Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG)
Second substantive session 28 March – 1 April 2022

“National intervention under agenda item 5: Discussions on substantive issues”

Statement by
Kingdom of the Netherlands

NEW YORK, 1 April 2022
Thank you very much Chair,

My delegation aligns itself with the statement of the European Union and we would like to make additional remarks in our national capacity.

1. Before the Netherlands answers explicitly your questions on Regular Institutional Dialogue, I would like to address a specific point that had been raised throughout the week.

2. Chair, we noted with great interest all the suggestions for UNIDIR to undertake additional research and activities. The Netherlands supports many of these requests. Keeping in mind that UNIDIR is an independent research institute within the UN, which relies on voluntary funding to conduct its activities.

3. We would now like to answer your question on the last agenda item. And to finish on a positive note and reflect on a future institutional framework under the auspices of the United Nations to promote an open, free and secure cyberspace.

4. As stated in the report of the previous OEWG that has been endorsed by us all, any future mechanism for regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based.

5. The Netherlands believes that those should be our guiding principles for any discussion on a Regular Institutional Dialogue. For the Netherlands, this means the main focus should be to look at what is required to follow the ones we all already agreed to.

6. I would like to take a moment to emphasize the inclusiveness of such a process.

   - Of course, it should allow for all UN Member States to participate.
   - While being an intergovernmental process, it should include meaningful engagement with the multi-stakeholder community. Given the unique character of cyberspace, they have a role to play as owners of the infrastructure, the technical expertise and as users. Whether it’s about securing supply chains, mitigating cyber incidents or enhancing resilience – States are just one category of stakeholders – we cannot do it alone.
7. An open, free and secure cyberspace can only be achieved if we work **collectively**; collectively as states by abiding by the UN framework we all agreed upon, and collectively as a society by engaging the private sector, the technical community, civil society. Because international peace and security relies on the commitment of all parties involved in securing the digital world our societies rely upon.

8. It is time to be **action-oriented** and start the implementation of the agreed normative framework. We should not waste time, it is time to act.

9. A regular institutional dialogue should be a place to 1) monitor and share best practices and expertise; 2) support national **implementation of the normative framework**; 3) look at how to concretely address new challenges; and 4) provide concrete back-up for capacity building projects.

10. The **Programme of Action** has all the potential to provide the perfect venue for such a regular institutional dialogue. We hope that the progress report will reflect those points and that we can all agree upon the creation of such a platform as soon as possible.