Confidence Building Measure № 1 on the establishment of a global intergovernmental Points of Contact Directory

Proposal of the Russian Federation

Cosponsors: Republic of Belarus, Republic of Nicaragua

Confidence Building Measure (CBM) № 1: With a view to building and maintaining pragmatic interaction, Member States will identify, on a voluntary basis, points of contact at the diplomatic and technical levels among national authorized bodies. The points of contact will be included in a global intergovernmental directory for establishing dialogue on security of and in the use of ICTs, which will promote equal participation of all countries in these activities, as well as exchange of experience and capacity-building. Member States will update the contact details twice a year, notifying of any changes no later than 30 days after they have occurred. Considering the efforts of regional organizations, the global points of contact directory will include a basic list of data and parameters necessary to facilitate interaction between the national authorities of Member States. Member States will, on a voluntary basis, take measures within their area of responsibility so as to prevent and resolve conflict situations stemming from the use of ICTs.

Goals and objectives

1. The goal of this project is to establish, under the UN auspices, a global intergovernmental Points of Contact (PoCs) Directory on security of and in the use of ICTs.

2. The establishment of the UN PoCs Directory will contribute to fulfilling the following tasks:

   • defining and keeping updated a list of PoCs to promote direct interstate dialogue on security of and in the use of ICTs;
   
   • establishing practical interaction between authorized national organizations in the field of computer incident response;

---

1 2022 OEWG progress report, A/77/275, annex, paragraph 16 (a).
• reducing tensions and, as a result, the threat of conflicts resulting from misunderstanding and misperception of computer incidents.

3. It is reasonable to limit the scope of the PoCs Directory to preventing the escalation of tension between States and responding to computer incidents. Investigations against persons responsible for perpetrating computer attacks should be carried out through law enforcement agencies.

**Working principles**

- Communicability (the PoCs Directory should facilitate communication and interstate dialogue on security of and in the use of ICTs);
- Neutrality (regardless of the international situation, the PoCs must remain politically neutral and must not be subject to sanctions);
- Pragmatism (in carrying out their activities, PoCs will give preference to pragmatic interaction in order to avoid the risks of misperception, escalation and conflict that may stem from the use of ICTs);
- Confidence (exchange of information between PoCs is carried out in a confidential manner and can be made public only by mutual consent of all PoCs involved in such interaction);
- Consistency (in the framework of its activities, the PoCs should take into account the recommendations of the OEWG and relevant UNGA resolutions).

**Composition of the directory and functions of PoCs**

4. States, on a voluntary basis, will designate PoCs at the diplomatic and technical levels. States may designate for inclusion in the global directory the same PoCs that are included in regional directories². A template for the proposed directory is provided in Annex 1.

5. The PoCs Directory will comprise national authorities of the UN Member States assigned to address issues in the field of:

- development of international cooperation, as well as establishment of bilateral and multilateral contacts in the field of information security (diplomatic PoC);

---

² 2022 OEWG progress report, A/77/275, annex, paragraph 16(c).
• detection, prevention and elimination of consequences of computer attacks, as well as computer incident response (technical PoC).

6. PoCs responsible for interaction at the diplomatic level, within their competence and depending on the available capacities and resources, could contribute to:
   • facilitating and increasing the efficiency of communication and interaction on security of and in the use of ICTs, including by establishing conditions for direct dialogue, inter alia, consultations between authorized agencies and experts;
   • strengthening stability and reducing the risks of misperception, outbreak and unintentional escalation of conflicts stemming from the use of ICTs.

7. The PoCs responsible for interaction at the technical level, within their competence and depending on the available capacities and resources, could carry out:
   • exchange of information on computer incidents within information resources under their responsibility and suppression of malicious activity emanating from their national information space;
   • assisting other States in responding to computer incidents and detecting threats to security of information upon receipt of a corresponding request;
   • exchange of data on existing and potential threats to security of and in the use of ICTs, as well as sharing best practices.

