INDIA's comments
on the Initial Pre-Draft of the report of the
OEWG on developments in the field of information and telecommunications
in the context of international security

India submits that the Chair's initial pre-draft attempts to capture the essence of the discussions held during the two sessions of the OEWG in New York, by giving due consideration to the deliberations and inputs put forth by all the member states. While India commends the work of the Chair on preparing the initial pre-draft, it also observes that reflections proposed by member states are not captured in some topics of the pre-draft. Some areas of the pre-draft also need a closer look.

Keeping in mind the discussions at the two OEWG Sessions, India's comments on the specific sections contained in the pre-draft are given below for consideration of the Chair.

Section C . International Law

- Though applicability of International law, including IHL, has been agreed to, there are differences in the structure and functioning of cyberspace, including complicated jurisdictional issues. It is required to examine the gaps in the existing international laws in their applicability to cyberspace, and to work towards workable modifications to existing laws and exploring the needs, if any, of new laws.

- As per Article 33 of the UN Charter, there is no mention of word 'justice' and hence the use of "justice" in para-23 of the pre-draft may be avoided.

- During the two Sessions of the OEWG, there have been only discussions and therefore the use of term 'noted that' could be replaced with 'discussed about' (para-24 in particular)

- "**The issue of applicability of IHL to the use of ICTs by States needed to be handled with prudence**" was not flagged in the sessions. Since paragraph 27 only highlights the questions raised by the participants, the text above referred may be deleted from the paragraph.

- While India agrees in-principle to the proposal for sharing national views as annexure, it should be on a voluntary basis.

- Paragraph 31 proposes to have a guidance note, which in India's view is not a binding obligation. However, it reflects a common understanding regarding applicability of the international law to the use of ICTs. According to India, this para is an attempt to ring uniformity in practice.

- Paragraph 32 may be deleted, which is redundant, as the Security Council provides for decisions on political issues under Chapter VII of the UN Charter.

- There are challenges with respect to attribution of attack and in distinction between civil and military cyber infrastructure. These issues require addressing for applicability of international law. Further, current technologies facilitate IP spoofing and obfuscation and require to be looked into by standards bodies.

Section D. Rules, Norms and Principles for Responsible State Behaviour

- (On PARA 35): In 2015, the General Assembly had agreed that all States should be guided in their use of ICTs by 11 voluntary, non-binding norms of responsible State behaviour set out in the 2015 report of Group of Governmental Experts. Member states should work towards universalizing these recommendations and develop mechanisms for their adherence and implementation. In this regard, India recommends that steps should be taken to explore the possibility of a broader organization or any international body under the ambit of UN, which will:
    a) primarily act as a guiding body for supporting, enabling implementation of these agreed norms
    b) work on future norms and CBMs
    c) not adjudicate the state response but facilitate states in reliable attribution.

- (On PARA 39): Proposal for new norm related to need for an agreed standard of essential security in cyberspace on the most effective ways to optimize the promising technologies while safeguarding the public. To this end, the states shall strongly endorse the widespread adoption and verified implementation of basic cyber hygiene.

- With increasing attacks on critical information infrastructure (CII), there is a need to consider separate norm for CII. The following text is suggested for protection of CII as point 39:

  "**Protection of critical information infrastructure is the responsible behavior of the States. Threat to CII can spoil integrity of information and damage economy and economic development of the nation. States must consider protection of CII with public-private partnership. States should not conduct the ICT operations to disrupt CII. States should not create harmful functions in ICT products. States should be responsible to notify users when significant vulnerabilities are identified and notify to vendors to patch up the vulnerabilities. States should work collaboratively of CII, exchange of information on threats and sharing of mitigation tools and techniques.**"

- Large corporations and bodies have capacity and developed capabilities for protection against cyber-attacks. However, SMEs, because of inherent limitations, are vulnerable to cyber-attacks and their resilience is suspect. SMEs are the backbone of most developing economies and provide the bulk of employment. States should endeavour to protect their SMEs from cyber-attacks.

