Chair,

First, I’d like to congratulate Ambassador Lauber for his election as Chair. Cyberspace has brought many advantages to our societies, our economies and our daily lives. But it also brings new risks. We regularly see headlines about hackers, interference in democratic processes and other malicious or illegal cyber activity carried out by governments or their proxies. These put our collective security and prosperity at risk and increase mistrust, instability and the odds of conflict.

Canada welcomes the opportunity provided by this Open-Ended Working Group (OEWG) to examine threats to peace and security emanating from ICTs and explore how international cooperation can help preserve a free, open, stable and secure cyberspace, where human rights are respected online just as they are offline. I would like to share with you Canada’s perspectives on how this OEWG can best fulfill its mandate.

First, and most importantly, this Working Group must build on the important body of work that the international community has already agreed, particularly the consensus reports of the UN Group of Governmental Experts (GGE) on ICTs.
The 2013 and 2015 reports of the GGE recognised the applicability of international law to cyberspace. Greater understanding of international law will help ensure our shared security and stability in cyberspace. The GGE also agreed on voluntary, non-binding norms of responsible State behaviour aimed at reducing risks to international peace and security emanating from cyberspace. All UN Member States agreed to be guided in their use of ICTs by the 2015 GGE report in UN General Assembly resolution 70/237. This agreed framework for responsible state behaviour in cyberspace is the foundation upon which the OEWG’s work must be built.

Our major challenge remains the broad dissemination and implementation of these agreed norms by all Member States. That is why Canada believes that the OEWG should develop concrete and practical guidance on norm implementation. This Group can help explain what the norms mean in practice, and provide concrete assistance for States and regional organisations on implementation.

Monsieur le Président,

Les précédents rapports du Groupe d’Experts Gouvernementaux ont également détaillé les mesures de confiance que les États devraient mettre en place pour limiter les risques de malentendu, d’escalade ou de conflit dans le cyberspace. Là encore, la mise en œuvre des mesures existantes reste notre principal défi.

Le Canada espère que le Groupe de travail mettra l’accent sur des mesures concrètes visant à promouvoir la mise en œuvre par les États membres des mesures de confiance adoptées dans les deux derniers rapports du Groupe d’Experts Gouvernementaux.
Nous ne pouvons évoquer la mise en œuvre des normes et mesures de confiances existantes sans évoquer la question des ressources et outils nécessaires pour le faire. De nombreux États membres n’ont pas les capacités optimales pour mettre en œuvre les engagements existants et ainsi profiter pleinement des opportunités que le cyberespace pourrait apporter à leur sociétés et économies.

Pour le Canada, ce Groupe de travail a un rôle important à jouer pour mobiliser la communauté internationale, prioriser les besoins et favoriser l’accès des États membres aux ressources et capacités nécessaires pour mettre en œuvre les recommandations des rapports du Groupe d’experts gouvernementaux.

Le Canada est prêt à faire sa part. Au cours des deux dernières années, le Canada a contribué plus de 12 millions de dollars pour appuyer le renforcement des capacités de certains États membres en matière de cybersécurité.

Plus récemment, le Canada s’est associé à l’Organisation des États Américains ainsi qu’à l’Organisation internationale de la Francophonie pour tenir des ateliers de concertation et de renforcement des capacités avec les représentants des États membres de ces deux organisations à New York sur les enjeux qui seront traités par ce groupe de travail.

Chair,

UNGA resolution 73/27 created this Open-Ended Working Group to make UN work in this field more inclusive and transparent.

For this Group to be truly inclusive, it must allow for the participation of a wide variety of actors and voices with a stake in international cybersecurity issues.
Civil society, NGOs, women’s groups, human rights organizations, academics, industry groups, and the private sector should be included in this process and their input should be reflected in this Working Group’s report.

We are pleased that consultations with non-governmental stakeholders will take place in December. We regret, however, that only ECOSOC accredited organisations were allowed to formally participate in this week’s meeting. Several important voices will not be heard. We hope that a solution is found to allow their participation and contributions in future meetings. The credibility of this process will depend on its inclusivity.

We also believe that the OEWG should address an often overlooked but important issue: the gender dimensions of cybersecurity. We know that women are uniquely and differentially affected by threats to international peace and security and by technology.

This Working Group should pay particular attention to placing gender equality and the meaningful participation of women at the centre of its efforts. It should explore how to increase active engagement of women in discussions, negotiations, strategies and capacity-building programs on ICTs and international security, at the UN and elsewhere. It should also address the links between ICTs and the UN Women, Peace and Security agenda

In closing, you can count on Canada’s active engagement in the OEWG process. We will submit a national paper providing detail on our positions. We look forward to working with all Member States and other relevant stakeholders to constructively advance international cooperation for peace and security in cyberspace.

Thank you. Merci.