Comments by the Norwegian Delegation on the "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

The Norwegian delegation commends the Chair on his capable steering of the OEWG process, and the Secretariat for facilitating and supporting this work.

Having reviewed the letter from the Chair and the accompanying pre-draft report, circulated on 11 March 2020, we hereby present some initial comments on the current draft, ahead of the next meeting of the OEWG.

General:

- We understand the consensus to be that the 2010, 2013 and 2015 GGE reports form the *acquis* for the discussions. The previous GGE reports provide a framework for responsible State behaviour in cyberspace, and there is an agreement that adherence to this framework should be observed. We believe that this agreement is of fundamental importance, and should be clearly expressed as a central premise of the final report.

- The pre-draft gives a comprehensive view of many of the topics discussed and the positions presented in previous meetings. However, the pre-draft does not presently distinguish between areas of consensus and minority views. One example of the latter is the proposal for a new legally binding instrument, to which there are broad reservations from a large number of Member States. To strengthen the areas of agreement and mutual understanding, these should be clearly distinguished from the areas of current non-agreement. We would encourage referring to "some states" rather than "states" where consensus is not established.

Existing and Potential Threats:

- The rapid evolvement of digital technologies creates new challenges and vulnerabilities. This requires the international community to cooperate and establish shared understandings, in order to avoid misuse and potential negative consequences. We should focus on the effects and the security implications emanating from the *use* of ICTs, rather than on the specificities of ICTs in and of themselves. The language in the report should consistently reflect that the subject of study is the responsible behaviour of States.

- We should avoid the use of terms such as "militarization", as its significance can be unclear or potentially politicized. Our aim should rather be to give a factual and concrete description of the threat landscape, as it pertains to state-to-state behaviour in the context of international security.

International Law:

- Our mandate states that we "should continue to study, with a view to promoting common understandings, […] how international law applies to the use of information and communications technologies by States". While international law has its roots in a time preceding the evolvement of cyberspace, there is nothing new or unique in applying the rules of international law to new areas, following new technological developments. The existing framework of international law must be interpreted in the usual way. Exchanging

views on how international law applies (*opinio juris*) is a key contribution of the OEWG, and in itself also an important CBM.

Rules, Norms and Principles for Responsible State Behaviour:

- Our impression is that there is broad agreement about the importance of strengthening the implementation of the 11 agreed norms. At the same time, there are more diverging views on whether new norms are currently needed and should be developed. We believe this should inform our priorities in the time ahead, by concentrating our efforts on the operationalization of the existing norms, by providing additional guidance on implementation.

- It is important to maintain the distinction between voluntary, non-legally binding norms, and international law, which is binding upon states.

- To avoid any confusion we would prefer this section to be titled in accordance with the 2013 and 2015 GGE reports, with the word order being "Norms, rules and principles". We recommend that this wording is used consistently throughout the report.

Capacity-building:

- We support proposals to recognize and integrate the link between capacity building and the UN Sustainable Development Goals. We would also support the recognition of the principles laid out in the 2017 Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building.

- We welcome the recognition of the "gender digital divide" and the need to strengthen the link to the Women, Peace and Security agenda. Inclusivity and diversity should be a guiding principle for the capacity-building agenda.

Regular Institutional Dialogue:

- A continuation of the institutional dialogue must not in any way impede ongoing processes. Decisions on the nature of any future processes must be based on the recommendations of the current OEWG and GGE, and not pre-empt any conclusions of either process.

Conclusions and Recommendations:

- We welcome the proposal, echoed in several recommendations, for the establishment of a global repository, containing information about States' implementation of the agreed framework for responsible State behaviour. A comprehensive, unified repository should be established to prevent fragmentation of information and duplication of efforts. The repository could include information on states' a) National Laws and Policies for the protection of data and ICT-enabled infrastructure; b) National Points of Contact at the policy and technical level to address serious ICT incidents; c) National efforts to implement the agreed norms rules and principles; d) National efforts to implement confidence-building measures following existing recommendations and agreements, on a bilateral, sub-regional, regional and multilateral basis; and e) Capacity-building priorities, programs and partnerships.

The Norwegian delegation welcomes this opportunity to comment on the pre-draft of the OEWG report. The above comments are preliminary and should not be considered exhaustive. Once again,

we wish to praise the Chair and the Secretariat for the efforts in facilitating this process, and look forward to continuing the dialog.