8. In the absence of objective possibilities to determine a technical PoC, a UN Member State may appoint any other authorized body during transition period to convey information to the national level and coordinate actions in order to resolve situations related to the use of ICTs. With a view to raising efficiency of computer incidents response, it is important to seek to appoint a technical PoC as such a body.

**Protocols and procedures of interaction between the PoCs**

9. Annex 2 defines the protocols and procedures of interaction between the PoCs, including the main areas and forms of cooperation, as well as the basic algorithm for the UN Member States’ actions in the event of a computer attack against their information infrastructure and / or a computer incident.
10. Annex 3 defines a basic list of information required to study a computer attack and a computer incident, which should be used in the event of tension and threat of conflict.

11. Upon receipt of an appropriate request from the affected party, the UN Member States will take the necessary measures within their scope of responsibility aimed at preventing and, if necessary, resolving interstate conflicts that may arise from the use of ICTs. Any subsequent cooperation and/or exchange of information are exercised on a voluntary basis.

**Technical specifications**

12. The United Nations Office for Disarmament Affairs will be responsible for maintaining and updating the PoCs Directory. The PoCs Directory may be posted on a specialized online portal under the UN auspices.

13. UN Member States will update contact information twice a year and notify of any changes no later than 30 days after they have been made. In the absence of access to Internet means, offline communication of relevant information should be made possible, for instance, through the means of diplomatic PoCs.

14. The PoCs Directory should be established before the end of the OEWG’s work in 2025 by a decision of the UN General Assembly. The directory will be deemed usable if 70% of the UN Member States appoint their PoCs.

**Financing**

15. No additional financial resources are required to establish and launch the proposed PoCs directory, since the exchange of information on security of and in the use of ICTs is carried out through already existing communication channels. Additional funding may be required if a decision is made to create a specialized online platform, as well as in the course of further activities of the PoCs directory.
### Annex 1

**Template for the global intergovernmental PoCs Directory at the UN**

<table>
<thead>
<tr>
<th>UN Member State</th>
<th>Point of Contact</th>
<th>Organization (webpage)</th>
<th>Email</th>
<th>Phone</th>
<th>Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Diplomatic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technical</td>
<td></td>
<td></td>
<td></td>
<td></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 respond to computer incidents, is appointed as a technical PoC.

3. Email 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 draft.

4. A contact phone number is indicated, which may not be tied to a specific person and through which a diplomatic or technical PoC can be contacted at any available time.

5. The languages spoken by contact persons for communication are indicated.
The procedure for interaction between the authorized bodies of the UN Member States on security of and in the use of ICTs

General provisions

1. The procedure is intended to determine the basic processes, scenarios, areas and forms of interaction between the national authorized bodies of the UN Member States (authorized bodies) on security of and in the use of ICTs.

Areas of interaction between authorized bodies

2. Authorized bodies may interact in the following areas:
   • exchange of data on existing and potential threats to security of and in the use of ICTs;
   • exchange of experience and provision of mutual advisory assistance;
   • suppression of malicious activity emanating from national information space and exchange of relevant technical information;
   • exchange of information on national legislation in the field of security of and in the use of ICTs, as well as open methodological manuals;
   • conducting bilateral and multilateral consultations at an appropriate level to reduce the possibility of misperception and conflict or either political or military tensions stemming from the use of ICTs, as well as to protect national information infrastructure, including critical infrastructure;
   • in other areas of mutual interest within the competence of national authorities.

Forms of interaction between authorized bodies

PoCs Directory

3. A PoC is contacted by sending a request through mutually agreed communication channels (email, phone or, if necessary, others), including diplomatic means. PoCs must ensure accounting and storage of information transmitted in the interaction, as well as establish conditions ruling out illegal access, amendments and modifications to such information or its disclosure.

4. To suppress malicious activity, the UN Member States affected by computer incidents should provide technical information on the incident, as comprehensive as possible, to the PoC of the Member State from whose territory the malicious activity
with the use of ICTs is assumed to have been detected. Exchange of information will be carried out on a voluntary basis and in conformity with the national legislation of the parties involved. For these purposes competent authorities may use standardized communication templates.

