**[check against delivery]**


**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, 31 March 2022**

**OEWG March - Capacity-Building**
**Thursday 31 March**

Thank you, Chair.

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

1. Cyber capacity building is of vital importance to global digital development and the attainment of the **Sustainable Development Goals**.
2. States should cooperate to enhance global cyber resilience. This can range from technical steps – like ensuring that all States have a national CERT – to supporting the development of national cyber policies and strategies.
3. In undertaking these efforts, it is of utmost importance that all actors adhere to the principles for capacity building laid out in the previous OEWG report.
4. One such principle is that capacity-building should be demand driven. In this regard, I would like to highlight several complementary tools that can help States identify their needs and priorities in different areas. These include the Cybil Portal of the Global Forum on Cyber Expertise; UNIDIR's National Survey of implementation; and the Capacity Maturity Model developed by the Oxford Global Cybersecurity Capacity Building Centre.

Chair,

5. On Monday, the High Representative, Ms. Nakamitsu, highlighted the need for a permanent platform to support capacity-building and the implementation of the existing normative framework.
6. We believe such a platform could complement the OEWG's work to further develop common understandings and elaborate the consensus framework for responsible State behavior.
7. The Netherlands believes that the **Programme of Action** may act as such an implementation body. It could facilitate the sharing of expertise, best practices and capacity building, to allow states to effectively implement the framework. It can also facilitate other mechanisms as shared earlier by France and Egypt.
8. Multi-stakeholder organizations can make a valuable contribution to the PoA. And here I would like to highlight the work of the **Global Forum on Cyber Expertise**, which helps match capacity building needs with expertise and resources.
9. Finally, Chair, we believe that the OEWG should further promote a **gender-sensitive approach** to cyber capacity building as was also suggested by Canada. This also applies to the area of cyber diplomacy, where we seek to increase the representation of women in our discussions through the Women in Cyber Fellowship program.

Thank you, Chair.