Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

Comments by ARGENTINA

Argentina considers extremely important the existence of inclusive spaces such as this Open Ended Working Group in which countries from all regions and diversity of visions can engage actively with the aim of building consensus regarding the rules, norms and principles of responsible state behaviour and the way international law applies in cyberspace. At the same time, it is necessary to recognise the important contribution done so far by the GGE.

It is important to acknowledge that discussions both in the GGE and in this OEWG do not start from scratch. Well to the contrary, there is a valuable acquis of voluntary norms, rules and principles that have been accepted by consensus by all members of UN General Assembly to guide State´s use of ICT and responsible state behaviour in cyberspace. This is a starting point and a basis that we should preserve and continue to work upon so that it can become more operative.

As mandated by its National Cybersecurity Strategy, Argentina promotes the peaceful use of cyberspace and supports all initiatives aimed at the establishment of values such as Justice, respect for International Law, equilibrium and the narrowing of the digital gap among States, while encouraging dialogue and cooperation. Respect for Human Rights and individual freedoms enshrined in Argentina´s Constitution as well as in International Treaties are fundamental principles for the protection of individuals in cybersecurity.

In the context of continuous innovations in ICT and increasing use of emerging technologies such as Internet of Things and Artificial Intelligence, among others, it´s necessary to actively work so that the benefits of these technologies can be enjoyed by all nations with fairness and equilibrium.

1. **General comments on the document**

1.1. It is important to point out that the OEWG has proven a very positive exercise so far, providing an inclusive and transparent space in which all states are able to participate, as well as recognising the added value of a multistakeholder approach.

1.2. From our point of view, most of the discussions and ideas shared during the first two substantive sessions of the OEWG are properly reflected in the document, in particular in sections A- G

1.3. In this sense, we consider the document to be a balanced and good base for the future OEWG report.

1.4. We believe that as an initial pre draft report of this OEWG, that includes a multistakeholder approach, the document reflects some minimum consensus upon which it is expected to acquire more specific recommendations during future discussions.

1.5. Within this framework, it is deemed important to move forward, in particular**,** in the following aspects that would contribute in a significant manner to keep an open, secure, resilient and peaceful cyberspace:

- Broad support on initiatives designated to narrow the digital gap;

- Broad understanding on the application of international law in cyberspace;
- Greater understanding on the technical capacities for attribution of responsibility for cyberattacks;
- Achieve consensus with regard to the institutionalisation of a regular dialogue in the framework of OEWG and GGE.

2. **Specific comments on the different sections of the document**

Section A “Introduction”:

- Para. 9: We particularly support the recognition that narrowing the digital gap is an urgent priority for the international community and that should be mainstreamed through the all the chapters of the group´s agenda.

- Para. 13: This paragraph states that sections B-G “reflect the substantive discussions of the OEWG and its recommendations”. Hence, it would be important to clarify the scope of section H and distinguish which of the paragraphs from section B-G are descriptive and which are prescriptive or contain recommendations.

Section B “Real and potential Threats”:

- Para. 16: We strongly support the notion that the lack of capacity is a threat in itself.

Section C “International Law”:

- Para. 20: We share the emphasis on the notion that solutions will be more effective and long-lasting if they are inclusive and all the actors of the international community contribute to them.
- Para. 27: We consider that for clarity it would be better to divide this paragraph into two independent paragraphs. This is due to the fact that as it stands now it refers to a variety of questions related to the application of international law that deserve a differentiated treatment. It is proposed that a first paragraph refers to the clarifications that are needed as regards to what kind of ICT-related activity might be interpreted by other States as a threat or use of force (Art. 2(4) of the Charter) or might give a State cause to invoke its inherent right to self-defence (Art. 51 of the Charter). It is also understood that these are the questions that should be addressed with prudence.

  A second and separate paragraph should refer to the additional clarifications that may be required on the application of Humanitarian International Law principles to cyberoperations in the context of armed conflicts.
- Para 32: We strongly support the notion that it is necessary to work towards developing common approaches regarding attribution at a technical level, which would contribute to transparency, accountability and responsible behaviour, enhance deterrence and could provide grounds for legal action by victims of malicious cyber activities.

- Para. 33: We fully agree that it´s crucial to promote capacity building on how international law applies in cyberspace, with the aim that all states can develop their own understandings on this matter, participate actively in discussions and contribute to building consensus within the international community.

Section E “Confidence Building Measures”:

- Argentina shares the view that the existence of this OEWG is a confidence building measure at a global scale.

Section F “Capacity Building”:

- Para. 55: It would be important to include a recognition of the efforts and important initiatives developed by regional organisations to promote capacity building, enhance consensus, strengthen confidence building measures, as well as the positive results of their work.
- Para. 56: We strongly support the acknowledgement of the need for specific measures to address the digital gender gap and promote the meaningful participation of women in international discussions on cybersecurity and in capacity building programs on ICTs and international security.

Section H “Conclusions and Recommendations”:

- Para. c) on confidence building measures: We support the recommendation to establish a Global Registry of National Points of Contacts and believe that Ministries of Foreign Affairs should play an important role in it.
- Para. d) on capacity building:
  - ♣ It is proposed that the following principles be included in order to guide the capacity building efforts: inclusiveness; political neutral approach; evidence based, with adequate metrics to measure results; avoid duplication; work in cooperation with the private sector and civil society; promote ownership; promote learning processes for all the actors involved; be demand driven; be gender-sensitive.
  - ♣ We believe that instead of creating a new mechanism for capacity building, the General Secretary could take into account all the existing platforms and mechanisms, such as the GFCE, in order to articulate them and facilitate the coherence among them.
- Para e) on “regular institutional dialogue”: It would be appropriate to recommend that the 75° UNGA (not the 76° UNGA) extend the mandate of the OEWG, as the UNGA Res 73/27 that created the OEWG foresaw its work would conclude on July 2020. By the same token, at this point it seems premature to include a recommendation that the 76 UNGA creates a new GGE, since the current GGE has more than a year ahead to continue its work and its report is due to be presented during 76° UNGA.