5. In the event of tensions and threat of conflict, exchange of information will be carried out in accordance with the list of basic information necessary to study a computer attack and a computer incident (Annex 3).

6. A PoC that has received a request for assistance in responding to a computer incident or a computer attack takes the necessary measures within its scope of responsibility (national segment of the Internet) in conformity with the national legislation (domestic regulations).

7. At the national level, Member States should ensure that there is adequate interaction between the PoCs to efficiently fulfill the tasks assigned to them.

8. If it is inappropriate to convey any information via the established communication channels, the PoCs use other possible information exchange channels by mutual agreement.

9. Information about the scope and nature of the interaction between the PoCs is confidential and shall be made public only by consent of all the PoCs involved in such interaction.

**Sequence of actions of a UN Member State whose information infrastructure is maliciously affected**

10. To mitigate the risks of misperception, escalation and conflict that may arise from the use of ICTs, the sequence of actions of UN Member States whose information infrastructure is maliciously affected includes two basic scenarios:

- malicious activity with the use of ICTs has not led to the risks of misperception, escalation and conflict, interstate interaction is carried out on a daily basis;

- malicious activity with the use of ICTs has caused tension in interstate relations, there is a risk of misperception, escalation and conflicts.
11. The first step is to define the technical details of a computer incident. It is carried out through interaction of technical PoCs by sending a request to the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected. Practice shows that most concerns can be addressed at this stage.

*Technical PoC – technical PoC interaction*

12. A UN Member State whose information infrastructure is maliciously affected evaluates a computer attack / a computer incident at the national level and collects all necessary information available for transmission.

13. Information, as comprehensive as possible, is transmitted to the technical PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected.

14. Upon receipt of information, the technical PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected:

- notifies the requesting side of its receipt as soon as possible, but no later than in 72 hours, and also evaluates the correctness and completeness of the data provided with the possibility of further clarification;
- if any measures need to be taken, informs of expected deadlines for their implementation;
- forwards information about the results of the measures taken to the requesting side.

*Technical PoC – diplomatic PoC interaction*

15. If there are objective reasons that impede interaction through technical PoCs, a UN Member State whose information infrastructure is maliciously affected evaluates the computer attack / computer incident at the national level and collects all the necessary information available for transmission.

16. The technical PoC of the Member State whose information infrastructure is maliciously affected sends as comprehensive information as possible to the national diplomatic PoC for subsequent transmission to the diplomatic PoC of the UN
Member State from whose territory, as the requesting side assumes, malicious activity with the use of ICTs was detected.

17. Upon receipt of information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected notifies the sender of its receipt as soon as possible and promptly transmits the relevant information to national authorized bodies.

18. Having received information on the implementation of the necessary measures and other relevant information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected, forwards the relevant information to the sender.

*Diplomatic PoC – diplomatic PoC interaction*

19. A UN Member State whose information infrastructure is maliciously affected evaluates of a computer attack / computer incident at the national level and collects all necessary information available for transmission.

20. The diplomatic PoC of the Member State whose information infrastructure is maliciously affected sends as comprehensive information as possible to the diplomatic PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected.

21. Upon receipt of information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected notifies the sender of its receipt as soon as possible and promptly transmits the relevant information to national authorized bodies, taking into account that the response time to the request should not exceed 15 days from the date of its receipt.

22. Upon receipt of information on the implementation of the necessary measures and other relevant information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected shall forward the relevant information to the sender.
**Consultation at the appropriate level**

23. If the first step does not result in easing tension or if the malicious activity with the use of ICTs has led to a risk of misperception, escalation and conflicts, further action may be taken as agreed by the parties involved, including bilateral and multilateral consultations at the appropriate level on security of and in the use of ICTs.

