Courtesy translation

Concept paper of the Russian Federation on establishing a directory of Points of Contact

Preamble

The current level of development of information and communications technologies (ICTs) demands that all governments pay greater attention to ensuring information security. The growing need of businesses and society to go online frequently causes hasty decisions taken without particular attention to security of information resources. The omnipresent use of ICTs in the lives of people and the wider use of achievements of digitalization increase threats in this domain.

Taking advantage of anonymity and cross-border nature of global information space, malicious actors remain unpunished while deliberately conducting computer attacks against critical infrastructure of states and information systems of companies and individuals.

Since modern computer attacks are of cross-border character, and establishing sources of malicious actions in information space in a trustworthy manner is almost impossible, the only way to effectively counter them is through tailored cooperation between relevant state authorities.

If a computer incident occurs, in order to decrease tensions and mitigate its consequences it is necessary to eliminate malicious activity related to it as soon as possible. To that end, rapid engagement of competent experts, provided with technical data of the incident, is required. It is particularly important given the fact that many computer attacks are carried out under “false flag”.

Goals and objectives

The UN Open-ended Working Group could undertake steps to elaborate mechanisms of cooperation between/among competent authorities. The establishment of **a directory of Points of Contact (PoCs)** could serve as a way for streamlining and enhancing efficiency of such interaction.

This instrument is already used as a confidence-building measure at regional fora (OSCE Informal Working Group; ASEAN Regional Forum). There is no such mechanism within the UN. As the first universal confidence-building measure, the

OEWG could provide for the creation of the PoCs directory. The 2021 OEWG final report (para 51) and the 2021 UN Group of Governmental Experts final report (para 78) recommended considering this issue.

The establishment of the PoCs directory will contribute to addressing the following issues:

– Designating points to be contacted by competent authorities in their countries or abroad in case of incidents, to facilitate communication and dialogue on security of and in the use of ICTs;

– Keeping updated the directory of main contacts for information exchange on computer incidents which need to be addressed immediately;

– Establishing pragmatic cooperation between main national bodies on computer incident response;

– Easing and overcoming tensions, as well as threat of conflict arising from misunderstanding and misperception of incidents in ICT security.

Composition of the PoCs directory

The PoCs directory will comprise national authorities of the UN Member States competent to address issues in the following areas:

1) Detecting, preventing and eliminating consequences of computer attacks, as well as computer incident response (technical PoC);

2) Developing international cooperation, as well as establishing bilateral and multilateral contacts on ensuring information security (diplomatic PoC).

The PoCs responsible for cooperation at the **technical level**, within their competence and depending on their capacity and resources, could:

– Exchange information on computer incidents concerning information resources under their responsibility and counter malicious activity emanating from their national information space;

– Assist other states in responding to computer incidents and detecting threats to information security (upon request);

– Exchange data on existing and potential threats to security of and in the use of ICTs, as well as share best practices.

The PoCs responsible for cooperation at the **diplomatic level**, within their competence and depending on their capacity and resources, could:

– Facilitate and speed up communication and interaction on security in the use of ICTs, *inter alia*, by creating conditions for direct dialogue between competent authorities and experts;

– Increase stability and reduce risks of misunderstandings, unintentional escalation and conflicts arising from the use of ICTs;

– Organize consultations between interested parties on issues of national security concern.

Working principles of the PoCs directory

We deem necessary to build the work of the PoCs directory within the UN on the following guiding principles:

– The PoCs directory within the UN should foster communication and dialogue on security of and in the use of ICTs;

– Despite international situation, the PoCs will aim at preserving political neutrality, maintaining interaction with other PoCs on addressing threats to security of and in the use of ICTs;

– The PoCs should not be subject to sanctions;

– The PoCs will opt for pragmatic interaction on addressing threats to security of and in the use of ICTs in order to exclude risks of misperception, escalation and conflicts which can arise from the use of ICTs;

– In their activities PoCs should take into account the recommendations elaborated by the OEWG and follow the rules, norms and principles of responsible behaviour of states in information space.

Description

While elaborating the directory, it is necessary to determine protocols and procedures of interaction between/among PoCs responsible for information

exchange at the technical and diplomatic levels that will help define the main areas and forms of cooperation on security of and in the use of ICTs, elaborate a basic scenario of actions for the UN Member States in case of a computer attack against and / or a computer incident in their information infrastructure, as well as manage and overcome the probability of misperception and possible conflict, or political or military tensions as a result of the use of ICTs.

The PoCs will be contacted by sending a request via mutually agreed channels of communication (e-mail, telephone or others), including diplomatic ones. The PoCs should ensure accounting and storage of information transmitted during the interaction, as well as create conditions excluding illegal access, amendments and changes or public revelation of such information.

Member States will update PoCs contact information on an annual basis and notify about changes to it no later than 30 days after they were made.

In order to enhance interstate cooperation on security of and in the use of ICTs at the next stage it is also required to develop a list of basic information (including technical data) which is necessary for studying a computer attack and a computer incident.