Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures

Samuele Dominioni

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study is part of UNIDIR's Security and Technology Programme cyber workstream, which is funded by the Governments of Czechia, France, Germany, Italy, the Netherlands, Switzerland, the United Kingdom, and by Microsoft. The author wishes to thank the following individuals for their invaluable advice and assistance on this report: Giacomo Persi Paoli, Alisha Anand, Andraz Kastelic, Moliehi Makumane, Wenting He and Harry Deng of UNIDIR, Katherine Prizeman, Hermann Lampalzer, and Erika Kawahara of UNODA, and all the anonymous experts and practitioners who took part in the interviews and the survey.

Design and layout by Trifecta Content Studio.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

THE AUTHOR

Dr. Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and IMT School for Advanced Studies, Italy.

TABLE OF **CONTENTS**

Executive Summary

This report has two main purposes. First, it supports further substantive deliberations and facilitate the progress of the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security by elaborating possible options and practical recommendations for establishing an effective global directory of Points of Contact (PoC) on security in the use of ICTs. Second, it serves as a reference study on procedures, parameters, and practices (including lessons learned) of existing PoC directories and networks in the field of disarmament and cyber.

The research project had two phases. In the first, the research focused on the analysis of selected existing PoC directories and networks in the field of disarmament and cyber, with a view to analysing how they work and how they are managed, and identifying good practices as well as recurrent challenges. The second phase built on those findings with a survey distributed to all Member States to learn their preferences regarding key elements relevant to establishing a directory of points of contact in the context of international ICT security.

The first phase of the research identified six good practices (see section 3.6) for the establishment and management of PoC directories and networks, which include:

1. **Keep the directory updated.**
   If the secretariat has the capacity/mandate, it should reach out to State members or parties to ask for updates (as PoC contact details may be out of date) on a regular basis or set a time frame for States to send updates.

2. **Engage regularly with PoCs.**
   A few secretariats conduct 'ping' tests, which measures the time needed for a PoC to respond to an activation/test message, or other communication exchange exercises

3. **Guide national authorities.**
   To help the States smoothly manage their PoCs, the legal basis that establishes the PoC network should clearly indicate the expected functions of the PoC at the domestic level and possibly state the language requirements.

The second phase of the research identified key characteristics concerning several important aspects for the establishment of a global directory of PoC in the context of international ICT security. Overall, the results of the survey (see section 4) are in line with what is currently discussed at the OEWG and suggest additional elements to be taken into consideration by member states (see section 5).

Finally, this report identifies three general and key foundational aspects that should be taken into consideration for the effective functioning of any PoC directory (see section 5.3).

1. **A clear understanding of PoC functions and roles.** If these aspects are covered and detailed from the outset, Member States might have a better sense of where to structure it and of the capacities needed to equip the PoC at the domestic level.

2. **A clear mandate and resources** for the secretariat, especially concerning its responsibilities and duties regarding the key and sensitive tasks of receiving States' nominations or updates for their PoC (including verifying such information), and assisting Member States with capacity-building.

3. **A clear understanding of how often and for what purposes** Member States use the PoC directories. The research for this project revealed that often secretariats do not have data to assess if the directory they maintain is used by members. Having such information would be important for improving the efficiency of this confidence-building measure.

1. Introduction

Direct communication between Member States is key for maintaining stability and peace in the international community. Indeed, over the last decades, systems for information exchange, such as Points of Contact (PoCs), have allowed Member States to de-escalate potential crises in various domains and to build confidence.[1] With the increased relevance of cyberspace for international peace and security, direct communication channels would also be beneficial in this domain. In fact, threats coming from cyberspace show peculiar characteristics, making them difficult to be mitigated unilaterally by Member States. Indeed, malicious cyber activities that may pose a threat to international security are often transnational, taking place in an opaque environment, and their attribution is challenging. As such, misunderstanding and miscalculation of malicious information and communication technologies (ICT) activities may lead to rapid escalatory responses, thus endangering international stability and peace.

The establishment of PoCs for international cybersecurity is currently gaining momentum after its first appearance in the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013.[2] Since then all subsequently agreed reports, including the substantive report of the 2021 Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, further referred to the relevance of PoCs in the cyber domain underlining that "establishing national Points of Contact (PoCs) is a CBM [confidence-building measure] in itself, but is also a helpful measure for the implementation of many other CBMs, and is invaluable in times of crisis".[3] In the current OEWG on security of and in the use of ICT 2021–2025, there is consensus among Member States toward establishing a global directory of PoC in the field of CBMs.[4]

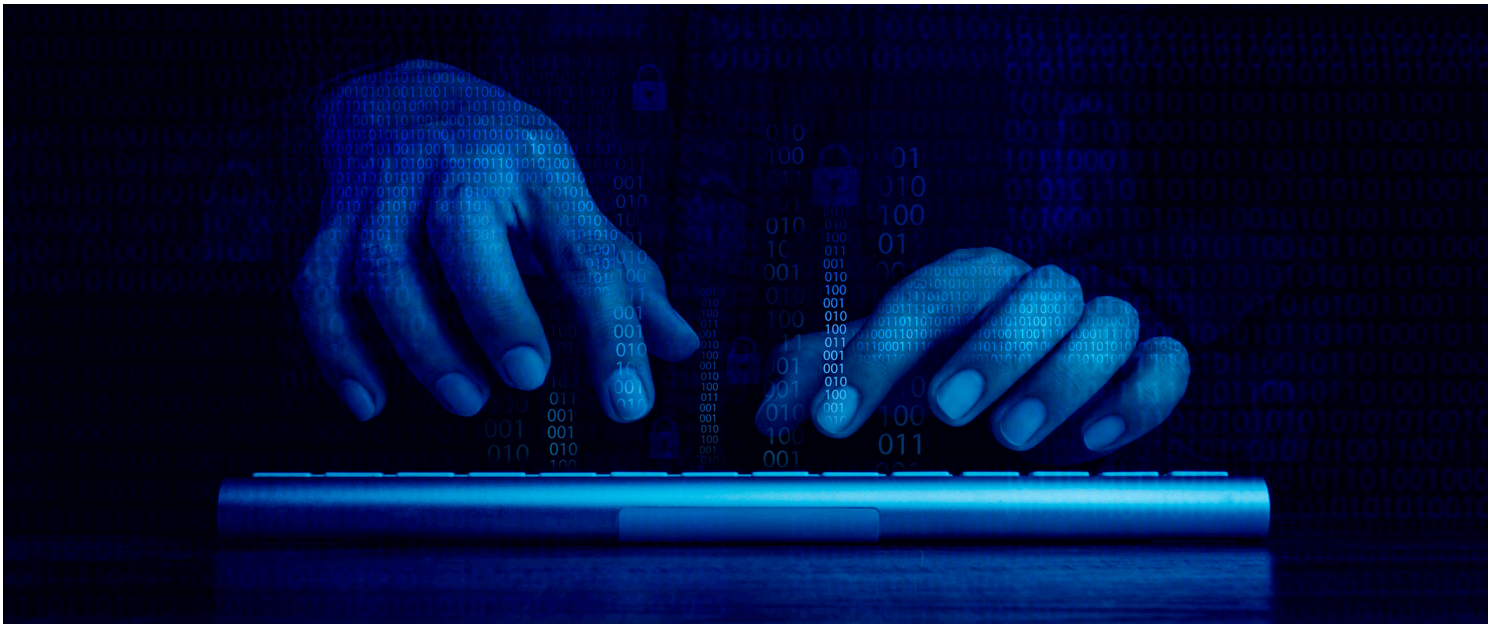
---

[1] See, for example, Steven E. Miller. 2020. "Nuclear Hotlines: Origins, Evolution, Applications". Stanley Center for Peace and Security. Available at https://stanleycenter.org/publications/nuclear-hotlines/.

[2] "States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms". See General Assembly. 2013. Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Document A/68/98, para. 26(c).

[3] General Assembly. 2021. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/75/816, para. 47.

[4] General Assembly. 2022. Report of the Open-ended Working Group on Security of and in the use of Information and Communications Technologies 2021–2025. UN document A/77/275, p. 12.



2. Purpose and Structure of the Report

The main purpose of this report is to support further substantive deliberations and facilitate the progress of the OEWG by elaborating possible options and practical recommendations for establishing an effective global directory of PoCs on security in the use of ICTs. Moreover, at the time of writing, there are no studies or analyses on how these PoC directories and networks work or are managed; therefore, this report may also serve as a reference study on procedures, parameters, and practices (including lessons learned) of existing directories and networks in the field of disarmament and cyber.

The research project had two phases. In the first, the research focused on the analysis of selected existing PoC directories and networks in the field of disarmament and cyber, with a view to analysing how they work and how they are managed, and identifying good practices as well as recurrent challenges. The second phase built on those findings with a survey distributed to all Member States to learn their preferences regarding key elements relevant to establishing a directory of points of contact for cyber CBMs.

This report is structured as follows: the following section explains the methodology and the results of the first phase of the research project. Subsequently, the fourth section presents the findings of the survey. Finally, the fifth section contextualizes the research results within the ongoing discussion at the OEWG and proposes some recommendations for the establishment, maintenance, and further development of a PoC directory in the field of cyber CBMs.

3. Review of Existing PoC Directories

The PoC directories and networks[5] are well-established mechanisms adopted in several fields (including disarmament and crime) by organizations, conventions, and treaties at the international and regional levels. This report does not assess or evaluate the effectiveness of PoC directories included in this research.

The selection of existing PoC directories was made based on criteria of relevance and information available. The selection constitutes the dataset for the case study analysis.[6] The following PoC directories (in alphabetical order) have been included in the research:

1. Arms Trade Treaty—National Points of Contact
2. ASEAN-Japan—Cybersecurity Points of Contact
3. Convention on Cluster Munitions—National Points of Contact
4. Council of Europe—The Budapest Convention 24/7 Points of Contact
5. G7—24/7 Network Points of Contact
6. INTERPOL—Cybercrime Points of Contact
7. OAS-CICTE—Working Group on Cooperation and Confidence-Building Measures in Cyberspace, Points of Contact
8. OSCE—CBMs to Reduce the Risks of Conflict Stemming from Use of ICTs, Points of Contact
9. UNODA Biological Weapons Convention—National Points of Contact
10. UNODA Programme of Action on Small Arms and the International Tracing Instrument—National Points of Contact

[5] A directory usually consists of a list of contact details of points of contact. A network is usually a more structured system, which may imply the establishment of dedicated and secured channels for communication. Nevertheless, no commonly agreed definitions exist for these concepts, and they are often used interchangeably. For the purpose of readability in section 3 of the report any use of 'directory' should read as 'directory/network'.

