Austria fully aligns itself with the Statement delivered by the European Union. In our national capacity we wish to add the following.

Cybersecurity has become a buzzword, but its real life implications for global peace and security go to the core of the mission of the United Nations.

Austria welcomes the very constructive and interactive debates during the Open Ended Working Group on Cybersecurity in September, expertly chaired by Amb. Lauber whose approach we fully support. We welcome the emerging consensus on UNGGE reports as the basis for our work as well as on the application of existing international law and the UN Charter in its entirety in cyberspace. Human rights, fundamental freedoms and IHL are a central part of this package.

We welcome the multi-stakeholder event in early December but also strongly favour a much broader involvement of all stakeholders during the sessions of the OEWG. Coherence and consistency are essential between the parallel tracks of the Open ended working group and the UNGGE.

The widespread concern on threats from cybercrime was notable during the OEWG. Although strictly speaking not on the agenda, we need to find a link to the excellent work done in Vienna by UNODC and the open-ended intergovernmental expert group on cybercrime without duplicating it. We will therefore support UNODC presenting its work on
helping countries set up effective structures to fight cybercrime at the upcoming session of the OEWG.

Practical steps are also what is most needed to move forward in a situation where trust is thin on the ground, concretely:

- **Confidence Building Measures** - like those established at the OSCE, and now also at OAS and ARF, should be considered in all regions and connected at the global level. By offering transparency and predictability these measures also strengthen the expectation that international law will be adhered to.

- Previous UN GGEs have done valuable work on rules, norms and principles of responsible state behaviour. We now need to build a common understanding on this basis, breaking down how the implementation can best be achieved in each individual state, comparing best practice models, for instance on safeguarding critical infrastructure, which is a key problem facing all states. In other areas of discussion at the UN, where guidance is needed on how existing norms apply in new circumstances, **guiding principles** have proven very helpful. Guiding principles could also be considered in the context of cybersecurity.

- Capacity building is central to safeguarding cybersecurity. The EU and its member States strongly support a range of programmes to assist countries with capacity-building and best practice exchanges.

Cybersecurity has become a global public good that needs to be strengthened, for all of us to enjoy the benefits of an open, stable and secure cyberspace. Fighting malicious cyber activities that cause great damage on targets and unintended victims alike, must not serve as a pretext for tightening control over citizens/users and thereby undermining basic human rights such as the right to privacy and the freedom of expression.