- Priority should be accorded for implementing the norms already agreed to, with non-binding timelines and a mechanism for reporting, monitoring and dissemination of achievements.

Section E. Confidence-building Measures

- Speed of response is of essence to combat cyber-attacks for mitigation, resolution and to take down the threat actors. Internationally agreed timelines on sharing of information may be in order.

- (On PARA 43): When considering development of the normative framework, there should be measures for creation of a body to help conduct "peer-reviews" and assessments of adherence to norms and CBMs. Countries not adhering to norms and CBMs could be made to respond and provide explanations and details of corrective measures. Such a mechanism will not take away sovereign rights of countries to act in their own interest.

Section F. Capacity-building

- (On PARA 49) Additional significant technical areas that shall be the focus of capacity-building are:

  (i) Establishing Centers of Excellence in different countries.

  (ii) Institution building support through institutional cooperation with countries that require such support. For example, building CERTs or CSIRTs and other cyber protection institutions and mechanisms in developing countries, including by sharing of experiences and best practices.

  (iii) States must undertake to build cooperative mechanisms, including for setting up of infrastructure for testing of ICT products.

Section G. Regular Institutional Dialogue

- (On PARA 61). There is a need to discuss promulgation of an obligation of States to cooperate on countering terror propaganda on the internet, in removing such content, in alerting each other of such activities and in investigating terrorist attacks mounted through the ICTs. Distinguishing cyber terrorism from other cyber incidents and stronger recommendation for cooperation in case of former needs to be recognized. Absence of such cooperation can enhance mistrust among States and could adversely affect international peace and security and therefore directly relevant for this report.

Section H. Conclusions and Recommendations

- (On PARA 68 (c)): Other recommendations: Though not directly impinging on international peace and security, the following could be an important CBM: "**A state**

should not conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

General Comments:

- International law and its applicability in cyberspace is an important concern that is paramount for establishing peace and security. Efforts should be undertaken to address the applicability aspect of international law in cyberspace which should be based on the essential tenants of sovereignty and other fundamental principles of international law.

- It is paramount to understand that norms form the foundational pillars for development of subsequent hard laws or legally binding tenants on international community hence norms are the key to state behaviour in cyberspace which subsequently would be the underlying tenant of application of international law in cyberspace. In spite of the fact that technology has advanced and the global scenario in the global security domain has changed, there has always been a general consensus that international law's applicability is universal immaterial of these aspects. The tenants of human rights and essential principles which form the bedrock of international law should essentially also apply to the cyberspace though there are certain gaps and voids especially with regard to the understanding of the ways in which international Law is applicable. These voids need to be filled and a larger outcome should come which would find the basis for guiding nations across the world with regard to the state behaviour in cyberspace.

- Thus it should be strongly recommended that a set of guiding principles and outlines should be created which would in an essence be the harbinger of light in the domain of cyberspace relying on the bedrock of principles norms confidence building measures and most importantly addressing the threats and trust gaps among the nations.

- The territorial jurisdiction and sovereignty are losing its relevance in contemporary cyberspace discourse, due to growing ambiguous nature of jurisdiction on ICT infrastructure vis-a-vis the data centric jurisdictional aspects. This is evident in scenarios related to, cloud infrastructure where computing, storage, data, platforms etc are physically located at different geographical locations. Hence it is important to recommend a new form of sovereignty which should be based on ownership of data i.e. the ownership of the data would be that of the person who has created it and the territorial jurisdiction of a country would be on the data which is owned by its citizens irrespective of the place where the data physically is located.

- This new notion of jurisdiction which is based on the ownership of the data would essentially be based on the aspects of privacy and ownership of data thus reaffirming the universality of the right to privacy. This new concept of data oriented sovereignty extends beyond the classical territorial-based jurisdiction.

*****