[6] This phase of the research project relied on three distinct research methods corresponding to three different research steps. The first step relied on desk research of the existing PoC directories in the field of disarmament (and other cyber-related fields, such as fighting cybercrime). The second step concerned targeted structured interviews with experts and practitioners involved in the selected PoC directories. The interviews provided insights into how these directories are established, maintained, and managed, and what challenges and lessons have been learned. Overall, 10 interviews were carried out from March to June 2022. The third step concerned the identification of key parameters relevant to the establishment and maintenance of PoC directories, plus the main challenges and lessons learned. These parameters constitute the focus of the empirical analysis of the PoC directories.

Each of the selected PoC directories and networks was analysed according to key parameters, including:

1. establishment and purpose of PoCs;
2. key characteristics of the PoC (typology, position in the national framework, language);
3. secretariat role and capacities (dedicated body, staff, budget);
4. the directory (location, access, cybersecurity, updates);
5. main challenges; and
6. good practices and lessons learned.

The following subsections are structured according to the identified parameters. For each of them, the report provides an empirical analysis with aggregated data from the selected PoC directories.[7]

3.1 Establishment and Purposes of the PoC

The creation of a PoC directory is normally mandated by a decision taken by an authoritative political body (e.g., a general assembly, or a working group on specific matters), and it is usually composed of the States members or parties of the organization, convention, or treaty.

The authoritative body can establish the PoC directory through formal or informal processes. A formal process implies the adoption of a document with a formal decision requesting States to nominate PoCs and to create a dedicated directory. The document often specifies the central body (secretariat) responsible for the maintenance of the directory. The informal process refers to a decision taken informally by all or some of the States to establish a PoC directory without the adoption of a formal document.

Figure 1: What kind of decision was made to establish the directory?

The review of existing PoC directories shows that most of them have been established through a formal process (8 out of 10). In some cases, the provision to create a PoC directory is included in the founding document of the convention or treaty.

[7] Some information concerning the PoC directories is not retrievable from open sources. Therefore, to ensure the confidentiality of the information gathered through the interviews, we opted for an anonymized analysis.

Another key element to consider in the establishment of a PoC directory is its purpose. There are four main tasks the PoC may fulfil: communication, assistance in cooperation, reporting, and national coordination. **Communication** refers to relevant information exchange among PoCs (horizontal exchange) and with the secretariat (vertical exchange). **Assistance in cooperation** refers to operational, technical, or legal assistance that States may require from another State. **Reporting** concerns submitting scheduled reports (e.g., annual reports) to the secretariat concerning information or activities that States may be required to report about. PoCs can also serve as **national coordination** points for activities that involve multiple agencies or institutions at the domestic level.

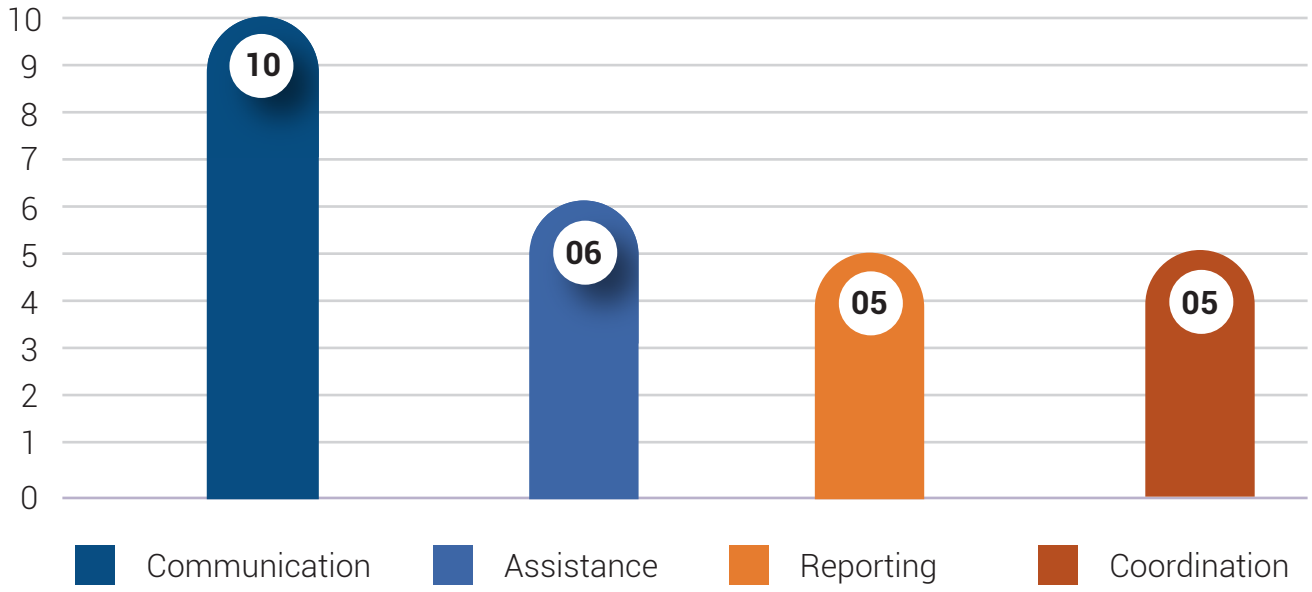


Figure 2: The purposes of the Point of Contact

The most common task for PoCs is communication (all 10), followed by assistance (6 out of 10) and reporting (5) and coordination (5).

Finally, the nomination of a national PoC to include in the directory may be mandatory or voluntary.

Figure 3: Requirement for member states to establish the PoC.

In general, the establishment of a national PoC is requested in a binding convention or treaty (3 out of 10).

3.2 Key Characteristics of the PoC

This section looks at key parameters for the PoC at the domestic level. In particular, it takes into consideration provisions regarding the typology, the position in the national framework, and language requirements.

In terms of typology, the research follows the classification expressed in the last OEWG Annual Progress Report, which outlined two different types of PoC: **diplomatic** and **technical**.[8] It should be underlined that a directory may request/recommend the establishment of both.

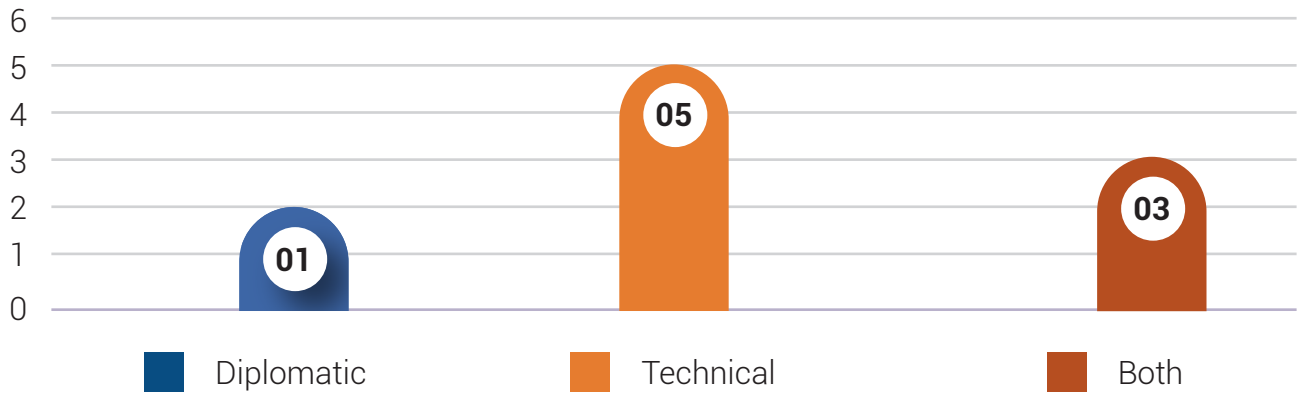


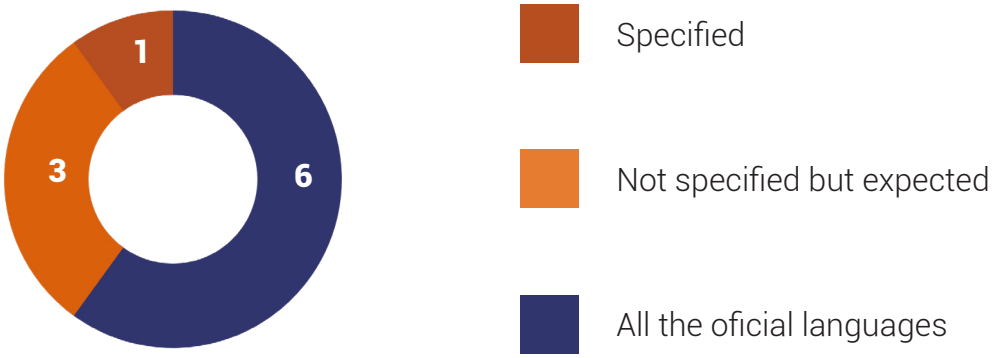
Figure 4: Typologies of PoCs

Among the selected case studies, there are more directories with solely technical PoCs (5 out of 10) than those that have both or only diplomatic (2 out of 10). One of the reasons is that the PoC is often established in the framework of international instruments or organizations with specific aims and objectives. Therefore, at the domestic level, the choice is usually a specialized authority.

Another aspect regarding the PoC concerns its **location within the national framework**—in particular, the existence of provisions at the international level concerning its institutional setting (e.g., the PoC should be established within a specific ministries). The empirical analysis shows that there are no directories that specify the location of the PoC at the national level. It is left to each State to identify the position of the PoC in its national framework.

