On behalf of Cyber Justice Watch Institute, I would like to appreciate you, Mr. Chair, for giving us this opportunity to express our views in the Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs).

Nowadays, Digital technology has created various challenges in the enjoyment of human rights and will be a benchmark for governments, private actors, members of civil society, and the technology community. Governments routinely extend their access to data and information beyond their boundaries and will affect the enjoyment of human rights of non-citizens outside their territory through digital means.

Therefore, it can be stated that the obligation to respect, support, and role playing at the international level is the same as at the domestic level, especially in the digital space. In other words, governments have a primary duty to avoid any action that impedes the realization of human rights in other countries. The Economic, Social, and Cultural Rights Committee has emphasized such a commitment and even considers non-governmental organizations as responsible in this field (commentary 2).

States with the Highest Technological Expertise shall cooperate in a spirit of Responsible partnership to conserve, protect and restore, and integrity of the digital ecosystem with Less Developed Countries. Because of the different contributions and capabilities in the digital ecosystem, States have common but differentiated responsibilities. The developed states and giant private companies, in view of their determinant playing role and ownership of more resources in this field, will bear different duties to take into account of differing circumstances, particularly in relation to each state's contribution to the creation of a particular digital problem and its ability to prevent, reduce and control the danger.

Regarding the obligation to support, according to the Covenant on Economic, Social, and Cultural Rights, member states are obliged to ensure that all entities under their control respect the rights of other member states. From the point of view of the committee, it is not enough for governments to refrain from actions that harm other states; rather they must also make efforts to promote the realization of economic, social, and cultural rights. This obligation can be understood in the context of commitment to due diligence

This commitment is not restricted to the states and User-centric, social data technology companies have an immense and unique role in developing responsible behavior in the digital ecosystem. As governance roles and responsibilities have shifted in the digital ecosystem, privatizing governance for semi-public fields and infrastructures means private sector companies now play an outsized role in setting the all dimensions of security for their users. Ultimately, a process in transition from government-centered towards the agency of private sector technology companies exists in various aspects of law enforcement and foreign intelligence surveillance. Through internal policies, algorithms, and terms of service agreements, private sector companies are effectively governing

multiple dimensions of society that have a direct impact on the enjoyment of human rights. Even private companies at times, using newfound technologies provided the possibility to accomplice global crimes by increasing the amount of surveillance and illegal collection of information or accomplice the occupation or dispossession of the nations under domination. This paradigm shift requires increase the private sector's responsibility and making it more responsive. In other words, the obligation to due diligence is the standard of conduct that qualifies a private company’s responsibility for third-party impacts.

Article 3 of the Universal Declaration of Human Rights recognizes the right to security for persons. Whether through multi-stakeholder collaboration, they can develop proactive and holistic policies that ensure that technology is used to increase both freedom and security and that the benefits of digital technology are spread to people around the globe.

Unilateral sanctions are not only an obvious interference in states' internal and external affairs but also violate Article 2, Paragraph 7 of the United Nations Charter and the right to development as an inherent and inalienable part of human rights, so Governments shall work together to ensure development and remove impediments. Sustainable progress towards the implementation of the right to development requires the existence of fair economic relations and an equitable economic environment at the international level. Also, governments should refrain from unilateral actions that impede the full realization of human rights, especially the right to enjoy life with an adequate standard of health and well-being.

The goal of moving toward a less vulnerable and more secure digital future is already a shared global priority. New multi-stakeholder alliances will emerge based on the recognition that human rights protection, national and international security, and protection of the interoperable Internet platform for innovation — are all interrelated and interdependent. The interests of citizens, governments, and the private sector are aligned around the need for digital security. Going forward, digital security should serve as an essential organizing principle around which creative coalitions will form. These new alliances will provide a basis for collaborating governance responsibilities in the digital ecosystem. Such a future would be largely meaningless without an obligation to due diligence.

In the field of norms of digital space, we believe that by emphasizing the applicability of the normative human rights frameworks of the digital ecosystem, there is a need to strengthen and modify and create more accurate and relevant themes and definitions in the field of digital space. To implement the human rights objectively and widely in cyber space States and private companies need to pay attention to the possibility of maintaining national security and respecting human rights, and not giving priority to one over the other.

Moreover, it is necessary to change the paradigm in the global approach to fighting against any threat to the peace, breach of the peace, or act of aggression in the digital field, in such a way that the support of human rights and freedom is considered a tool to protect national and international security. Therefore, it is necessary to play a more effective role for all actors and stakeholders in the field of digital security by increasing interactions and trying to overcome the existing gaps.

Regards.