24. The format, venue and agenda of the meeting shall be agreed by the parties in advance through available channels of communication, i.e. through the PoCs or other mutually acceptable means.

25. In this case, diplomatic PoCs should take all necessary steps to de-escalate conflict or political or military tensions stemming from the use of ICTs, among which:
   - an initial assessment of the situation by the UN Member States whose relations are at risk of misperception, escalation and conflicts, including in collaboration with other national authorities. It is recommended to establish a correlation between the scale of incidents and the level of consultation required (expert, political, senior political, etc.);
   - establishment of communication between the diplomatic PoCs on conflict resolution or easing political or military tensions stemming from the use of ICTs;
   - determining the format, location and agenda for bilateral (if necessary, multilateral) consultations with the participation of interested parties;
   - assessment of the outcome of the meeting by the UN Member States whose relations have been at risk of misperception, escalation and conflicts, in order to determine next steps.

26. However, UN Member States should take into account that a conclusion on the involvement in malicious activity with the use of ICTs should be based on objective verifiable information. UN Member States will endeavour to take appropriate steps to reduce the likelihood of misperceptions and the potential for conflict or political or military tension stemming from the use of ICTs.

27. A general recommendation for the sequence of actions in the event of a malicious activity is that the discussion of a computer incident should raise to the
level of the diplomatic PoCs or national security and policy coordination bodies if all previous steps have failed.

**Developing cooperation**

28. This Procedure lays the basis for effective cooperation between authorized bodies, but is not exhaustive.

29. UN Member States may conclude additional agreements, memoranda or other documents to supplement and/or clarify the areas and forms of cooperation described in this document in order to facilitate cooperation.
Annex 3

List of basic information required to study a computer attack and computer incident (template)

The working language of requests may be specified by the States Parties of the exchange.

Lack of information on the above items is explicitly indicated.

**Computer attack**³ (CA) notification

1. Information on CA.
   
   1.1. Restrictive indicator of information disclosure contained in CA Notification according to the Traffic Light Protocol (TLP):
      
      1.1.1. TLP: WHITE – «disclosure» is not limited;
      
      1.1.2. TLP: GREEN – «disclosure» is limited to the competent authorities, which are not engaged in responding to CA;
      
      1.1.3. TLP: AMBER – «disclosure» is limited only to the competent authorities, which are engaged in responding to CA;
      
      1.1.4. TLP: RED – information is limited to recipient only.
   
   1.2. Description of the information security event.
   
   1.3. The measures expected of the addressee State.

2. The name of information resource (IR) targeted by the CA.

3. Category and type of CA.

   3.1. Breach or slowing down IR’s availability
      
      3.1.1. Denial-of-service (DoS) attack aimed at IR;
      
      3.1.2. Distributed Denial-of-Service (DDoS) attack aimed at IR.
   
   3.2. ICT-assisted information gathering
      
      3.2.1. IR scanning;
      
      3.2.2. IR traffic hijacking;
      
      3.2.3. Social engineering, aimed at compromising IR.
   
   3.3. IR intrusion attempts

---

³ Computer attack is a targeted impact on information resources aimed at compromising and/or disrupting their functioning and/or posing security threats to information processed by the objects; the sources of which have network address originating from the Internet segment of the addressee State.
3.3.1. Exploit attempts;
3.3.2. Login attempts.

3.4. Malware distribution
   3.4.1. Malware infection attempt;
   3.4.2. Malware C&C;
   3.4.3. Malware infrastructure.

3.5. Fraud
   3.5.1. Phishing.

3.6. Abusive content
   3.6.1. Spam.

3.7. Other (CA which do not fall into any of the given categories).

4. Date and time of CA beginning (UTC+0).

5. Date and time of CA ending (UTC+0).

6. Technical data on the targeted IR
   6.1. IPv4-address of IR
   6.2. IPv6-address of IR
   6.3. IR’s IP route subnet addresses (in the CIDR format)
   6.4. IR-associated domain name
   6.5. IR’s URI address
   6.6. IR-registered e-mail address
   6.7. Attacked Autonomous System Number (ASN)
   6.8. Attacked network service, network port and protocol
   6.9. Exploitable vulnerabilities

