Statement by

Mr. Upender Singh Rawat

Joint Secretary (EG & IT) (Cyber Diplomacy)

Ministry of External Affairs

Open-ended Working Group

on

Developments in the field of Information and Telecommunications in the context of international security

09th September 2019

Mr Chairman:

We congratulate you on being elected to Chair the OEWG.

2. India hopes that OEWG will contribute to the cyber norms development process with a view to promoting common understanding among UN member States on the existing and potential cyber threats; practical cooperative measures to address them and how international law applies to ICT domain, including developing a consensus on attribution of cyberattacks; legality of use of countermeasures; as well as norms, rules and principles of responsible behavior of States, confidence building measures and capacity building.

3. OEWG and GGE will be functioning parallel to each other. Both the processes are complementary to each other having their own advantages. Despite the creation of these two groups, there are challenges in reaching consensus on finalizing non-legally binding and voluntary norms of responsible State behavior in cyberspace.

Mr. Chairman:

4. The mandate of OEWG is to “further develop” the rules, norms and principles of responsible behavior of States and the ways to implement them, if necessary, to introduce changes, whereas the GGE mandate is to continue to study the existing issues leveraging and consolidating the gains already attained. India, is of the view that while sticking to the mandate of OEWG, we need to be open, prudent and flexible to consider issues of both the Groups with a view to work upon common minimum denominator to develop consensus on the contentious issues to improve the quality of the outcome of the discussions.

5. The impact of cybercrime and cyber terrorism on national, regional and international peace and security need to be considered as international cooperation on them will facilitate building trust and confidence among member States, thereby contributing to international peace and security.

Mr. Chairman:

6. The collaborative efforts to deal with cybercrime and cyber terrorism should be seriously taken up and real time cooperation between Government agencies should be developed to tackle this menace. Further, the issue of cyber warfare, cyber doctrines and their impact on international security should be taken up at all relevant international fora.

7. It is of concern that cases of malicious use of new ICTs to the detriment of States are increasing and there is a need to express strong condemnation and rejection of these violations.

8. Keeping in mind the existing and potential threats in the use of ICTs to the international peace and security, it is important that the States should not knowingly allow their territory to be used for committing internationally wrongful acts using ICTs including cross border cybercrime and cyber terrorism.

9. The applicability of International law to the ICT domain and the cybersecurity -related laws, policies and practices at national, regional and international levels should be developed through open, inclusive, transparent and non-discriminatory approaches that involve all stakeholders. Stakeholders should promote education, digital literacy and technical and legal training as a means to improving cybersecurity as well as bridging the emerging digital divide.

10. We feel that the norms, rules and principles elaborated by the 3rd and 4th UNGGE are a considerable advancement aimed at promoting an open, secure, accessible and peaceful ICT environment. The 11 norms elaborated upon by the 4th UNGGE are broad enough to cover a wide landscape. However with the evolving threat landscape and emergence of new ICTs, there is a need for additional norms including the norms to avoid tampering of supply chain, condemn offensive cyber operations by malicious actors and take down ICT infrastructure being used for botnets.

11. Capacity building is an important aspect of OEWG discussion as it promotes adherence among States to cyber norms as well as CBMs especially for developing countries, which lack the requisite cyber structures, policy, cyber law and cyber capabilities. It is mutually beneficial for both developed and developing countries in addressing cyber threats to ensuring national, regional and international peace and security. Hence, these measures should not be seen from the construct of donor-recipient lens. Improving capacities and strengthening national cyber security capability is equally in the interest of UN member States, including countries which have advanced

capabilities given the interconnected nature of the domain. CBMs include developing mechanisms for practical cooperation between cyber agencies, including CERTs, promoting bilateral cyber dialogues, cyber capacity building, exchange of information on cyber threats, cyber policy, structure and law enforcement, cooperation on cybercrime and cyber terrorism and mechanisms for protection on information infrastructure.

12. In summary, we believe that as a responsible group of experts, it is our duty for future of our digital society for : (a) Developing a consensus on definitions of cyber sovereignty, jurisdiction in ICT domain, data sovereignty, cyber weapon, cyber conflict, cybercrime and cyber terrorism, cyber deterrence, cyberattacks, etc. (b) The measures of countering terrorism in the use of ICTs. (c) Universalisation and operationalisation of the OEWG reports in letter and spirit.

Thank you Chairman.