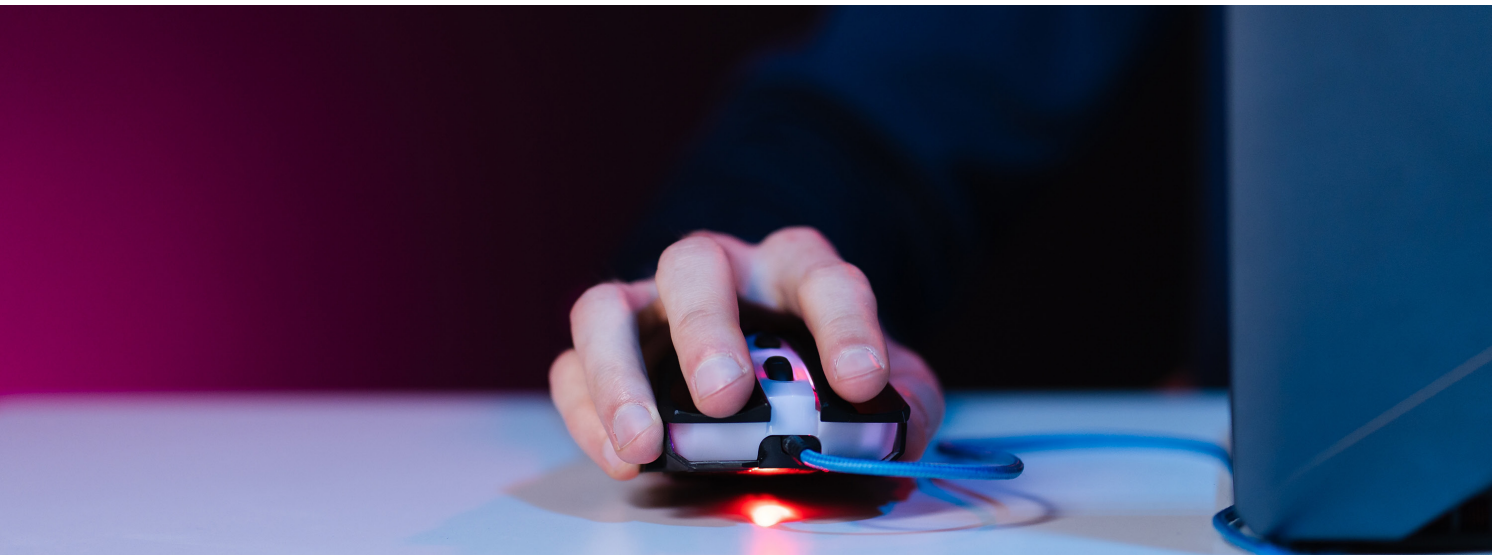
The last parameter analysed is the **language requirement**. Considering the different languages spoken across countries and regions, having a defined or at least an expected language across the PoCs might ease communication.

Figure 5: Languages requirements for PoCs



[8] There is no agreed definition of the term 'technical'. For the purposes of this research, the term refers to PoCs established within agencies or departments with technical or legal expertise (such as a computer emergency response team, or the cybercrime unit of a law enforcement agency).

Most of the directories work with all official languages recognized by the convention, treaty or organization (6 out of 10); in case a language is not specified, there is a general expectation that English is the language for communication (3 out of 10).



3.3 Secretariat Roles and Capacities

For the purpose of this study, the term 'secretariat' refers to any administrative body that, at the multilateral level, is tasked with responsibilities concerning the management of a PoC directory. In some cases, the secretariat is a permanent office within an international/regional organization, and in others, it is an external implementation unit. This research looked at three main topics concerning secretariat roles and capacities: i) **the responsibilities of the body**; ii) **the presence of dedicated staff**; and iii) the availability of a **dedicated budget** for the activities related to the management of the PoC.

In terms of **responsibilities and activities of the body**, the empirical analysis revealed that in terms of management of the PoC the secretariat is tasked with a diversified portfolio that can be grouped into the following categories:

- **information management** (among and with State members or parties and other stakeholders);
- **maintenance and support of the PoC directory** (including updating the PoC directory);
- **capacity-building for the PoC** (including training);
- **organization of meetings** (with the PoCs or with other directories); and
- **exercises or communication checks** (including 'ping' tests).[9]

[9] The ping test originated in the ICT sector and its goal is to measure the minimum amount of time to send the smallest possible amount of data and receive a response. In the context of a PoC directory, the ping test measures the time needed for a PoC to respond to an activation/test message.

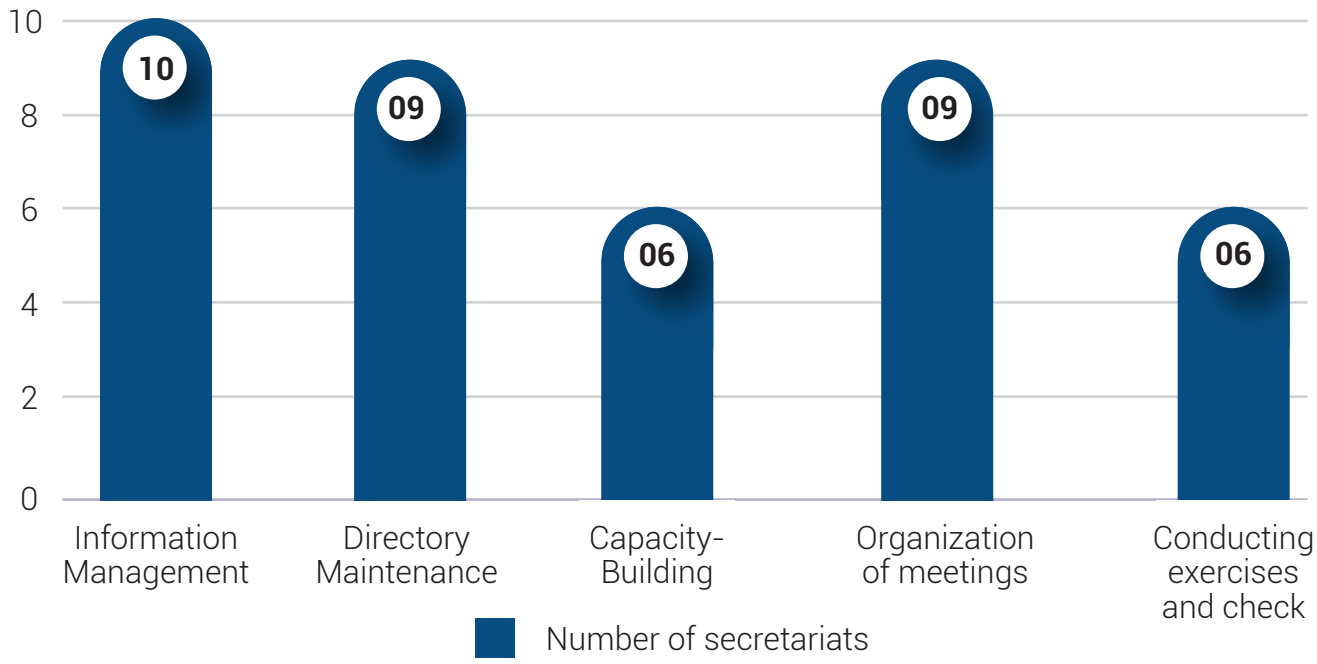


Figure 6: Responsabilities and activities of the Secretariat

As figure six shows, all 10 secretariats hold responsibilities related to information management, and almost all of them maintain the PoC directory and organize meetings (in both cases 9 out of 10).

Another parameter for the secretariat is the **presence of dedicated staff** tasked with the management of the PoC directory. Most secretariats have staff or personnel that oversee the management of the PoC directory as part of their duties. The average number of people working in the secretariat on this duty is two. In the case of specific or ad hoc tasks (such as comprehensive updates of the directory), a few of the secretariats hire dedicated temporary personnel (e.g., consultants).

Finally, this section includes an analysis of the allocation to the secretariat of a **specific budget** for the management and maintenance of the PoC directory.

Figure 7: Budget for maintaining the directory of PoC

It is noteworthy that, among directories with a dedicated budget, in most of the cases (3 out of 4) it comes from voluntary contributions from States and organizations.

3.4 The Directory

The information regarding PoCs across States members or parties is often stored in a common directory. This is usually kept by the secretariat, which makes it available to States for consultation and, in some cases, updates.

There are multiple methods in which the directory can be preserved, accessed, and updated. This research identified four main parameters regarding the maintenance of a directory: location, accessibility, cybersecurity, and updates.

In terms of location, there are two methods to preserve the directory: online and offline.

Figure 8: Location of the directory

Directories stored online (6 out of 10) can further be categorized according to whether they are found in a specific section of the website of the organization/convention/treaty or on a dedicated and external website. Most directories stored online (4 out of 6) are found in a section of a pre-existing website. Directories stored offline usually consist of an electronic document that is shared directly by email among States members or parties.

It is noteworthy to mention that over the years there has been an increase in the number of directories stored online. Conversely, this research did not register any case of directories being converted to an offline mode.

The second parameter under analysis is the **accessibility of the directory**. Within this parameter, the research considered the following elements: the public/restricted availability of the directory, and, in case it is restricted, how the directory is made accessible.

In terms of public/restricted availability, most of the directories are restricted. Only one directory out of the 10 analysed have information publicly available online (this is the National Points of Contacts directory on the implementation of the Programme of Action and the International Tracing Instrument managed by UNODA).[10]

[10] Available at https://smallarms.un-arm.org/national-contacts.

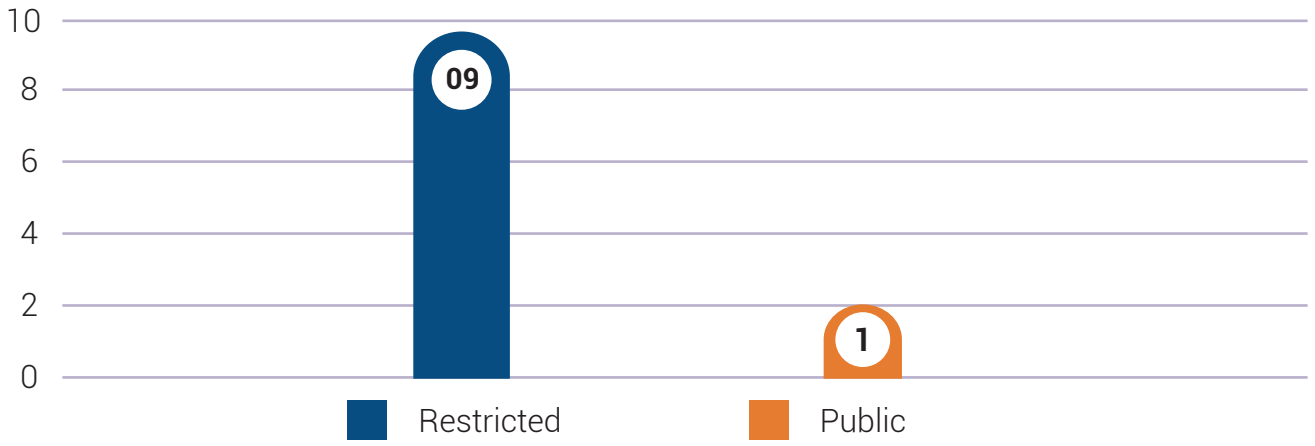


Figure 9: Accessibility of the directory

The accessibility of restricted directories is determined by its location. Directories stored online usually have a restricted area accessible only by authentication. For the directories stored offline, the secretariat relies on the distribution of the directory document through verified emails.

