STATEMENT


New York, 31 March 2022
Within thematic discussion on confidence-building measures:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

With a view to increasing predictability and reducing the likelihood of misunderstandings, as well as the risk of conflict states should develop confidence-building measures. These measures include, inter alia, voluntary exchange of information on national strategies, legislation and organizational structures aimed at ensuring information security of a country and exchange of best practices, where practicable and appropriate.

We believe it is an urgent task is to create a **mechanism for interstate interaction** aimed at preventing computer attacks on information resources of states, including exchange of information about computer incidents through channels of authorized bodies, at the global level. We could also think of elaborating a list of basic information (including technical data) necessary to jointly determine the source of illegal ICT-activities.

In case of a computer incident, in order to reduce tension and minimize its consequences, it is necessary to promptly eliminate the malicious activity associated with this incident. This is possible, if competent experts quickly engage in these efforts and if they are provided with the necessary technical data on the incident. Given that today many computer attacks are carried out under “false flag”, lack of relevant technical data leads to misinterpretation of incidents and misunderstandings between the parties.

We reaffirm our readiness to strengthen contacts through national computer incident response teams (CERTs). From the Russian side, such a competent agency is the National Coordination Center for Computer Incidents (NCCC).

NCCC’s experience of interaction with CERT groups of foreign states shows that in order to build effective interstate cooperation, it is necessary to
ensure that this process is strictly regulated. One of the ways to formalize the mechanisms of interaction between CERT groups is to establish a directory of points of contact (PoCs) that carry out and coordinate interaction in the field of detecting, preventing and mitigating consequences of computer attacks, as well as responding to computer incidents.

This tool is already used as a confidence-building measure at regional fora such as the OSCE (OSCE Informal Working Group on Confidence-Building Measures in Information Space) and the ASEAN Regional Forum on Security of and in the Use of ICTs. However, there is no such mechanism within the UN.

The establishment of a PoCs directory within the UN will contribute to achieving the following goals:

– identifying PoCs with which a CERT group can communicate in its own and in other countries in the event of an incident in the area of ICT-security;
– reducing and overcoming tension and threat of conflicts due to misunderstanding and misperception of incidents in the area of ICT-security;
– keeping up to date the list of main contacts for exchange of information about computer incidents that require immediate response.

In this regard, as a practical measure to improve interaction and communication between CERT groups, it seems appropriate to use the already existing experience of the aforementioned organizations and establish a directory of PoCs within the framework of the OEWG.

When developing this tool, it is necessary to define protocols and procedures for interaction of PoCs responsible for exchange of information at the technical and political levels.

At the same time, the PoCs responsible for interaction at the technical level, within their competence and in accordance with the available potential and resources, could carry out:

– exchange of information about computer incidents occurring to information resources located within their area of responsibility;
– rendering assistance to another state in responding to computer incidents and identifying threats to security of information upon receipt of a relevant request;
– informing about new threats to security of information, as well as disseminating best practices.

We believe it would be useful to establish the directory of PoCs on the basis of the following principles:
– the directory of PoCs at the UN platform should contribute to reducing tension and threat of conflict due to misunderstanding and misperception of incidents in the area of ICT-security, which could lead to miscalculations and possible escalation, as well as facilitating communication and dialogue on security of and in the use of ICTs;
– PoCs at the national level should be authorized to carry out and coordinate interaction in the field of detection, prevention and mitigation of consequences of computer attacks, as well as to respond to computer incidents;
– regardless of the international situation, the PoCs will strive to maintain political neutrality, continuing to interact with other PoCs in the field of responding to threats to security of and in the use of ICTs;
– PoCs should not be subject to international sanctions;
– PoCs will opt for pragmatic cooperation in the field of responding to threats to security of and in the use of ICTs in order to avoid the risks of misperception, escalation and conflict that may arise from the use of ICTs;
– in their activities PoCs should take into account the recommendations developed by the OEWG, as well as to follow the rules, norms and principles of responsible behavior of states in the information space.

We also suggest discussing the possibility of establishing the practice of exchanging national lists of areas in which critical information infrastructure entities operate, as well as criteria for their categorization.

Thank you for your attention.