Non-paper

On the initial pre-draft of the report of the OEWG on the developments in the field of information and telecommunications in the context of international security

Open Ended Working Group (OEWG) on developments in the field of ICTs has been established as an inclusive and transparent platform to express interests and opinions of the broad membership of the UN, which might significantly contribute to filling the gaps left by the previous efforts, particularly GGEs in producing universal and comprehensive set of rules and norms acceptable for all states.

Therefore, we are of the view that the OEWG’s main task is to focus on developing consolidated list of rules, norms and principles of responsible state behaviour in the use of ICTs. Armenia supports continued activities of the OEWG to this end.

The initial pre-draft report of the Open-Ended Working group provides a solid basis for our further work on developing rules, norms and principles of responsible state behaviour in the cyber space. We appreciate the efforts of the chair to draw balance between the application of the International law, confidence building measures and capacity building, which are indeed interrelated and complementary elements to increase transparency and reduce the risks stemming from the use of ICTs.

Having mentioned this, below we would like to present our position with respect to several aspects of the report.

1. The OEWG and GGE should conduct their work in accordance with their mandates, avoid duplication, and their results should contribute to the implementation of the tasks of maintaining international peace and security in the use of ICTs. In this regard we believe that OEWG, as an inclusive and transparent platform for discussions between Member States, should lay down its own set of comprehensive rules, norms and procedures in the field of ICTs, which will come to fill the gaps of GGE. In this regard mere replication of the 11 norms, elaborated by the GGE cannot produce an outcome, acceptable for all member states.

2. While referring to current and potential threats it is important to apply human rights-based approach to ICTs. The report should make more explicit the link between the cyber security and human rights and freedoms, in particular by highlighting that cyber security should not be used as a pretext to violate human rights and freedoms and the protection for human rights should be at the centre of cybersecurity policy development. Furthermore, it should be emphasized that undue restrictions for access to information and its underlying infrastructure violates the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, as enshrined in the International Covenant on Civil and Political.

3. In this vein, it is noteworthy the denomination prescribed to the “non-state actors, including terrorists and criminals”, which is a vague articulation and could give ground for misinterpretations. Therefore, we propose to rectify this using more precise and concrete wording as following “non state actors, such as terrorists and criminals”, otherwise to remove it from the text.

4. In the framework of the international law the cyber security approaches should be in line with the international law and the purposes and principles of the UN Charter. In this regard it is important to avoid selective approaches and singling out any specific principle taking into consideration the ubiquitous nature of the cyber space.
5. Finally, with regard to the placeholder under the para 39, we would like to submit the following proposal for consideration:

“The states will refrain from any action that might result in attempted disruption of the integrity of critical infrastructures and government activities, and offer through secure channels timely clarifications to prevent further possible escalation”.