In the Name of God, the Merciful, the Compassionate

"Functional equivalence as an essential element for effective functioning of POCs"

Concept paper of the Islamic Republic of Iran

November 22, 2022

Background

During the first OEWG, States concluded that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a helpful measure for the implementation of many other CBMs, and is invaluable in times of crisis.[1] States also concluded that the prior existence of national and regional mechanisms and structures, as well as the building of adequate resources and capacities, such as national Computer Emergency Response Teams (CERTs), are essential to ensuring that CBMs serve their intended purpose.[2]

At the first annual progress report of the OEWG, States agreed to establish a global, intergovernmental, points of contact directory on security in the use of ICTs at the diplomatic and technical levels for enhancing interaction and cooperation between States and to engage in further focused discussions on the development of such a directory at the fourth and fifth sessions of the OEWG, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building.[3]

Essential requirement

The need for capacity building has been firmly established in previous and current OEWG. By its 2021 report, OEWG agreed that Capacity-building plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs.[4]

[1] - 2021 OEWG report, para 47.
[2] - 2021 OEWG report, para 46.
[3] - Annual progress report, Section E, Recommended next steps, para 2.
[4] - 2021 OEWG report, para 54.

While establishing a global, intergovernmental, points of contact directory is essential to promote an open, secure, stable, accessible and peaceful ICT environment, its operationalization may not immediately be possible, in particular for developing countries, until they acquire adequate capacity.[5]

States can only implement expected roles and responsibilities of PoCs, especially at the technical level, if they have the required technologies and technical capacity to address serious ICT incidents (for example to detect, investigate, prevent, alert and respond to incidents) to then cooperate and communicate with the appropriate points of contact in other countries.

We deem necessary to build the work of the PoCs directory within the UN on the basis of functional equivalence, meaning that, regardless of whether they are located in a developing or developed State, they must function with an equivalent degree of effectiveness.

To achieve functional equivalence for PoCs and to adapt them to the fast-moving ICTs context, developing States need to acquire capacity through technology transfer and capacity-building measures to ensure that they have the necessary technical and technological capabilities to set up strong, well-functioning and adequately resourced PoCs.

Without prior capacity building measures, difficulties may arise from the fact that some PoCs may have not the capabilities to carry out their functions with respect to increasingly complex and sophisticated issued related to ICTs security and provide an effective mechanism for dealing with the broad range of existing and potential threats. Therefore, capacity building arises as a prerequisite and essential tool before establishing and operationalizing a global, intergovernmental points of contact directory on security in the use of ICTs, especially at the technical level.

Capacity building ACTION PLAN on PoCs

Recognizing the above mentioned need and prerequisite, States could elaborate, at the fourth session of the OEWG, a Capacity Building Action Plan on PoCs which will cover the period 2023-2025.

[5] - Based on 2015 GGE report, para 14.

The Action Plan will sets out concrete capacity building measures to assist developing States in setting up strong and well-functioning PoCs so as to foster functional equivalence.

Capacity building measures can take the form of activities (workshops, training courses, table top exercises, webinars, technology transfer etc.) and the development of tools (papers, guidelines, standard operating procedures (SOPs), databases, etc.).

Working principles of the global, intergovernmental PoCs directory

- Since cyber-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 cooperation between relevant state authorities including through PoCs Directory;[6]

- Although all states must behave responsibly in/on cyberspace, they have common but differentiated responsibilities (CBDR) based on their different levels of ICT capabilities (Digital Gap);

- PoCs should be governed by functional equivalence, meaning that, regardless of whether they are located in a developing or developed State, all PoCs should be able to function and fulfil their mandate with an equivalent degree of effectiveness.

