct result of Canada’s support, the Organization of American States, through the Inter-American Committee against Terrorism (OAS-CICTE) has been able to support the implementation of at least one of the cyber norms by improving or implementing new Computer Security Incident Response Teams (CSIRTS) throughout the Americas.

Finally, on gender, over the last year alone, the OAS Cyberwomen Challenges trained over 500 women in cybersecurity, while also implementing relevant gender events to promote the role of women in cyber. These included online networking events and a webinar on cybersecurity and countering online gender-based violence.

Canada is also a donor and supporter of the Women in Cyber Fellowship.

We welcome the interventions from Argentina & Chile, whose representatives are here with the Fellowship. Chair I would also request that the Secretariat take note, when looking at the recordings, of how many interventions were made by women.
It would be good to build on the success of the last OEWG when we achieved gender parity. Canada continues to support the meaningful participation of women in these cyber negotiations.

On the point of the OEWG improving engagement and working with organizations to optimise global capacity-building efforts

Canada would suggest that the OEWG canvass members to see what capacity building is already underway and what developing countries might need before deciding on this. The OAS has already been doing substantial national cyber security strategy development. The ASEAN-Singapore Cyber Center of Excellence is also developing programming that would overlap with some of this work.

Together also with partners from non-government organizations (NGOs), the tech community and academia, stakeholders are an able and critical part to develop practical initiatives to build cyber capacity. The Global Forum for Cyber Expertise (GFCE) has also made significant progress since its establishment to increase participation and provide all participants with the tools, knowledge and expertise required to coordinate global efforts in cyber capacity building.

With regard to the useful lessons the OEWG can draw from these existing mechanisms

The OEWG should take advantage of existing cyber capacity building coordination bodies such as the GFCE, in order to maintain coordination and coherence as it relates to cyber capacity building efforts.
The GFCE regularly produces roadmaps and publications on how to improve cyber capacity building efforts and develop Confidence Building Measures and standards.

The combination of regional organizations, working in tandem with States, while also supported by the non-governmental multi-stakeholder community, can ensure the most effective capacity building projects possible.

Lastly Chair, we have heard how this process itself is considered a capacity building exercise. But in order for it to be truly effective, there needs to be a degree of trust among States. It is therefore incumbent of us, to speak out against the unprovoked and unjustifiable devastation that Russia’s military forces are causing in Ukraine. President Putin’s war of choice threatens Ukraine and Europe’s security, but also international peace and security, the rules-based international order, and the normative framework for responsible State behaviour in cyberspace.

Canada would like to remind all states of their obligations under the UN Charter and other normative and legal commitments made in previous UN cyber processes. In perhaps the most pertinent example I could give on capacity building, I would humbly suggest the following. We would invite the delegation of Ukraine, to present to the entirety of the OEWG, their exemplary efforts in cyber resiliency and bolstering their defences.

The January 15 malware targeting systems belonging to Ukrainian government agencies, and other malicious activities that have occurred in past years, should be indicative to all, that the need to strengthen and implement commitments to norms, confidence and capacity building measures, is greater than ever. What Russia has done cannot be normalized.
In conclusion Chair, Canada reaffirms, the importance on the respect of the framework for responsible State behaviour in cyberspace. A framework which we have all worked to build together these last 12 years. Which has since been undermined by Russian cyber operations, including most recently in Ukraine.

We stand with the government of Ukraine and its brave and resilient people as they defend their country. Thank you Chair.