**Statement by the representative of the Russian Federation at the informal intersessional meeting of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025**

New York, 6 December 2022

*Check against delivery*

*Confidence-building measures*

Distinguished Mr.Chair,

Distinguished colleagues,

Confidence-building measures (CBMs) at the international level can serve as a tool to increase predictability and reduce the likelihood of misunderstandings, as well as the risk of conflict between States.

We believe that one urgent task in this domain is to create a mechanism for interstate interaction aimed at preventing computer incidents and attacks against information resources of States, and ultimately at reducing the risk of conflicts stemming from malicious use of ICTs. A first step in this direction could be the establishment of a global intergovernmental PoCs directory, facilitating direct communication between competent authorities of States in the field of detecting, preventing and mitigating consequences of computer attacks, as well as responding to computer incidents.

Other such measures could include voluntary exchange of information on national policies, strategies, legislation and organizational structures aimed at ensuring information security of a country and relevant best practices, where practicable and appropriate. It is important to include in this list the notion of adherence to national legislation and exchange of implementation practices. This kind of information could be shared by States within the OEWG itself, as CBMs are part of its mandate. We see merit in further studying the proposal to establish an online platform for such an exchange.

With a view to enhancing trust and transparency it is also essential to encourage States to consult on issues related to their activities in information space that may cause concern in order to prevent conflicts and peacefully settle any

arising divergences. Para 23 of the 2021 GGE report endorsed by the UN General-Assembly explicitly provides for this recommendation.

When developing CBMs it is particularly important to observe the principle "do no harm". It might, therefore, be useful to agree upon basic universal principles of confidence-building measures in ICT-environment. The adoption of such measures should not:

– cause harm to security of participating States, as well as that of third States;

– provide advantages to any State or group of States in the military, political, economic or other domain, and in the field of intelligence;

– be used as a tool for interference in internal affairs of States, for subjective political assessment of activities and intentions of States in information sphere;

– be used as an instrument of or pretext for sanctions and other unilateral coercive measures.

The voluntary and non-binding nature of CBMs is a factor that naturally limits their efficiency. For the purposes of ensuring peace and security in information space we should also bear in mind the objective of improving and raising the level of cooperation among States and their competent authorities.

As far as our interaction with other interested parties is concerned, we presume that CBMs are, above all, an instrument to build trust among States. Hence, in future activities of the OEWG, it would be more appropriate to dedicate intersessional meetings with non-governmental actors not to CBMs, but to specific technical aspects of information security. This would allow national delegations to take full advantage of the relevant technical expertise of the private sector, without prejudice to the central role of States in dealing with issues of national security.

Last but not least, building confidence and trust is ultimately about making people meet each other, talk to each other, find points of convergence. Much of this work is always done outside of the rooms. That said, there is a pressing need to ensure in-person participation of all representatives of national delegations, as well as other interested parties accredited to the Group, in formal sessions and

intersessional meetings of the OEWG held at the UN Headquarters through timely issuance of visas. We strongly recommend that this issue be reflected in the Group's deliberations.

Thank you for attention.

*Right of reply*

Distinguished Mr. Chair, answering your question about a possible result of the OEWG in 2023, we would like to see the establishment of the PoCs directory and its basic elements – composition, modalities, interaction procedures – reflected in the next Annual Progress Report. Following the step-by-step approach, we could also define areas for further development of the directory, like templates of notifications.

As far as CBMs as a whole are concerned, we acknowledge that some work in this area has already been done at the regional level and it is important to take into account this experience. But we have to be mindful of both positive and negative examples. I would like to stress that not all regional experiences are replicable at the global level, not even within all countries of the same region.

One thing that should be avoided at the universal level is the replication of politicized mechanisms of groundless attribution of computer attacks. Instead, we suggest a pragmatic approach based on professional cooperation between States and their competent experts. Within the OEWG we should focus on developing new universal measures rather than create repositories of regional practices.

Thank you.