The third parameter pertains to the **security policies/practices** in place, particularly concerning the cyber domain. Here it is also necessary to split the analysis of the directories according to their location and how they are made accessible.

- For directories stored on pre-existing websites, the cybersecurity of the directory is usually managed by those in charge of the cybersecurity of the website. For example, the OSCE—CBMs to Reduce the Risks of Conflict Stemming from Use of ICTs, Points of Contact directory is stored in a restricted section of the polis.osce.org website.
- For directories stored on external websites, the cybersecurity is, in principle, entrusted to authorized third parties. For example, the UNODA Programme of Action and the International Tracing Instrument website is hosted by Amazon Web Service, which is endorsed and supported by the United Nations Office of Information and Communications Technology.
- For directories stored offline that are distributed by email, the secretariat sends the directory only to trusted and verified email accounts.

In terms of credentials to access online and restricted directories, the analysis of the different PoC networks revealed multiple options. For some directories, the secretariat implements personal credential policies (e.g., only PoC staff can access the directory, and each person has their individual credentials); for others, the secretariat opts for the policy 'one State—one password', and thus log-in details can be shared among selected offices or institutions of the State.

For the **updating of PoC directories**, the secretariats, which are often in charge of the maintenance of the directories, may adopt solicited or spontaneous update options. For solicited procedures, the secretariat usually sends reminders or expects regular updates concerning the PoC (e.g., when States members or parties submit their reports on a scheduled basis). The second option, spontaneous updates, permits States members or parties to send updates whenever there is a need. Nevertheless, most of the time the two methods overlap; States are reminded to submit updates for the PoC directory, and they can also do it spontaneously. In one of the cases under analysis, States may also decide to edit the information regarding the PoC by themselves, accessing their national profile page on the directory webpage.

3.5 Main Challenges

This section considers the different challenges reported by experts and practitioners in the interviews conducted for this research project. The challenges are ranked from most to least common.

1 **Obsolescence of PoC details.**
This is the most common challenge that interviewees reported. It is a systemic challenge—if the PoCs are not updated in the directory, the directory loses its utility.

2 **Lacking the capacity to establish a PoC.**
The challenge is two-fold. On one hand, there is the challenge of capacity-building, which some States might experience when setting up a PoC (e.g., having resources or technical skills); on the other hand, certain States might lack the political will to establish a PoC, especially for topics that are not considered a priority at the domestic level (e.g., cybersecurity).

3 **Non-responsive PoCs.**
There could be PoCs that are more active than others. The challenge might be particularly relevant when PoCs are not responsive for long periods. This situation can be considered a systemic challenge because it lessens the utility of the directory.

4 **Domestic management flaws.**
This can refer to several aspects concerning the national establishment and management of the PoC. Two recurrent issues are the lack of handover policies (thus when the incumbent in charge of the PoC leaves, the institutional knowledge is lost), and the lack of capacity or standing of the domestic PoC (because the role is covered by a junior staff member, or because it is located in a low-ranked institution or agency).

5 **Cyber and digital concerns.**
For online directories, cyber threats can pose a severe challenge to the integrity, availability, and confidentiality of data stored online. Because of this possibility, States might be reluctant to share their information on an online platform. Moreover, users might find certain platforms' interfaces unfit or not user-friendly, and therefore they might not engage with them.

6 **Suspicious updates.**
This can happen when State send updates to the secretariat through an unverified channel (such as an unknown email, or through a person or office that is usually not in charge of the PoC at the domestic level).

3.6 Good Practices and Lessons Learned

This section presents good practices and lessons learned that experts and practitioners working with PoC directories shared during the interview phase. The list of good practices and lessons

learned is organized following the challenges ranked in the previous section. The objective is to provide possible solutions to these challenges.

1 Keep the directory updated.

If the secretariat has the capacity/mandate, it should reach out to State members or parties to ask for updates (as PoC contact details may be out of date) on a regular basis or set a time frame for States to send updates. Furthermore, it is suggested that the secretariat may consider working with cooperative States to improve the system of updates expecting others to follow. It should also be clarified from the outset (i.e., in the moment of establishing the PoC directory/network) what information the secretariat must collect and what information security standards should be adopted.

2 Provide capacity-building and raise awareness.

To cope with the challenges regarding practical and political capacities, the secretariat, along with States or stakeholders, should assist and inform State members or parties of the establishment of the PoC at the national level. These activities may include technical assistance (e.g., connecting the PoC to specific channels or databases) and awareness-raising events (e.g., on the importance of CBMs for the cyber domain).

3 Engage regularly with PoCs.

A few secretariats conduct 'ping' tests, which measures the time needed for a PoC to respond to an activation/test message, or other communication exchange exercises with PoCs. As reported in the interviews with experts and practitioners, these might be a helpful way to keep the PoCs reactive and functioning.

4 Guide national authorities.

Each State may have distinct institutional settings and therefore PoCs may be set up within different frameworks. To help the States smoothly manage their PoCs, the legal basis that establishes the PoC network should clearly indicate the expected functions of the PoC at the domestic level and possibly state the language requirements. Moreover, the secretariat may provide guidance and training in terms of accessing the directory, sending updates and reports, and responding to requests coming from other States members or parties.

5 Invest in digital solutions and security.

Migrating to or establishing digital platforms is key to maintaining more functional and updated directories. In terms of cybersecurity there are multiple solutions, from establishing the directory within a pre-existing institutional website, to relying on third-party cybersecurity services. As previously stated, information security standards should be adopted to protect information shared by States. Another relevant aspect for digital directories is a user-friendly design of the platform to improve the user experience. Some secretariats reported that they shared the draft design of the digital platform with States and asked for feedback before implementing it.

6 Verify updates.

As a good practice to cope with the problem of suspicious updates received from unusual senders at the national level, the secretariat should double-check the contact information received with the minister of foreign affairs (including permanent missions) or relevant authorities of the State concerned.

Finally, the analysis of selected PoC directories reveals that there are different structures of PoC directories, which can be categorized as follows:

1 **Vertical directory.**
These are established mainly for the purpose of reporting to the secretariat about actions undertaken at the domestic level (e.g., concerning the implementation of certain provisions). In this case, PoCs are often acting as focal points for collecting information, drafting reports, and submitting them to the secretariat.

2 **Horizontal directory.**
These are established with the main aim of facilitating communication among States members or parties. In this case, PoCs are often tasked to be the first responders for requests and assistance from other members or parties (sometimes even from third parties). Horizontal directories can be set up with operational '24/7' PoCs.

3 **Mixed directory.**
In some cases, the directory is tasked with both vertical and horizontal responsibilities.

Having a clear understanding of the different categories of directories could be useful for further defining more operational characteristics of the directory in the field of cyber CBMs. Indeed, Member States might have different preferences on several parameters, such as the tasks and responsibilities of the PoC, the budget, or the contact details included in the directory.

4. Survey of Member States on the PoC Directory

This section provides an overview of the findings of a survey of national preferences for the establishment of the global intergovernmental directory of PoC in the context of international ICT security.[11]

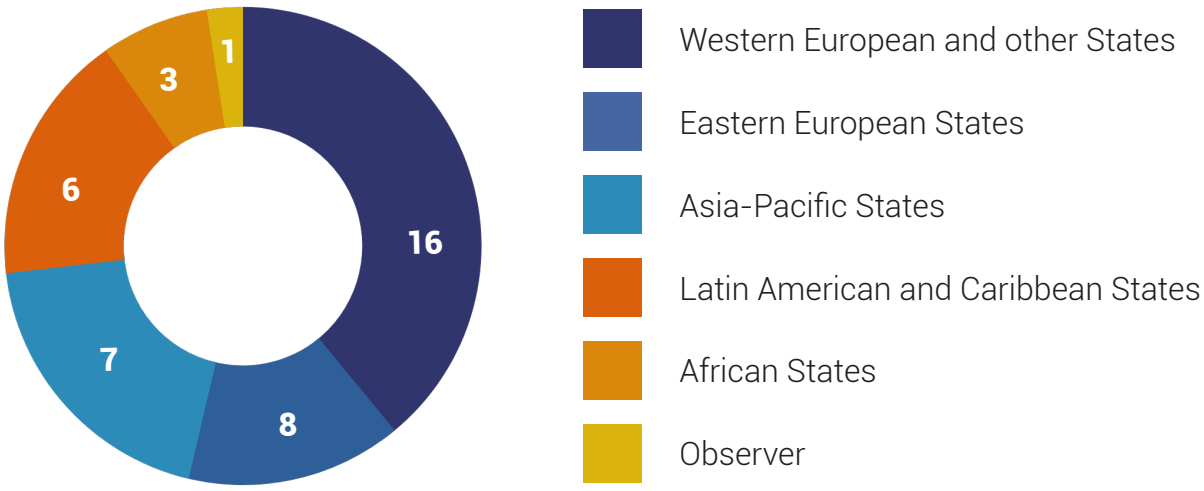


Figure 10: Regional Coverage of Respondents

In terms of the geographical distributions of the respondents, Member States from all regional groupings, with varying degrees, took part in the survey.

[11] The survey was launched on 30 August 2022 with a letter sent to all Member State missions to the United Nations in New York, and it remained open until 10 March 2023. During this period, 47 people from 41 Member States responded to the survey. For analytical purposes, only one answer per Member State was considered. In case of multiple and different responses from the same Member State, we reached out to the respondents and asked which answer to consider.

