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 – Confidence-Building Measures
Thursday 31 March

Thank you, 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. Under the current circumstances, the international community faces an unprecedented risks of misinterpretation, miscalculation and escalation of cyber incidents. As one key element of the framework for responsible State behavior in cyberspace, confidence-building measures are an essential tool in mitigating these risks.

2. In an effort to step up global CBM cooperation, the Netherlands joined an open, cross-regional group to advance cyber confidence-building measures in the OEWG. It is our hope that this informal group can put forward practical ideas that bring the CBMs to life.

3. An important first step would be to establish a global network of Points of Contacts at the policy, diplomatic and technical levels. In addition, States may consider to establish or identify appropriate points of contacts within the private sector.

4. A global network of points of contacts should be more than an Excel sheet. For it to have practical value, the network should work on the basis of clear procedures to ensure effective exchanges, and conduct regular communication checks and exercises.

Chair,

5. You asked us in your guiding questions how the OEWG may facilitate cross-regional exchange of ideas. Regional organizations are well-placed to develop effective CBMs by tailoring them to their specific contexts and priorities. As we have heard in different interventions, several regional organizations have done so successfully, and managed to go beyond the global CBMs developed at the UN level. We believe cross-regional sharing of experiences and best practices can be helpful for regions to develop new CBMs or advance the implementation of existing ones.

6. Allow us to share our experience regarding a CBM agreed within the OSCE on Coordinated Vulnerability Disclosures. We identified that an important first step in promoting regional cooperation among States was to develop national Coordinated Vulnerability Disclosure policies. Such policies can lead to the establishment of mechanisms by which vulnerabilities can be disclosed in a controlled manner, allowing for faster remediation and enhanced security. The Netherlands has published its Policy online, and would be happy to share it with the group.
7. Finally, Chair, it should be emphasized that these practical steps by themselves will not be enough to prevent conflict in cyberspace. We continue to encourage all States to publicly reiterate their commitment to – and act in accordance with – the framework for responsible State behavior developed by consensus. Because, we believe, that is ultimately the prerequisite for confidence-building.

Thank you.