

**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, 5 December 2022

Check against delivery

Global intergovernmental PoCs Directory

Distinguished Mr.Chair,

Distinguished colleagues,

I am taking the floor, by way of interactive discussion, to further comment on the variety of views expressed by delegations today.

The Russian Federation is pleased to note the increased interest of the UN Member States in the idea of establishing a global intergovernmental PoCs Directory. We hope this initiative can become one of the specific practical deliverables of the OEWG in 2023.

We welcome the efforts of the UNODA to compile the submissions of States. We also acknowledge UNIDIR's survey that adds up to the Secretariat's study. What immediately caught our attention is the big number of different ideas and possible elements of a future PoCs directory that need to be assessed and thoroughly discussed by States. We have also heard relevant proposals at the UNIDIR Conference on Interstate Cooperation on ICT-security held last Friday, 2 December 2022, in Geneva.

Against this background it is important, at this initial stage, not to get lost in details and not to lose sight of our main objective which is to improve communication and cooperation between States and their competent agencies, reduce tensions and prevent conflicts. Russia, therefore, welcomes the gradual approach suggested by the Chair. In our view, this is the right way to achieve a tangible result by the 5th OEWG session in 2023.

We believe that we need to start, as a priority, by defining the purposes, composition and working principles of the directory. We also see merit in agreeing upon the interaction procedures and standardized notification templates at an early stage. Those will include a basic scenario for the UN Member States in the event of computer attacks carried out against their information infrastructure and / or computer incidents.

They will also help unify the exchange of information in order to enhance the effectiveness of response to relevant threats.

Given the specificities of ICTs, pragmatic interaction to ensure security in their use, including computer incident detection, response, recovery and mitigation actions, is only possible with participation of duly authorized and competent technical experts. We, therefore, see added value in establishing PoCs at two levels – diplomatic and technical.

Amidst growing tensions in the global information space and unilateral coercive measures taken against CERTs, it is important to objectively assess the existing PoCs directories, at the regional level, in terms of their efficiency and usefulness. Our analysis shows that not all of the regional instruments can be equally used for the purposes of conflict prevention. In a summarized way, two of the main drawbacks consist in (1) politicization of technical issues, and (2) absence of one particular national body duly authorized to take measures to detect, prevent and mitigate the consequences of computer attacks, as well as to respond to incidents.

Hence, we believe that the composition of the global PoCs directory should not be determined by the existing regional instruments, but by the criteria of powers and competence of a particular agency at the national level. Nominating an institution rather than a particular person as a PoC would facilitate keeping the directory updated and operational 24/7.

At a first stage, the directory could use the existing bilateral communication channels including diplomatic ones. This will not require any additional funding. As regional experience shows, new communication means do not necessarily guarantee security of sensitive information, require greater resources and time, and need to be developed by technical specialists of States.

To conclude, we suggest focusing our efforts on three basic tasks: create a pragmatic and depoliticized PoCs directory, agree upon the interaction procedures and develop standardized notification templates. These steps would serve as a basis for further development of the PoCs directory. Measures to promote capacity-building and provision of the necessary technical assistance are very important and could be taken in parallel. At a next stage of discussions, proposals to conduct joint trainings,

communication checks could be further elaborated. At this point we see them as premature.

Thank you for attention.

Right of reply

Distinguished Mr.Chair,

Distinguished colleagues,

I am forced to take the floor once again for a brief remark.

It is very unfortunate that the constructive spirit of today's meeting is spoiled by a delegation that could not refrain from politicizing even this informal intersessional meeting envisaged by the Chair for very specific, in-depth discussions on concrete issues. This is none of a surprise, as it has become the preferred tactics of certain countries that want to distract attention of the international community from solving significant issues of international information security. I will refrain from going into details of what, in Russia's perception, constitutes a source of tension in the ICT domain. A country that has just hosted yet another cyber drill of a military alliance would know that for itself. But I strongly encourage delegations to stick to the pragmatic approach proposed by the Chair.

Thank you.