- States may, on a voluntary basis, provide points of contact at the diplomatic and technical levels;[7]

- The Directory will consist of relevant points of contact from all United Nations member States and will be available to them only;[8]

- Each country's input to the Directory will be unique, and reflect their domestic circumstances. Some countries may list multiple agencies under one function, others may only list one for each function, while others may provide one single coordination point of contact. If a country prefers communications to be initiated

[6] - Russian concept paper, preamble, para 3.
[7] - Annual progress report, Section E, para 16 (b).
[8] - Based on ASEAN Directory.

through a particular channel or organization, this should be noted in its entry to the Directory;[9]

- Each country will determine their respective point of contact for each specific ICT security incident, taking into account the technical details and possible consequences;[10]

- Given that ICT incidents can emanate from or involve third States, it is understood that notifying a State about malicious cyber activity emanating from its territory or cyber infrastructure, does not imply responsibility of that State for the incident.[11] It is particularly important given the fact that many cyber-attacks are carried out under "false flag".[12]

- Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein;[13]

- Notification from an affected State must be made in good faith and should be accompanied with all relevant supporting information. Supporting information may include sharing possible Indicators of Compromise (IoCs), such as IP address and computers used for malicious ICT acts and malware information;[14]

- A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond, is not responsible based on principle of common but differentiated responsibilities (CBDR) and should be assisted by technology transfer and forensic tools to combat the ICT malicious activities;

- States will be guided in the implementation of the functions of the PoCs Directory by a firm commitment to the principles of non-interference in the internal affairs of States, national self-determination, States territorial sovereignty and national jurisdiction over their cyberspace a fortiori all its elements and their equality in the Internet governance, to international law and to the observance of fundamental human rights and freedoms;[15]

---

[9] - Based on ASEAN Directory.
[10] - Based on ASEAN Directory.
[11] - Based on 2021 GGE report, para 30 (d).
[12] - Russian concept paper, preamble, para 4.
[13] - 2021 GGE report, para 30 (c).
[14] - 2021 OEWG chair's summary, page 11, Canada proposal,
[15] - Based on Russian comment on OSCE CBMs.

- Despite international situation, the PoCs will preserve political neutrality, maintaining interaction with other PoCs on addressing threats to security of and in the use of ICTs;[16]

- The PoCs and their resources should not be subject to restricting and blocking measures, including unilateral coercive measures (UCMs);[17]

- The PoCs will opt for pragmatic interaction on addressing existing and potential 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;[18]

- In their activities PoCs should take into account the recommendations elaborated by the OEWG.[19]

- Member States will update contact information annually and notify changes no later than thirty days after a change has occurred;[20]

- Any information exchanged will be voluntary and in line with the respective domestic policies and circumstances of the States;[21]

- States involved in the information exchange will only share that information with third parties by mutual consent;[22]

- 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 disclosure of such information;[23]

- States should ensure high levels of security of the focal points contact database;[24]

- Contact details of focal points to be stored in a secure database with the Secretariat;[25]

[16] - Russian concept paper, section of working principles of the PoCs directory, para 2.
[17] - Russian concept paper, section of working principles of the PoCs directory, para 3.
[18] - Russian concept paper, section of working principles of the PoCs directory, para 4.
[19] - Based on Russian concept paper, section of working principles of the PoCs directory, para 5.
[20] - Russian concept paper, section of description, para 3.
[21] - ASEAN PoCs directory.
[22] - ASEAN PoCs directory.
[23] - Russian concept paper, section of description, para 2.
[24] - HD PoCs directory.
[25] - Based on HD PoCs directory.

- The decision on how to respond to communications received via the Directory and the content to be communicated will be determined by each country. Any subsequent cooperation and/or information sharing will proceed according to mutual consent;[26]

- Information may be submitted by the States in any of the official UN languages, accompanied by a translation in English, or only in the English language;[27]

- With respect to the activities of PoCs Directory, States will take into account the needs and requirements of developing States taking part in such;[28]

- Information exchange, when occurring between States, should use appropriately authorized and protected communication channels;[29]

- In the elaboration of PoCs directory, due regard should be paid to the requirement of protecting confidential information and data.

[26] - ASEAN PoCs directory.
[27] - OSCE Directory.
[28] - OSCE Directory.
[29] - OSCE Directory.