[12] The sections are built on those identified in the first phase of the research.

The survey was composed of 20 questions referring to the key parameters for the PoC directories, grouped into four sections:[12]

1. establishment of the directory and PoC;
2. key characteristics of the PoC (typology, functions, language);
3. secretariat role and capacities (responsibilities, staff, budget); and
4. the directory (location, contact details, updates).

The following subsections present the aggregated and anonymous results for each of the four sections.

4.1 Establishment of the Directory and the PoC

This section covers several foundational aspects of a global directory of PoCs, such as the relevance of the directory, how the international community should establish it, and what organ should be responsible for its establishment. It also covers one aspect concerning the establishment of the PoC itself, namely the obligatoriness for Member States.

Key findings:

- Most of the respondents (39 out of 41) reckon the establishment of a global directory of PoCs to be relevant—the majority of them, in fact, consider it to be essential (*see fig. 11*).
- In relation to how to establish the directory, the majority of the respondents prefer to have it established by a formal decision of an authoritative political body (*see fig. 12*).
- In relation to which body should establish the directory, there is a clear indication that the General Assembly should be the authoritative political body in charge of the establishment of a global directory of PoCs (*see fig. 13*).
- The establishment of PoCs at the national level should remain voluntarily (*see fig. 14*).

Figure 11: How important is the establishment of a global directory of PoCs?

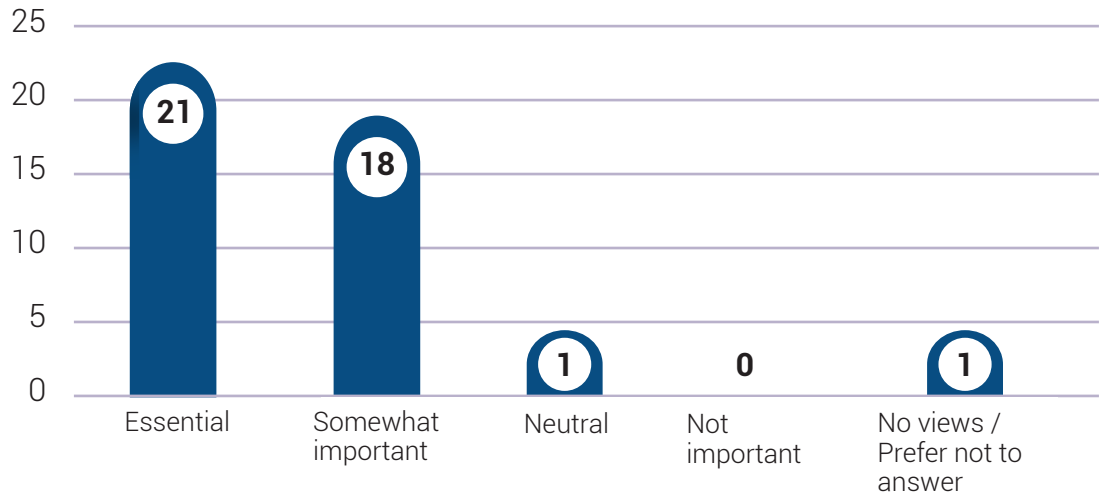


Figure 12: How should the establishment of the PoC network and directory take place?

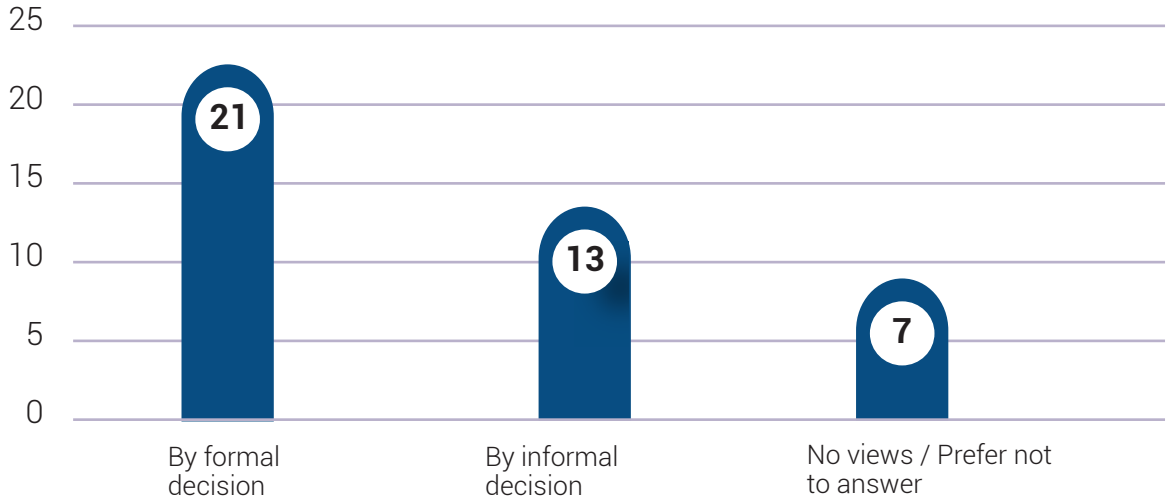


Figure 13: Which body should be responsible for mandating such establishment?

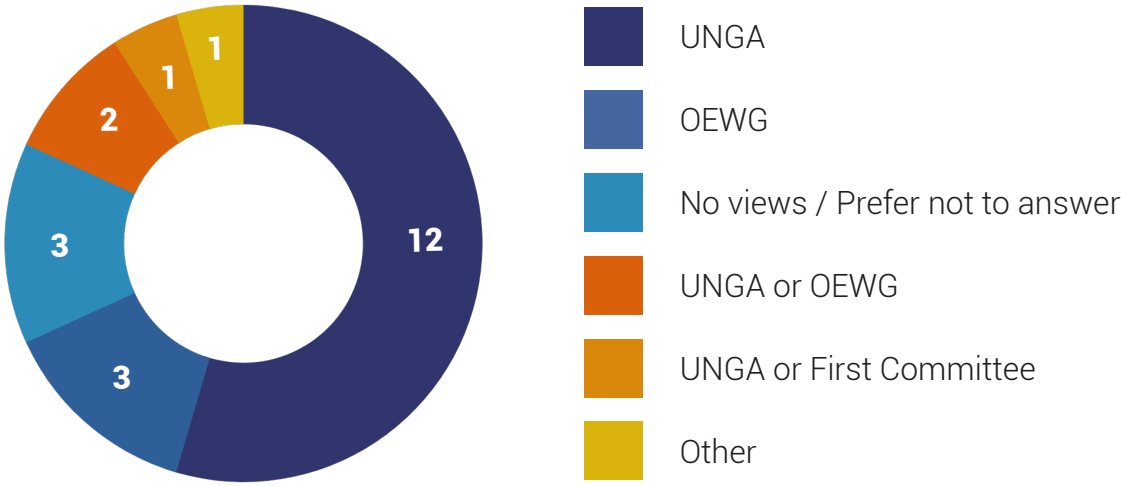
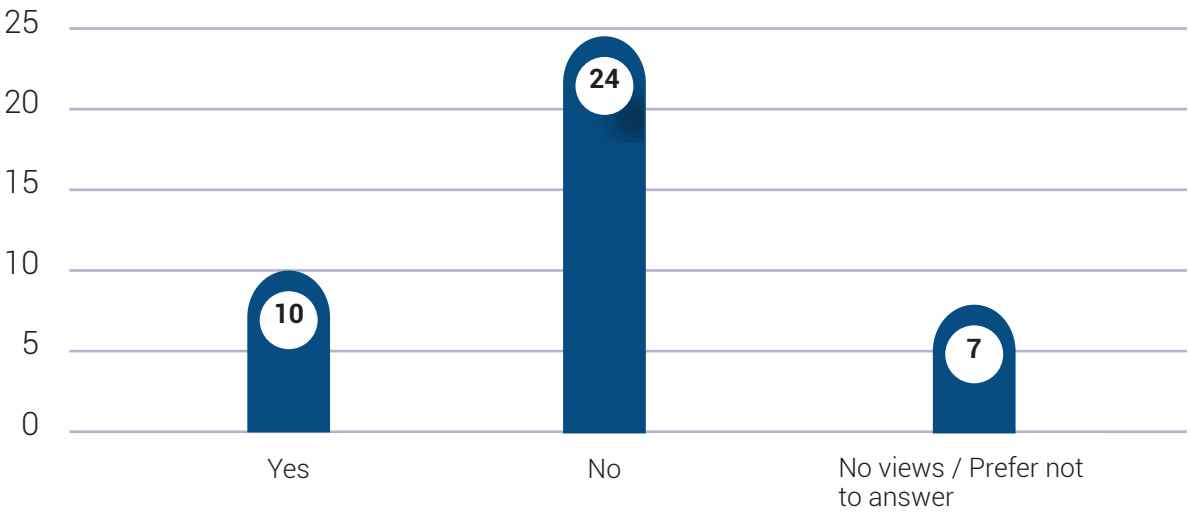


Figure 14: Should the establishment of a national PoC be mandatory for States members?



4.2 Key characteristics of the PoC

The subsequent section of the survey covers selected characteristics specific to the PoC, namely the typology, the functions that the PoC should perform, and language.

Key findings:

- In terms of a typology of PoCs the survey followed the classification indicated in the First Annual Progress Report of the OEWG, which outlines two types of PoC—diplomatic and technical.[13] The majority of respondents (31 out of 41) would like the directory to contain both types of PoCs (*see fig. 15*).
- In relation to the functions of diplomatic PoCs, most of the respondents opted for communication, followed by coordination and reporting (*see fig. 16*).
- With regard to the functions of technical PoCs, most of the respondents opted for assistance, followed by communication and coordination (*see fig. 17*).
- In terms of the language(s) that the PoC and secretariat should use for communication, the majority of respondents expressed their preference to consider all official languages of the United Nations (Arabic, Chinese, English, French, Russian, and Spanish ; *see fig. 18*).

Figure 15: What type of PoC would you like the global directory to contain?

