Remarks of the Russian speaker on the behalf of A.V.Krutskikh, Special Representative of the President of the Russian Federation on International Cooperation on Information Security, at the UNIDIR workshop "The Future of Norms to Preserve and Enhance International Cyber Stability"
(Geneva, February 9-10, 2016)

Distinguished colleagues,

First of all, I would like to thank the hosts for organizing this workshop and the opportunity to exchange views on a highly important issue – the elaboration of rules, norms or principles of responsible behavior of states in information space.

Today no one doubts the importance of this step. Russia together with its SCO partners has been promoting the need for such rules for several years. We have submitted a concrete draft code of conduct to the UN twice while calling on international community to keep in mind even a more ambitious goal – a universal treaty on international information security (IIS).

The unanimity on the prevention of conflicts and aggression in information space, keeping it peaceful and free, shared now by the majority of states is a victory that should be ascribed to common sense rather than diplomacy. International consensus around the rules of state behavior is a positive trend that should shape the international debate on IIS for years to come.

Year 2015 was very productive in this respect.

First, in January an updated version of "International Code of Conduct for Information Security" was officially submitted to the UN on the behalf of SCO member states. I would like to remind that it is a "living" document designed to outline the general parameters of how such rules, in our view, could look like.

Second, in June the UN Group of governmental experts on IIS concluded its work. It managed to reach a consensus on a whole range of essential issues, in particular that:

- ICTs should be used for peaceful purposes only, while international cooperation should be aimed at prevention conflicts in information space;
- such universally recognized principles of international law as refraining from the threat or use of force, respect for sovereignty and non-interference into the internal affairs of states apply to information space;
- states have sovereignty over ICT-infrastructure on their territory;
- all accusations of involvement in computer attacks brought against states should be substantiated;
- states should not use proxies for computer attacks and should seek to ensure that their territories are not used to these ends;
- states should fight with the use of hidden harmful functions – so-called backdoors – in ICT-products.

A number of recommendations that the Group came out with are regarded by many experts as initial norms, rules and principles of responsible behavior of states in the use of ICTs.

Third, in December the UN GA adopted by consensus the resolution "Developments in the field of information and telecommunications in the context of international security". This document has been submitted to the UNGA First Committee by Russia for 17 years in a row. At the UNGA 70-th session the number of its cosponsors broke a record mounting to more than 80 countries. I would like to seize an opportunity and thank them for their support and cosponsorship of our resolution.

This resolution suggests the establishment in 2016 of a new UN GGE on IIS. It is mandated to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, and how international law applies to the use of information and communications technologies by States, as

well as norms, rules and principles of responsible behavior of states, confidence-building measures and capacity-building,

A new Group is to be composed of the representatives from 25 countries. Its composition should take into account not only just geographic representation but also the specific features of this GGE and the fact that the issues discussed by it are equally important for all the states, with no exceptions.

The key players in the ICT domain, which have already put a lot of practical and negotiation efforts to ensure IIS, should be taken on board. It is no less important to engage in the GGE debate those states that have just started to develop this field. Their contribution to a large extent facilitated the success of the previous GGE.

In the run-up to the new GGE views on how the rules of state behavior in digital environment should look like are multiplying. Such a lively debate reflects that this issue arouses much interest. No doubt, it is necessary and useful.

However, the flip side of this variety of concepts should be taken into account.

Some of them seem to water down the core idea behind these rules – prevention of conflicts for the sake of peaceful and stable development of global information space. There are also suggestions to adopt a sort of "peacetime norms" which, seemingly, are designed to be enacted *ad hoc* and in some cases be rendered inoperative. The rules *per se* – which should lay done a broad political framework for the use of ICTs – are turned into technical agreements.

I would like to present Russian approach to the parameters of future rules, principles and norms (RPNs) of responsible state behavior in information space.

There are five parameters:

1) **Universality.** RPNs should be elaborated under the UN auspices. If we opt for the regional RPNs, there is a risk that the RPNs in different organizations will be contradictory. This may result in a world divided in the information space into a number of alliances united around their

own "norms" while the relations between these alliances will be confrontational. This is a straight road to a cold war in a digital domain.

2) **Peace-building nature.** RPNs should be designed to enshrine in information space the principles of refraining from the threat or use of force, respect for sovereignty and non-interference into the internal affairs of states. This is the essence of such RPNs that should reflect the basic principles of non-confrontational interaction of states in digital domain and unequivocally describe unacceptable actions in it.

   It is important to ensure that the language about these principles reflect the specific attributes of ICTs. Particularly, to solve the attribution problem (which does not exist in a physical world) the RPNs should stipulate that states should not commit such acts neither directly, nor through proxies.

   At the same time the RPNs should include a provision that a state's involvement into such actions should be substantiated.

3) **State-centrality.** RPNs should be designed to shape the model of interaction in information space which clearly defines the responsibilities of all participants and their respective roles.

   Along with states, there are a lot of other actors active in digital domain today. Their influence on it is substantial and cannot be neglected. The motives of these actors differ and include commercial, scientific and other interests. We do not oppose a model which suggests the engagement of all stakeholders – a so-called "multistakeholder" model. However, it is important to ensure that every actor plays its role, makes its contribution as well as bear relevant responsibilities. States should have a leading role which is confirmed in the report of the previous GGE on IIS (par. 19, 31).

4) **Framework substance.** RPNs should be a framework political agreement rather that technical measures. They should constitute a international legal 'umbrella" under which more narrow and specific

measures can and should be adopted. Along with the basic principles of non-confrontational interaction of states in information space, RPNs should cover political aspects of the following issues:

- cooperation on countering the use of ICTs for terrorist and other criminal purposes;
- confidence-building in information space;
- capacity-building in the use of ICTs;
- protection of human rights online;
- state policy on software vulnerabilities (states should neither use harmful hidden functions or backdoors nor force companies to insert them into their products);
- ensuring that states participate in Internet governance on an equal footing.

5) **Permanent validity.** RPNs should have a permanent validity. The adoption of separate norms only for "peaceful time", or for wartime, devaluates the very idea of "rules of behavior" that should draw a distinct line where unacceptable under any circumstances behavior starts. This line should be clear with no loopholes allowed. If we adopt such limited "norms", we overtly declare that in some cases they can be neglected.

Moreover, though RPNs are referred to as a so-called "soft law", one should not get an impression that they can be violated with impunity.

We are also flexible on their format. In our view, the best possible option could be to formalize such RPNs as a separate UN GA resolution.

I would like to make a special reference to confidence-building in information space. We regard it as an important instrument to enhance stability. However, CBMs should neither substitute nor contradict rules of behavior based on above-mentioned principles. They should complement and specify them taking into account regional peculiarities.

Meanwhile, the political basis - universal RPNs - will be the same for the whole world and facilitate substantial "compatibility" of the CBMs adopted in different regions.

Dealing with the adaptation and legal regulation of the use of ICTs, international community have to address one more issue - to ensure feasibility of fast and verifiable identification of the sources of computer attacks and their motivation as well as to find ways to overcome anonymity (covertness) of harmful acts in information space.

Another issue calling for solution with regard to the elaboration of RPNs is to agree in good time on at least basic terms comprising an international glossary on countering harmful and malicious use of ICTs adopted by consensus.

The work of the new UN GGE on IIS will be intense. I would like to reiterate that in addressing these issues it is important not to miss the key goal - prevention of conflicts in information space, its militarization and the information arms race.

Thank you for attention.