Statement of National Research University Higher School of Economics
(Professor Vera Rusinova, Head of the School of International Law, vrusinova@hse.ru)

Your Excellency, Mr. Chair, dear participants of the discussion, this is a big honor for me as an International lawyer to represent the submission of the academic institution – National Research University Higher School of Economics at this meeting.

Our ideas concerning the work of the second OEWG can be divided into two main blocks: a theoretical (and general) one, which will be critically assessing the standard-setting track, and a practical one with a number of concrete recommendations.

In the first one I would like to address the *added value of the standard-setting track*.

The approach taken by the OEWG sofar consists in the separation between questions of applicability of International law in the ICT context, on the one hand, and drafting of legally non-binding standards, on the other. The division between both groups reveals to be a formal one. The former are legally binding, but there is not much consensus on how exactly they apply in 'cyberspace', the latter are non-binding political commitments. However, what we can seriously question here is whether these standards do have added value by their content?

The answer may be really disappointing.

These non-binding rules, norms, and principles do not change the scope of binding provisions of International law, mainly because of two safeguards. The first one lies in the design of formulations. Standards that may be relevant for setting the contours of the outlawed cyberactivities are constrained by references to *lex lata* International law. It is true for many of the 'rules, norms, and principles of responsible state behavior'. For instance, a promising sixth norm, which could have significantly contributed to the outlawing of state-on-state cyberoperations should it be limited to state activity that 'intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public', remarkably confines the scope of this prohibition to the activities violating states' obligations under International law.

The second umbrella safeguard provides for that these 'norms do not seek to limit or prohibit action that is otherwise consistent with international law'.

Thus, the content of the standards did not generate any 'added value' with respect to the negative and positive obligations of the states. Moreover, these standards cannot serve as an interpretation or understanding as to how existing international law applies to ICTs precisely because of the caveat made by the states with respect to the additional, subordinated role of these 'norms, rules, and principles'.

Such constellation puts in place a 'normative gap scenario' showcasing that for the many states the legal uncertainty and legal gaps are a more profitable constellation.

A solution might be found in the stage-by-stage shift from the standard-setting to the law-creating track. Already elaborated rules, norms and principles of responsible state behavior allow this shift for, provided that the above-mentioned safeguards will be lifted. It can happen in two stages: at the level of content and then with respect to the nature.

In the second part I am going to share some concrete recommendations on how the OEWG can contribute to capacity-building of states.

Firstly, alongside with a global level, the bilateral and regional co-operation is of crucial importance. The OEWG can enhance these forms of co-operation by elaborating *model agreements and forms*. It can be, for instance, a model CERT-to-CERT agreement and a model form of notification about the ITC incident.

Secondly, the notion of critical infrastructure lies at the heart of different efforts aimed at bolstering the deterrence against malicious ITC-related acts, as well as defence and resistance of
states against cyber threats. So, it would be very practical, if the OEWG could have initiated drafting of a **non-exhaustive, indicative list of the objects of critical infrastructure**.

Thirdly, taking into account the huge importance of the experience-sharing mode, the OEWG could have suggested to the states to voluntarily share their best practices on the capacity building and bolstering the potential. As a result, the states and all other stakeholders will be able to profit not only from the 2021 GGE Compendium on applicability of International law to ICT acts, but also the **OEWG best practices collection**.

This concludes my submission and I would like to thank H.E., the Chair of the OEWG and all organizers for this chance to share some ideas with respect to our common objective, which is to 'shape a community of shared future for humankind in cyberspace'.