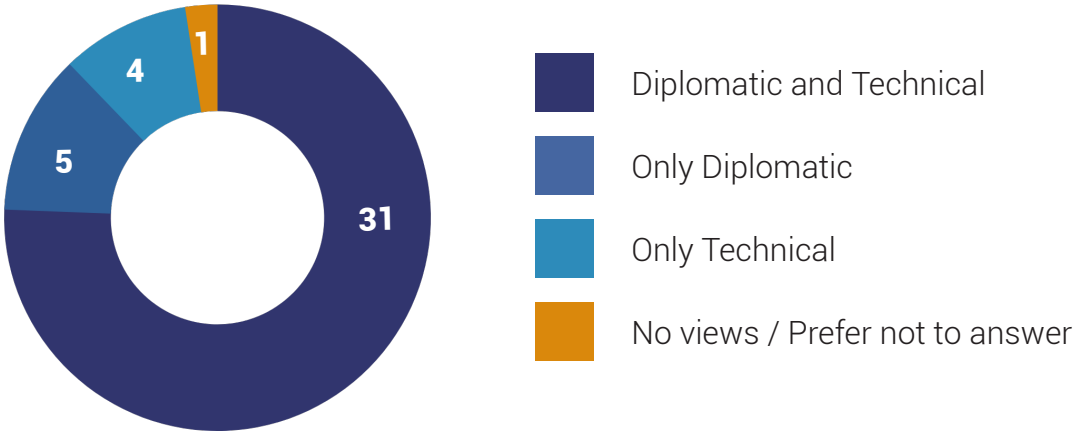
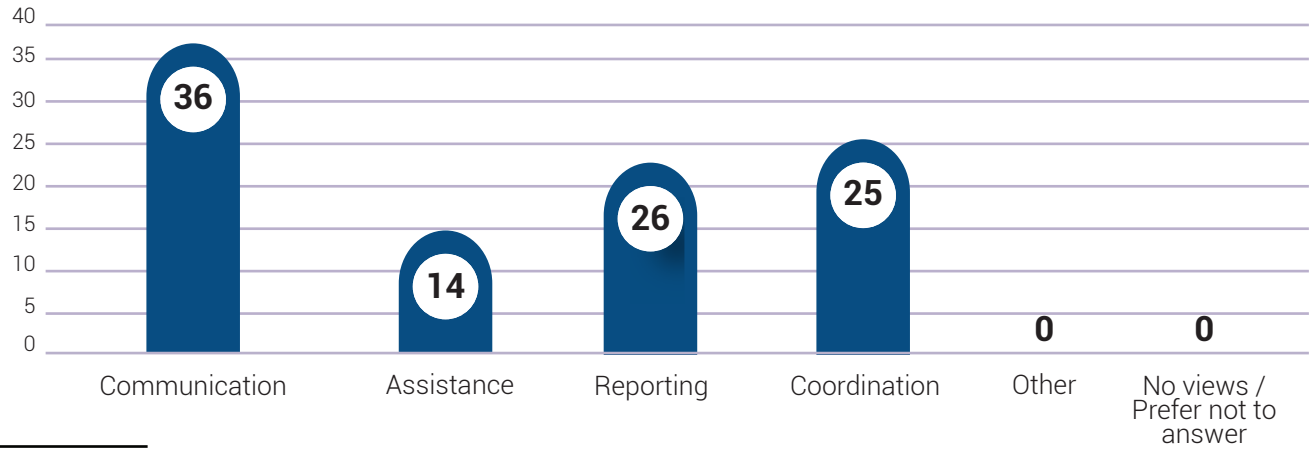


Figure 16: What specific functions would you like diplomatic PoCs to perform?



[13] General Assembly. 2022. Report of the Open-ended Working Group on Security of and in the use of Information and Communications Technologies 2021–2025. UN document A/77/275, p. 11.

Figure 17: What specific functions would you like technical PoCs to perform?

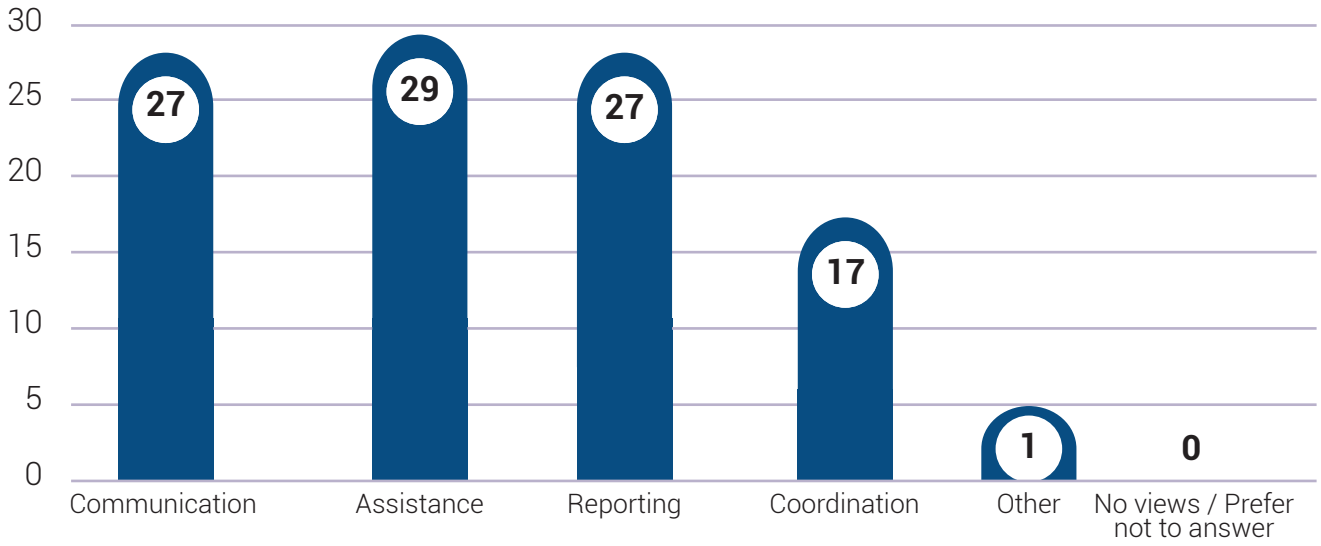
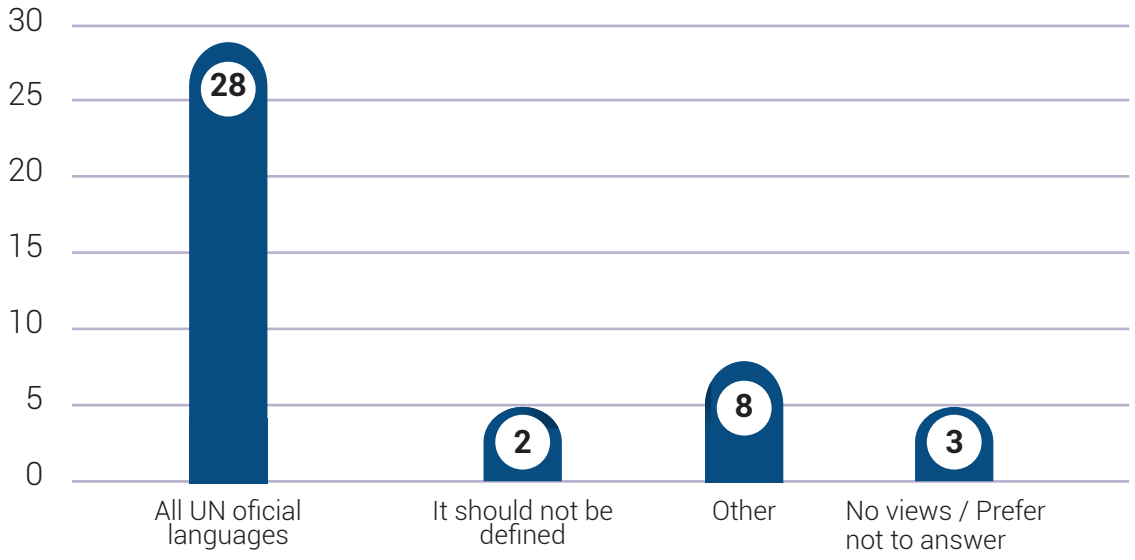


Figure 18: What language(s) should PoCs, and the secretariat use for communication?



4.3 Secretariat Role and Capacities

This subsection covers key aspects concerning the secretariat, such as responsibilities and capacities (budget and staff).

Key findings:

- In terms of activities/responsibilities of the secretariat, all respondents selected "directory maintenance", followed by "communication", "organization of meetings", and "conduct exercises". A few Member States selected "capacity-building" as a secretariat responsibility (*see fig. 19*).
- The secretariat should be properly resourced. The majority of respondents preferred the secretariat to have both a specific budget to manage the directory (*see fig. 20*) and a dedicated staff to manage the directory (*see fig. 21*).

Figure 19: Which activities should the secretariat be responsible for?

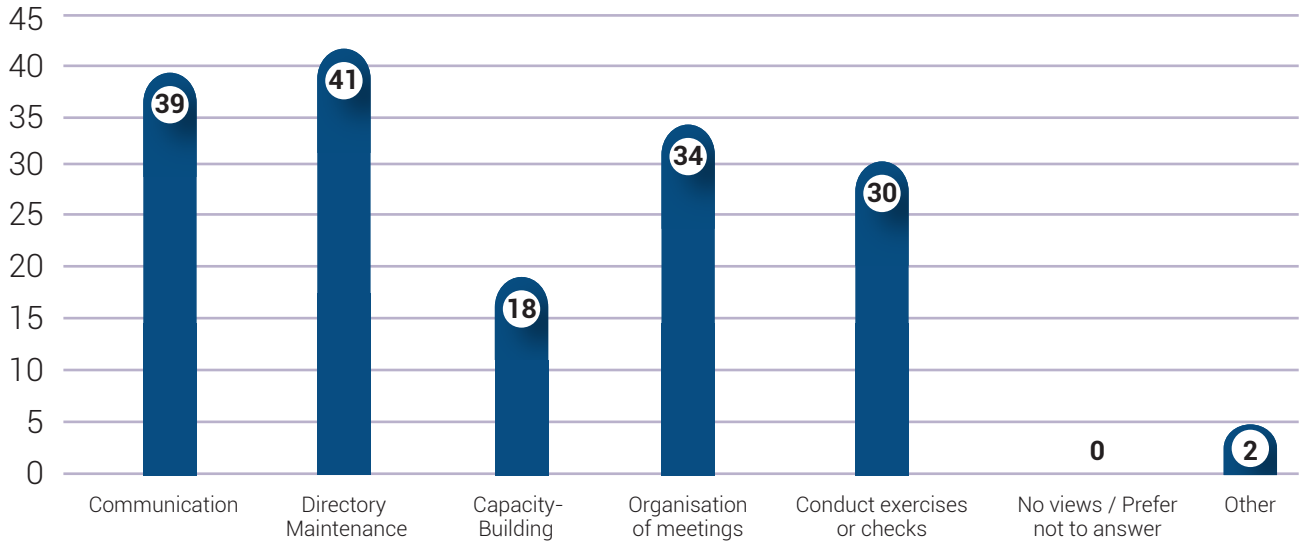


Figure 20: Should the secretariat have a dedicated budget to manage the PoC directory?

