OEWG Inter-Sessional Meeting

Developing Inter-State Cooperation on ICT Security: PoCs Directory

Contribution of the Russian Federation
December, 2022
It is necessary to enhance sharing of information among States on ICT security incidents for timely response, recovery and mitigation actions, including through the exchange of information between national CERTs bilaterally.
Establishment of the PoCs Directory is recommended in the consensus progress report of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025 as the first universal CBM.
National Computer Incident Response and Coordination Center: Russian organization authorized to detect, prevent and eliminate consequences of computer attacks, as well as respond to computer incidents

2019
Sent 2,083 notifications on malicious activity
Received 550 responses

2020
Sent 2,897 notifications on malicious activity
Received 649 responses

2021
Sent 3,303 notifications on malicious activity
Received 1,697 responses

December, 2022
### Reasons

#### Organizational
- Lack of unified rules of inter-State cooperation in the field of computer incident response
- Formal agreements
- Single “entry point”
- Authorized organization

#### Legal
- Lack of international and national legislation in the field of ICT security
- Non-binding CBMs

#### Technical
- Internal technical challenges (disruption, malfunctioning, etc.)
- Technical aspects: reliable means to identify the source of malicious activity, computer attacks as a service model, non-transparent Internet protocols

#### Political
- Accusatory rhetoric (political attribution), lack of evidence
- Achieving political goals, exerting political pressure
- Ignoring technical aspects

December, 2022
CSTO Coordinating Center for Computer Emergency Response

- Promoting cooperation in the field of computer incident response
- Collection and exchange of information on computer incidents, as well as analysis of threats
- Providing mutual assistance in resolving organizational, technical and regulatory issues
- Promoting the development of a legal framework for cooperation
- Organizing and conducting joint training
- Conducting seminars and conferences
### PoCs Directory

<table>
<thead>
<tr>
<th><strong>Goal</strong></th>
<th>Establishment of the Points of Contact Directory at the UN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objectives</strong></td>
<td>Designating points to be contacted to facilitate communication and dialogue on security of and in the use of ICTs</td>
</tr>
<tr>
<td></td>
<td>Keeping updated the directory of main contacts for information exchange on computer incidents</td>
</tr>
<tr>
<td></td>
<td>Establishing pragmatic cooperation between national authorities on computer incident response</td>
</tr>
<tr>
<td></td>
<td>Easing and overcoming tensions, as well as the threat of conflict arising from misunderstanding and misperception of incidents in ICT security</td>
</tr>
</tbody>
</table>

| **Principles** | Preserving political neutrality, performing pragmatic interaction, avoiding sanctions, taking into account the recommendations elaborated by the OEWG |

---

**Not amorphous tool for political accusations**

- **Diplomatic**
- **Technical**

December, 2022
<table>
<thead>
<tr>
<th>PoCs Directory</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>UN Member State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point of Contact</td>
<td>Organization (webpage)</td>
</tr>
<tr>
<td>Diplomatic</td>
<td></td>
</tr>
<tr>
<td>Technical</td>
<td></td>
</tr>
</tbody>
</table>

December, 2022
Standardized Template

Accepted by the UN Member States

Unified rules

Strengthening security

Reducing response time

More efficient response

December, 2022
Thank you for your attention!

“A journey of a thousand miles begins with a single step”
- Laozi