7. Technical data on CA source
   7.1. IPv4-address (routable)
   7.2. IPv6-address (routable)
   7.3. Domain name
   7.4. URI-address
   7.5. Email-address
   7.6. Malicious Autonomous System Number (ASN)
7.7. Information on malware modules

7.7.1. Hash value of the malware module;

7.7.2. Antivirus software verdict, name of the relevant antivirus software (if the malware module is identified).

8. Additional information on CA, including CA network traffic, malware modules, electronic images of e-mails, log files of the attacked network services, log files of the information protection tools, log files of the telecommunications equipment, etc.

9. Information describing connections of CA to the addressee State.

**Computer incident** (CI) notification

1. Information on CI.

   1.1. Restrictive indicator of information disclosure contained in CI Notification according to the Traffic Light Protocol (TLP):

      1.1.1. TLP: WHITE – «disclosure» is not limited;

      1.1.2. TLP: GREEN – «disclosure» is limited to the competent authorities, which are not engaged in responding to CI;

      1.1.3. TLP: AMBER – «disclosure» is limited only to the competent authorities, which are engaged in responding to CI;

      1.1.4. TLP: RED – information is limited to recipient only.

   1.2. Description of the information security event.

   1.3. The measures expected of the addressee State.

2. Name of information resource (IR).

3. Category and type of CI.

   3.1. Dissemination of abusive content

      3.1.1. Spam-bombing from the IR.

   3.2. Breach or slowing down IR’s availability

      3.2.1. Denial-of-Service (DoS) attack aimed at IR;

      3.2.2. Distributed Denial-of-Service (DDoS) attack aimed at IR.

---

4 Computer incident is a fact of violation and / or termination of an information resource functioning and / or a violation of security of information processed by such a resource, including those resulted from a computer attack.
3.2.3. IR traffic hijacking.

3.3. ICT-assisted fraud
   3.3.1. Use of IR for unauthorized purposes;
   3.3.2. Phishing.

3.4. Breach of information content security
   3.4.1. Unauthorized access to the IR-processed information;
   3.4.2. Unauthorized modification of the IR-processed information.

3.5. System intrusion
   3.5.1. IR’s application compromise;
   3.5.2. IR’s account compromise.

3.6. Malware infection
   3.6.1. Infection of the IR with malware modules.

3.7. Malware distribution
   3.7.1. Use of IR for malware command and control;
   3.7.2. Use of IR for malware distribution.

3.8. Other (CI which do not fall into any of the given categories)

4. Date and time of CI identification (UTC+0).

5. Technical data on the IR engaged in CI.
   5.1. IPv4-address (routable) of IR
   5.2. IPv6-address (routable) of IR
   5.3. Subnet of the IR (in the CIDR format)
   5.4. Domain name associated with IR
   5.5. URI-address
   5.6. Registered e-mail address
   5.7. Attacked Autonomous System Number (ASN)
   5.8. Attacked network service, network port and protocol
   5.9. Exploitable vulnerabilities

6. Technical data on the source of malicious activity, involved in CI, from the Internet segment of the addressee State.
   6.1. IPv4-address (routable)
6.2. IPv6-address (routable)
6.3. Subnet of the routable network addresses (in the CIDR format) involving the sources of malicious activity
6.4. Domain name associated with the malicious activity source
6.5. URI-address
6.6. Email-address
6.7. Malicious Autonomous System Number (ASN)
6.8. Information on malware modules
   6.8.1. Hash value of the malware module;
   6.8.2. Antivirus software verdict, name of the relevant antivirus software (if the malware module is identified).
7. Additional information on computer incident, including the records of network traffic of malicious activity, malware modules, electronic images of e-mails, log files of the targeted network services, log files of the information protection tools, log files of the telecommunication equipment, etc.