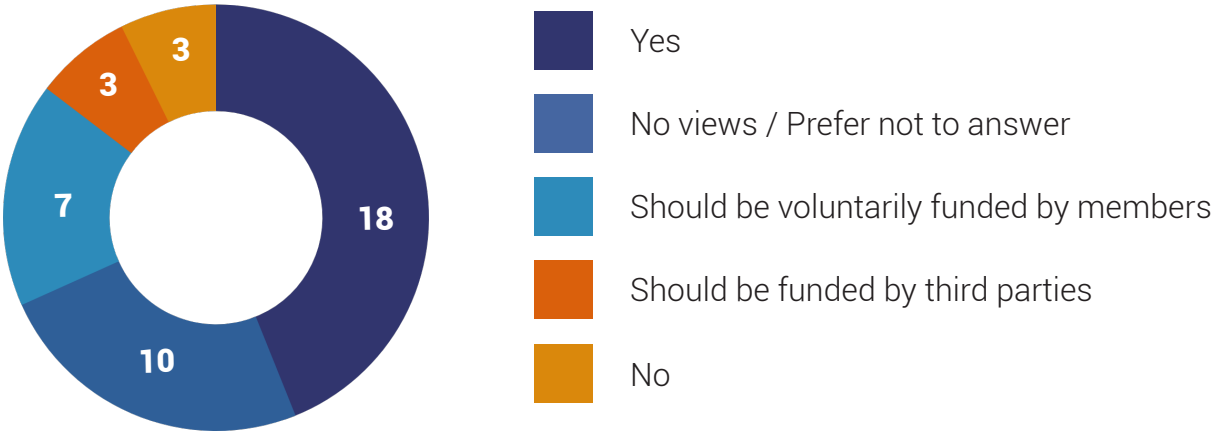
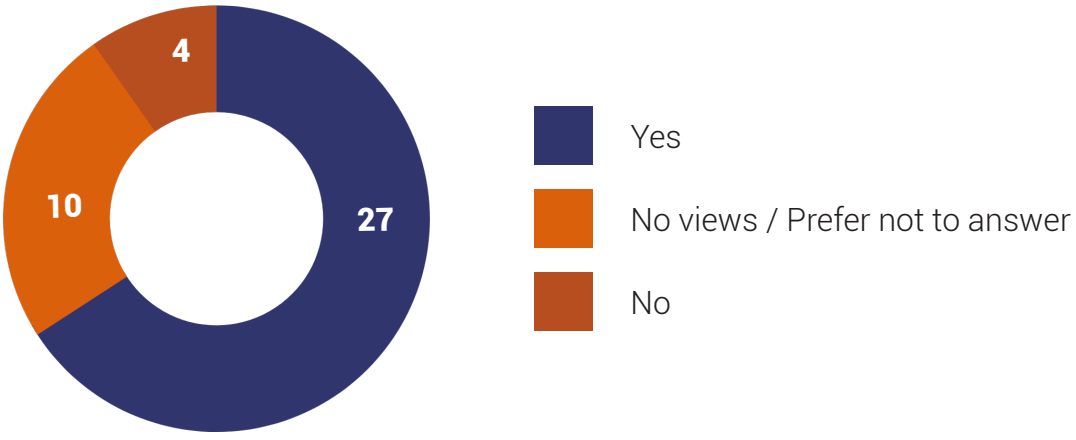


Figure 21: Should the secretariat have dedicated staff to manage the directory of PoCs?



4.4 The Directory

The last section of the survey concerned the directory itself. This is where information regarding PoCs is stored. This would usually be kept by the secretariat and made available to Member States. The survey addressed key elements concerning the location, access, and updates of the directory.

Key findings:

- In terms of the location of the directory, most of respondents prefer that it would be stored online (*see fig. 22*), in particular on a pre-existing United Nations website/platform (*see fig. 23*).
- In relation to the information that the directory shall contain, the majority of respondents prefer the name of the office/department/unit/agency in charge of the PoC, followed by the name of the contact person, and the type of the PoC. General email addresses were slightly preferred over the email of the contact person (*see fig. 24*).
- For updating the directory, the majority of respondents would prefer the Secretariat to send reminders to Member States (*see fig. 25*).

Figure 22: Where should the directory be stored?

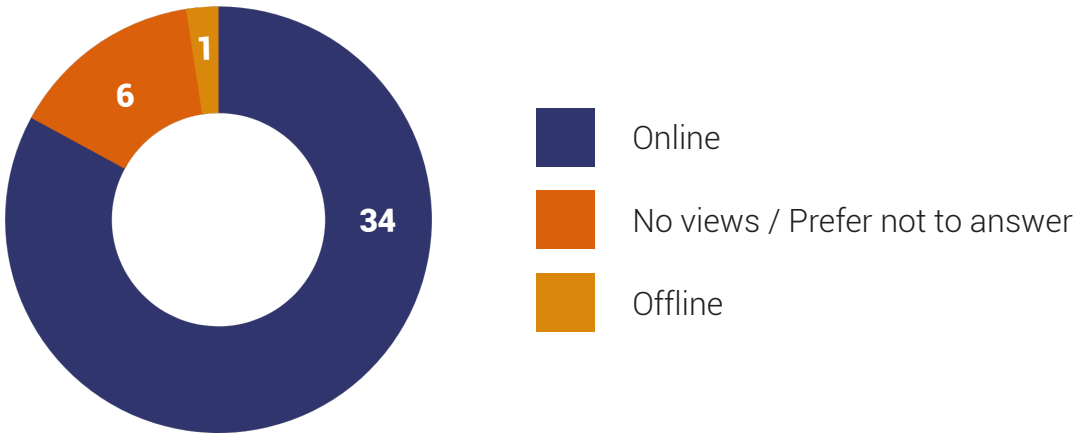


Figure 23: If "Online": Where exactly?

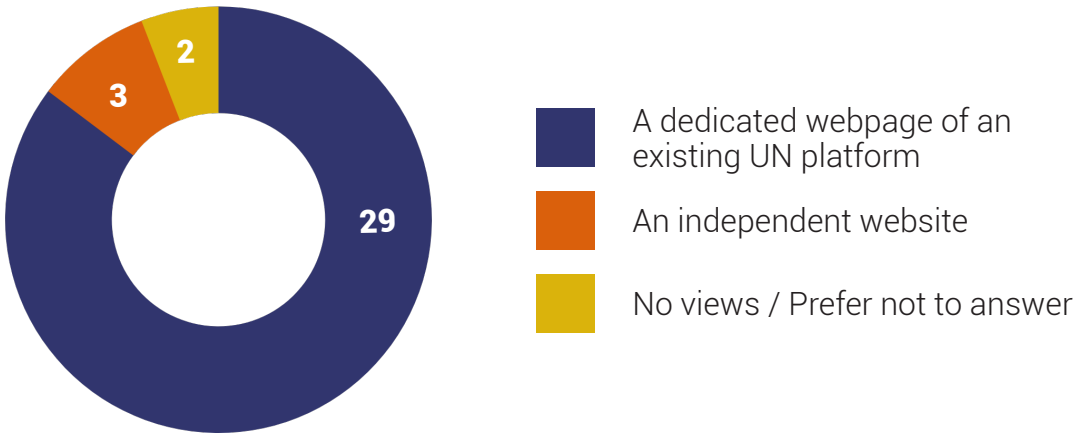


Figure 24: What information should the directory contain?

