Pakistan’s inputs in response to the letter dated 11 March 2020 from the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)

Pakistan appreciates the Chair’s efforts in steering this historic process in an efficient and transparent manner. We reiterate our full support to ensure that this process produces substantive outcomes, including practical and concrete recommendations on the way forward.

2. We also commend the efforts of the United Nations Office for Disarmament Affairs (UNODA) and the United Nations Institute for Disarmament Research (UNIDIR) in supporting this important process.

3. The active participation by Member States and the strong engagement by the relevant stakeholders including non-governmental organizations, the private sector, and the academia, provided an excellent opportunity for advancing UN efforts on promoting common understandings on this subject.

4. Pakistan welcomes the pre-draft as a good basis for discussions leading to the next substantive session of the OEWG and for a final report that contains a meaningful outcome in line with the OEWG’s mandate.

5. In this context, the following preliminary remarks and observations are offered:

**General remarks**

6. The pre-draft manages to capture the discussions held so far in a reasonably balanced and comprehensive manner.

7. Many delegations, including Pakistan, had emphasized the need for operationalizing the existing rules and norms previously endorsed by the UN General Assembly, through elaborating them and making them more binding for all States. These delegations also expressed willingness to agree on new rules and norms and highlighted the need for recommending the consideration of a binding instrument that regulates the behaviour of States in their use of ICTs.

**Descriptive part**

8. The narrative introduction and the descriptive part (sections A to G) take into account the discussions held so far, the inputs provided by Member States, as well as points of convergence and divergence on various issues of significance in an accurate manner.

**Recommendations part**

9. Pakistan is of the view that adoption of binding commitments for responsible State behaviour in relation to the use of ICTs, at least those based on the norms of responsible State behaviour contained in the 2015 GGE report, would have represented a good outcome. Nevertheless, the recommendations contained in the pre-draft, represent a meaningful step in advancing international efforts towards increasing stability and security in the global ICT environment.

10. Additional recommendations for consideration of the OEWG are provided below:

11. **International Law:** Member States should be encouraged to continue to consider how international law applies to State use of ICTs in the context of international security, with a view to identifying possible gaps that need to be addressed through development of further rules that take into account the unique attributes of the ICT environment.
i. **Rules, norms and principles**

a. Member States should be encouraged to continue to consider, as appropriate, the possible adoption of a legally and/or politically binding instrument(s) in order to regulate specific aspects of State use of ICTs in the context of international security.

b. Member States should be encouraged to arrive at an agreed common definition of what constitutes “critical infrastructure”, with a view to agreeing on the prohibition of ICT activity that knowingly or intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure.

c. Member States should be encouraged to cooperate to reach agreement on prohibiting the creation of harmful hidden functions or accumulation of vulnerabilities in ICT products, as well as to commit to responsible and timely reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities.

d. Member States should seek to facilitate cooperation with ICT products and services providers to prevent the exploitation or abuse of users’ data and privacy.

e. Member States should commit not to use ICTs for carrying out activities which run contrary to the maintenance of international peace and security, and refrain from using ICTs to interfere in the internal affairs of other States in any manner.

f. Member States should cooperate to address the challenges associated with attribution in the ICT environment. Developing a common approach to attribution in a universal setting under the UN auspices remains the most effective way forward in this regard.

g. Member States must be urged to arrive at an agreement on prohibiting ICT activity intended to disrupt the technical infrastructure essential to elections or referendums or plebiscites.

h. Member States should be encouraged to develop and implement norms in a manner that avoids undue restrictions on the peaceful uses of ICTs, international cooperation in this field or technology transfer.

12. **Capacity building**: the principles of capacity building should include the following:

i. Capacity-building should be demand-driven, made upon request by the recipient State, taking into account the specific needs and contexts of Member States, and have sustainable impacts.

ii. Mindful of the inter-linkage between confidence-building and capacity-building, Member States should ensure that ICT related capacity-building is seen as a trust-building measure, and that it remains transparent, accountable, non-discriminatory and politically neutral, with the objective of bridging inequalities caused by the digital divide.

iii. Efforts should be made to fully protect the confidentiality of information related to the recipient State’s policies and measures to protect its national infrastructures and the confidentiality of its ICT emergency response plans.

iv. The principle of “common but differentiated responsibilities” should be applied with regard to the provision of capacity building.

13. **Confidence building measures**: Member States should be encouraged to promote cooperation, including through respective computer emergency response teams, in addressing requests to investigate ICT-related incidents or to mitigate malicious ICT activity emanating from their territory, while taking into account the possible limitations on the technical capacities of developing countries to address such requests.

14. **Regular Institutional Dialogue**: Member States should be urged to continue promoting common understandings on the establishment of a specialized institutional forum, under the UN auspices, on the international security dimension of ICTs.