Madam Chair,

I would like to thank your leadership for fruitfully conducting the ongoing 1st Session of Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. There has been considerable progress in the past eight days in our deliberations. Member countries have expressed their views on what they expect out of this convention. During these interventions, strong emphasis has been made to the need to build this convention in a timely fashion in order to prevent and combat the crimes committed with the use of Information and Communications Technologies. There is strong convergence of views among member countries that the need of the hour is to increase international cooperation and provide for capacity building and sharing of technology to combat these ever increasing and evolving crimes which are being perpetrated in speed, scale and volume and are usually trans-border in nature involving complex jurisdictional issues.

Madam Chair,

However, there has been an intense debate to classify these crimes as either committed through use of ICTs or as Cybercrimes. To us, crimes are crimes, and there is no definition of cybercrime defined in UN. How far is it useful to

debate cybercrimes as cyber dependent and cyber enabled – when the mandate of the Ad Hoc Committee as given in its very title is to 'countering the use of ICTs for criminal purposes.'

Madam chair,

The Information Communications Technology in itself is neutral and its positive usage has brought prosperity and ease of living to the humanity. The malicious use of ICTs for criminal purposes is an unfortunate negative consequence of otherwise a great human achievement of this century resulting in complex and sophisticated cybercrimes which are adversely affecting all countries developed or developing; big or small and have serious negative consequences for the growth of economies and welfare measures of the Nation States.

Madam Chair,

Crimes have traditionally been defined based on its impact on the victims and not on the basis of the actors or the means used to commit such crimes. For example: a murder of a person cannot be categorized as more heinous or less heinous, depending upon the weapon used or in terms of who committed that murder. Irrespective of the fact that what weapon was used and who the actor was, murder of a person is still a murder and this is accepted globally.

But here in this convention, if we try to segregate cybercrimes as cyber enabled and cyber dependent, we will end up defining crimes in terms of the accused, totally ignoring the victims, despite the fact that a large number of countries have raised their voices to protect the rights of cybercrime victims. Such segregation while defining the cybercrimes will deny millions of victims their right to justice which is not the intended goal of this Convention. Rather, it is an attempt to bring justice to the cybercrime victims and prevent and combat the use of ICTs for criminal purposes.

Therefore, Madam Chair, this Convention should include all those crime which are committed using ICTs because this is the only way we can keep this Convention relevant, technologically neutral and flexible for decades.

Madam Chair,

It is heartening to note that a large number of countries have emphasized the issues of human rights, fundamental freedom, privacy of individual, protection of data and protection for victims of cybercrimes. These are very important issues and need to be addressed in this Convention. In this context, India had asked in its interventions that the issue of jurisdiction be defined and this be included in the Scope of the Convention to effectively deal with the crimes committed with

the help of ICTS as the existing Conventions like UNTOC and UNCAC provisions are found to be inadequate. Budapest Convention, howsoever useful and effective it may be, for some nations, is still a Regional Convention and a large number of countries are not party to it. Hence, there is an urgent need of a Convention under the auspices of UN which is universal in its acceptance and implementation as the use of ICTs for criminal purposes is also universal and need to be dealt with the effective and efficient cooperation of all the nations together. No single nation or group of nations or a regional convention can deal cybercrimes or use of ICTs for criminal purposes on their own effectively.

Madam Chair,

India also proposed that the new frameworks and the new mechanisms need to be built through this Convention that will facilitate sharing of non-content data / Meta data with speed, efficiency and efficacy that is required to prevent, mitigate and combat the criminal activities committed through the use of ICTs without the need to go through the existing Mutual Legal Assistance Treaties (MLATS) and Letter Rogatories (LRs) that are found to be time consuming and ineffective in such cases. The non-content data does not breach the right to privacy, but will help the Law Enforcement Agencies to initiate the investigation

and build up the case to seek the content data through faster inter-governmental mechanisms that would also need to be built through this Convention. India also proposed that once a request is made for the information, it should be obligatory on the parties and private sector to preserve the data pending formal request to enable the LEAs detect, investigate and combat crimes committed through use of ICTs or we may call these as cybercrimes whether these are cyber dependent or cyber enabled. There should not be any hesitation to put an onus on private sector in such cases. Private Sector is also part of the society, has benefited from the eco-system created by the society and this should be treated as part of their corporate responsibility. It is very well known that General Data Protection Regulation (GDPR) 2016 and The Health Insurance Portability and Accountability Act (HIPAA) 1996 do provide strict obligations including penalties on the Private Sector. Hence, when we call for multi-stake holder approach in this Convention, we should not have any hesitation in building provisions in this convention so that the Private Sector operates in a manner which helps it cooperate with the Governments and is not made to stand alone and suffer with the ever increasing consequences of malicious use of ICTs for committing crimes which are resulting in enormous financial and reputational losses to the private sector. When we speak about the issues of human rights, fundamental rights, right to

privacy, protection of data, etc., we should not forget that the cybercrime victim also has these rights which get violated when a cybercrime is committed – an individual losing savings through cyber fraud may adversely impact his/her day to day life is also violation of human rights and breach of personal data. If the member States keep resisting the international cooperation or make the international cooperation of sharing electronic evidence difficult, time consuming and very bureaucratic, it will indirectly incentivize and support the criminals using the ICTs and harm further the victims. An effective balance needs to be found by the member states to empower the Law Enforcement Agencies with enough tools so that they can do their job efficiently and effectively with a view to provide justice to the victims of malicious use of ICTs.

Madam Chair,

The Indian proposals were made keeping in mind to provide protection of human rights, fundamental rights, privacy of individual, protection of personal data and for protection of victims of cybercrimes to all and especially to those who are poor, vulnerable and less informed, including children, women and elderly in developing countries where the use of ICTs is growing and consequently the cybercrimes or criminal use of ICTs also.

Madam Chair,

The Ad Hoc Committee has the responsibility not to ignore such vulnerable people and take every measure possible to enhance the capacity and capabilities of Member States through this Convention to protect the rights of these vulnerable people whose numbers would be in millions, if not billions, and provide effective and efficient mechanisms for international cooperation for sharing of information with speed, efficiency and effectiveness to combat the crimes committed with the use of ICTs and not to restrict this Convention to high end crimes or emergency situations only. And this can be achieved only, when the Jurisdiction is defined on the premise of ownership of data by an individual and not repeat not by place of its storage or processing or any other criteria.

Thank you Madam Chair.