Chair,

I am pleased to make this statement on behalf of Australia, Chile, Estonia, Japan, the Netherlands, New Zealand, the Republic of Korea, the United Kingdom and my own country, Canada.

Cyberspace is a source of enormous economic, political and social benefits for all persons and States; when it is accessible, open, interoperable, reliable, and secure, and when it is not used in ways that restrict human rights and freedoms or the free flow of information. We all have a shared responsibility and mutual interest in improving our collective cyber security to achieve these benefits.

We are committed to promoting stability in cyberspace based on the application of existing international law, as well as agreed voluntary norms of responsible state behaviour and confidence-building measures supported by coordinated and targeted capacity-building programmes.

Yet, malicious cyber acts, particularly those undertaken by States, are increasing in number and severity.

Despite the international legal framework governing State behaviour in cyberspace, many States, either directly or through proxies and non-State actors, undertake malicious cyber activity directed at the essential systems, infrastructure and democratic processes of other States. Such behaviour threatens international peace and security, undermines the rules-based international order on which we all rely for our security, and imperils the benefits that arise from the development of cyberspace.

Civil society actors, human rights defenders and ordinary citizens are also being targeted by these same and other States in an effort to silence opposition and stifle criticism.

States undertaking these acts do so with flagrant disdain for their obligations, for norms of appropriate behaviour and with reckless disregard for the consequences.

Chair,

Cyberspace is not a lawless realm. Nor is it ungoverned as some would have us believe.

International law applies to the actions of States in cyberspace as it applies in other realms of State behaviour. All States have responsibilities and obligations online, just as they do offline.

This is not just our position. It is an international consensus that has been validated by the United Nations Group of Governmental Experts, or GGE, in the Field of Information and Telecommunications in the Context of International Security in 2013 and endorsed by the General Assembly in 2015.
In addition, the consecutive GGEs in 2013 and 2015 produced a number of consensus-based norms for State behaviour in cyberspace, which are being used as the basis for further cooperation around the globe. Cyber security confidence-building measures have also been developed by several regional organisations and have led to greater predictability and stability in cyberspace.

This consensus is the obvious starting point for any new initiative. We need to build on, not undermine, what we have already achieved, along with experts provided from a broad range of states, and the endorsement of the General Assembly.

We call on all those who are committed to the security and stability of cyberspace to continue to support efforts, at the UN and elsewhere, to promote the applicability of existing international law to States’ cyber activities.

It is essential that we continue the work done by previous GGEs to further strengthen and deepen this consensus. In order to make progress, we have to find a way to strengthen an inter-sessional consultative mechanism to allow all UN member States to engage in the process. Appropriate ways to consult other stakeholders should also be explored.

It is also essential that the GGE process find the right balance between being transparent and inclusive while remaining nimble enough to deliver a consensus outcome in a reasonable time frame. It should be expert-led, operate on the basis of consensus and focus on the critical issue at hand, namely the risks to international security arising from State behaviour in cyberspace.

Chair,

Each and every one of us must do our part to address threats to international peace and security in cyberspace.

We must deepen our commitment to the applicability of international law, implement the already agreed voluntary norms of responsible State behavior in cyberspace during peacetime, and reinforce our collective commitment to conflict prevention and the peaceful settlement of disputes. Examples of governments publicly setting out their views on how international law applies in cyberspace are to be welcomed.

We must continue to develop and implement confidence-building measures to limit the risk of conflict due to misunderstanding or miscalculation. We welcome the progress achieved in that regard within the OAS, the OSCE and in the ASEAN Regional Forum.

We must also increase international cooperation on cyber security and enhance capacity-building efforts to strengthen the ability of all States to secure their infrastructure and build their resilience against cyber threats.
At the same time, we emphasize that cyber threats should not be used to legitimize Internet controls that would restrict human rights and freedoms or hinder the free flow of information. Human rights and security are mutually reinforcing online, just as they are offline.

Chair,

The risks to international peace and security posed by threats to cyberspace are serious and far-reaching. We need to take a collective, global approach in responding to them. Consensus within the First Committee on the creation of a single, new GGE on cyber security, which would include time for consultation with all States and stakeholders, would be a tangible contribution to this collective effort.

Thank you.