Preamble

Amidst growing tensions in international information space UN Member States are in great need for a transparent mechanism to regulate effectively emerging interstate disputes. Modern computer attacks are often of cross-border nature, and establishing sources of malicious activities in information space in a trustworthy manner is almost impossible. Blaming States without providing technical evidence creates risks of uncontrolled escalation of conflicts up to a real confrontation. In this regard, it is only possible to effectively address modern threats to information security in case of well-established cooperation between authorized agencies of States. Proceeding from the recommendations of the previous UN Open-ended Working Group (OEWG), Member States should voluntarily take measures to ensure transparency through the exchange of relevant information and experience in the format and fora of their choice1.

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

Goals and objectives

As a follow-up to the recommendations elaborated by the OEWG, Member States are invited to agree, as the first universal confidence-building measure, to establish, under the UN auspices, a global directory of Points of Contact (PoCs) on security of and in the use of ICTs with a view to strengthening interaction and

cooperation among States. Both the final report of the first OEWG 2021\textsuperscript{2} and the progress report of the OEWG 2022\textsuperscript{3} recommended to consider this issue.

Such a mechanism will demonstrate the international community’s focus on regulating and increasing the effectiveness of interaction between national authorized bodies on security of and in the use of ICTs. In addition, its development will reaffirm the commitment of UN Member States to resolve disputes arising from the use of ICTs by peaceful means.

This instrument is already used as a confidence-building measure at regional fora (OSCE Informal Working Group; ASEAN Regional Forum).

In this regard, it must be emphasized that the UN should play a key role in the context of efforts to create a directory of PoCs. Relevant regional initiatives could be taken into account and complement the activities of the proposed global directory of PoCs.

The establishment of the PoCs directory at the UN will contribute to addressing the following tasks:

− 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 organizations on computer incident response;
− Easing and overcoming tensions, as well as the threat of conflict arising from misunderstanding and misperception of incidents in ICT security.

**Creation of the PoCs directory**

States, on a voluntary basis, will designate PoCs at the diplomatic and technical levels, which could be contacted in emergency situations. PoCs should be duly authorized to ensure security in the use of ICTs at the national level. States may wish to designate for inclusion in the global directory the same PoCs that are included in regional directories. A template for the proposed directory is provided in the annex.

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

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

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

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.

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;

---

4 OEWG Progress Report 2022, A/77/275, Annex, p.16 (c).
– 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.

**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;
– Regardless of the 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 diplomatic and technical 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,
– manage and overcome the probability of misperception and possible conflict, or political or military tensions as a result of the use of ICTs.

The directory will consist of relevant PoCs from all UN Member States. In order to build pragmatic cooperation on security of and in the use of ICTs, both diplomatic and technical PoCs should be included in the directory. At the same time, at the national level Member States should ensure appropriate interaction between the PoCs, which will allow them to effectively solve their tasks. They are included in the directory is on a voluntary basis.

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 to exclude illegal access, amendments and changes or public revelation of such information.

UN 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.

The United Nations Office for Disarmament Affairs (UNODA) will be responsible for maintaining and updating the directory of PoCs in the light of its institutional connection with the OEWG.

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.

**Financing**

No additional financial resources are required to create and launch the proposed directory of PoCs, since the exchange of information on security of and in the use of ICTs is carried out through already existing communication channels.
Annex

Template for a UN global directory of Points of Contact

<table>
<thead>
<tr>
<th>UN Member State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoC</td>
</tr>
<tr>
<td>Diplomatic</td>
</tr>
<tr>
<td>Technical</td>
</tr>
</tbody>
</table>

1. An organization of a UN Member State authorized at the national level to develop international cooperation, as well as to establish bilateral and multilateral contacts in the field of information security is appointed as a diplomatic PoC.
2. An organization of a UN Member State authorized at the national level to detect, prevent and eliminate the consequences of computer attacks, as well as to respond to computer incidents, is appointed as a technical PoC.
3. E-mail is indicated based on the possibility of sending notifications of computer attacks and incidents to this address for further interaction, as well as other information for the purposes provided for in the concept paper.
4. A contact phone number is indicated, which may not be tied to a specific person and by which you can contact a diplomatic or technical PoC at any available time.
5. The languages spoken by contact persons for communication are indicated.