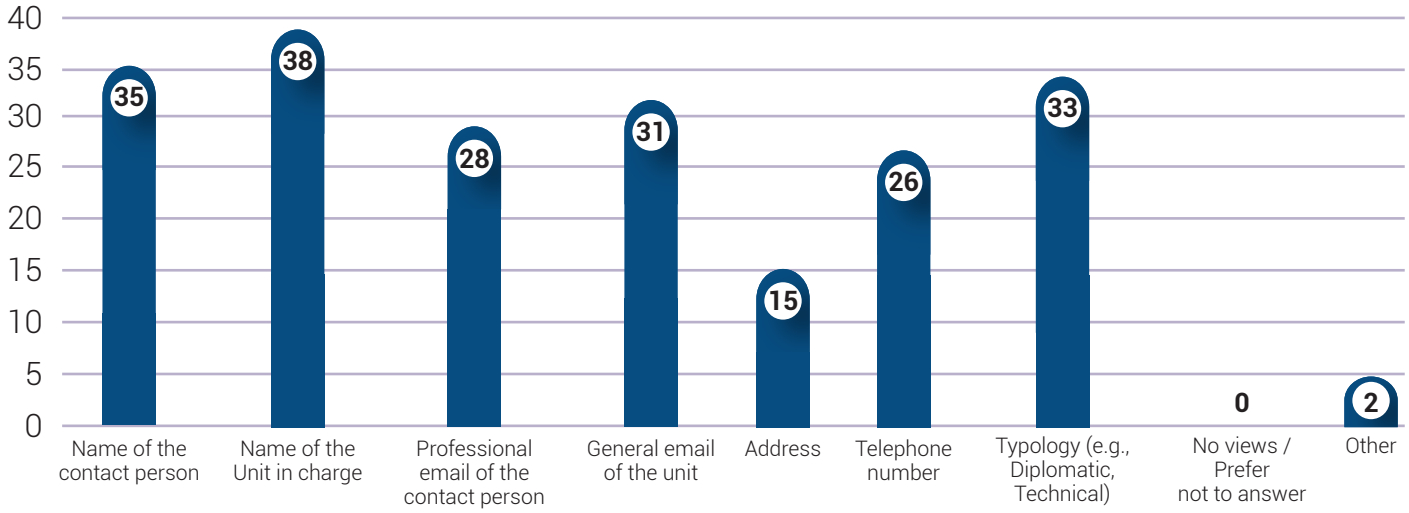
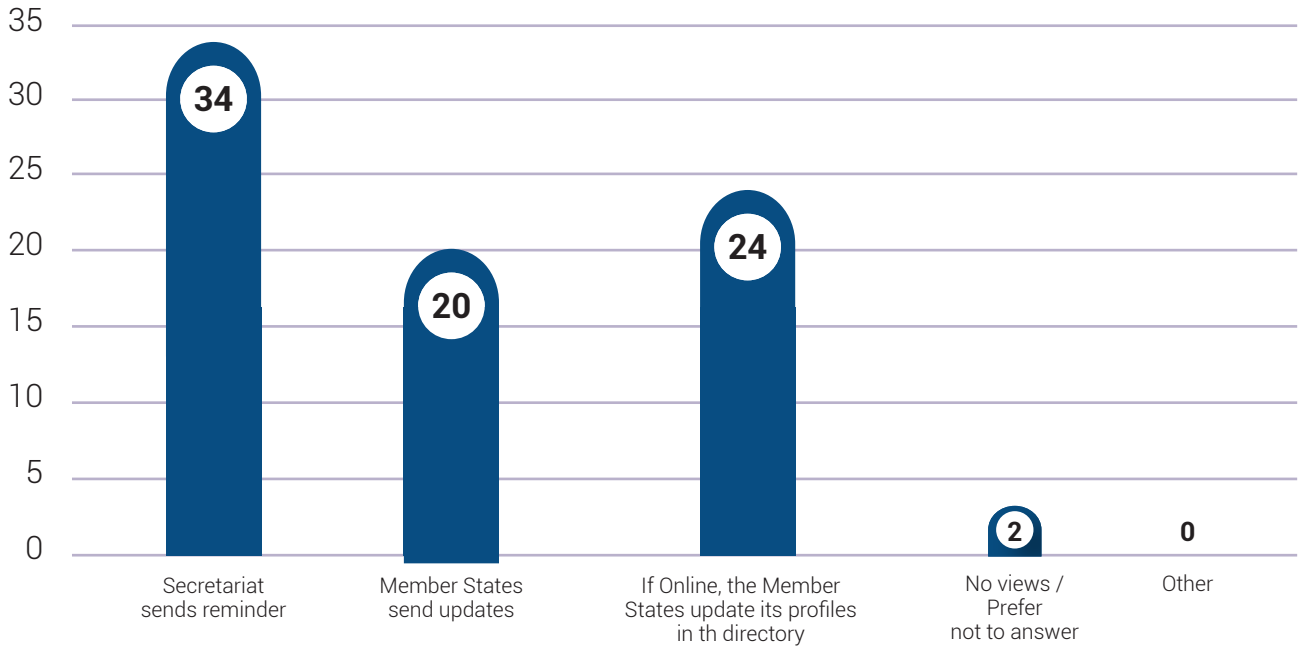
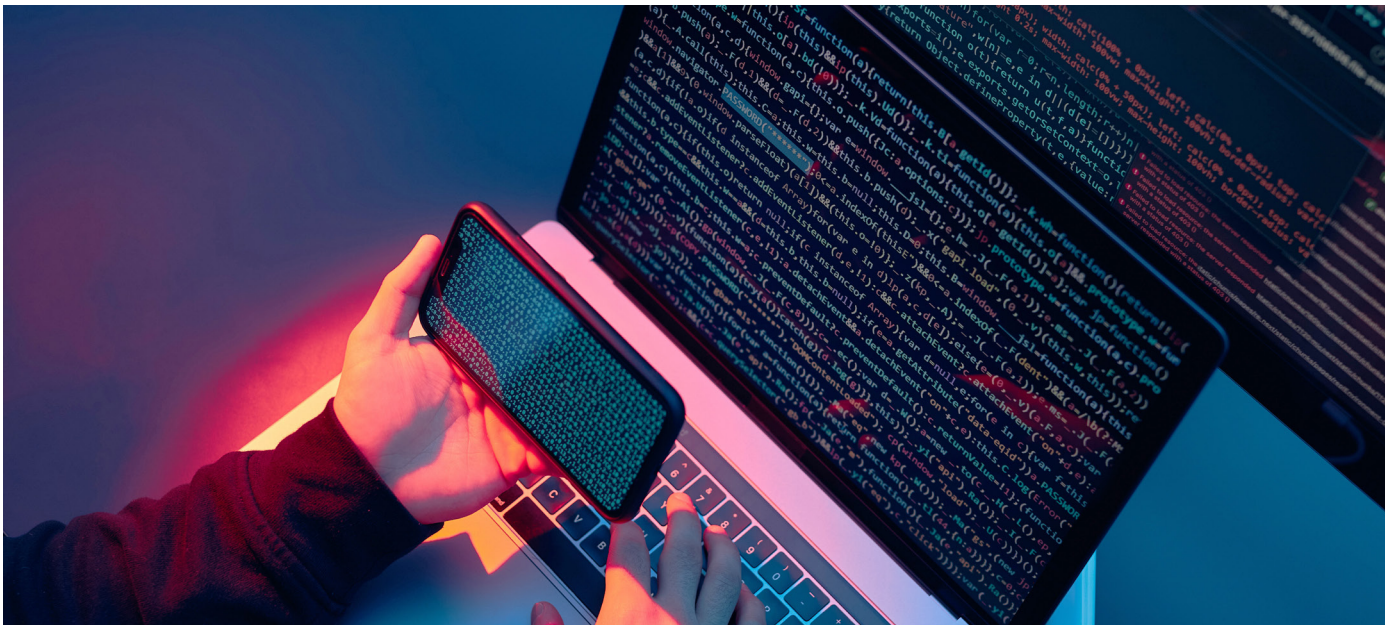


Figure 25: How the directory should be updated?





5. Contextualization and Final Recommendations

In this last section, the results of the first two phases of the research project are discussed and contextualized within the ongoing discussions at the OEWG.[14] The following sections suggest recommendations that can be considered for immediate and future developments of the global intergovernmental directory of PoCs. Moreover, some of the recommendations have a broader scope and applicability and may be applied to other directories in the field of disarmament and cybersecurity.

5.1 Recommendations on Purpose and Principles

The importance of clearly defining the purposes and principles of a directory of PoCs should not be overlooked. In the OEWG the Chair and Member States are attentively considering these elements.[15] Considering the ongoing and future discussions on the global intergovernmental directory of PoCs, this report identifies specific tasks for the PoCs.

With regard to diplomatic PoCs, the following tasks may be considered (ranked according to the results of the survey).

1. **Communication:** refers to relevant information exchange (political/diplomatic) among PoCs (horizontal exchange) and with the secretariat (vertical exchange).
2. **National coordination points:** activities that involve multiple agencies or institutions at the domestic level.

[14] To this end, this section makes some references to the OEWG Chair's revised non-paper, circulated among the Member States on 28 February 2023, which many States have recognized as a good basis for discussion during the fourth substantive session of the OEWG. (see Revised Non-Paper Prepared by the Chair of the OEWG: Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory, 28 February 2023., available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_28_February_2023.pdf)

[15] "The main purpose of the POC directory is to: (a) Enhance interaction and cooperation between States and in doing so promote international peace and security, and increase transparency and predictability; (b) Facilitate communication between States in the event of an urgent or significant ICT incidents; and (c) Reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents contributing to the prevention of conflict between States"; ibid.

Whereas for technical PoCs, the following tasks may be considered (ranked according to the results of the survey).

1. **Communication:** refers to relevant information exchange (political/diplomatic) among PoCs (horizontal exchange) and with the secretariat (vertical exchange).
2. **Assistance in cooperation:** refers to operational, technical, or legal assistance that a Member State may require from another Member State.

Moreover, based on the results of the survey, PoCs (both diplomatic and technical) may also be considered for reporting activities.

3. **Reporting:** concerns submitting scheduled reports (e.g., annual reports) to the secretariat concerning information or activities that Member States may be required to report about.

5.2 Recommendations on Modalities

Should the United Nations Secretariat be identified as the responsible body for the global intergovernmental directory of PoCs, it would be charged with management of the directory and with development and operationalization of its technical aspects.[16] Analysis of other secretariats in existing PoC directories, as well as the results of the survey, suggest that the following activities and capacities may be further considered.

In terms of **specific activities of the secretariat**, it would be relevant to consider the following specifications (ranked according to the results of the survey):[17]

- **Directory maintenance,**[18] such as updating the PoC directory;
- **Communication** among and with States and other stakeholders;
- **Organization of meetings** with the PoCs; and
- **Conduct of exercises or communication checks** (such as "ping" tests) with the PoCs.[19]

In terms of the **capacities of the secretariat,** it would be important to consider resources, including:

- **Having dedicated staff for directory management:** Most Member States that took part in the survey considered it necessary to have dedicated staff working on the directory. The analysis of existing PoC directories found that the average number of staff working on the management of a PoC directory is two
- **Having a dedicated budget for the management of the directory:** Many of the respondents to the survey agreed that a dedicated budget is needed.

The findings presented in this research report are in line with additional aspects discussed at the OEWG in relation to modalities.[20] This includes the nomination of both diplomatic and technical PoCs to the directory, the contact details of the PoCs, and the language used (all official languages

[16] Ibid., para. 4.
[17] Despite capacity-building having been addressed in the Chair's non-paper, the majority of the respondents of the survey did not envision this activity for the secretariat.
[18] In line with ibid., para. 5.
[19] In line with ibid., para. 5.
[20] Ibid., para. 4(a).

of United Nations). Concerning the nomination of PoCs at the national level, this report recommends that it may be more effective to designate an entity as PoC rather than an individual. The latter may not be available for extended periods of time (holiday, illness, etc.) or may be reassigned.

Moreover, additional elements might be taken into consideration in relation to the cybersecurity of the directory,[21] and accessibility of the directory.[22] In regard to cybersecurity:

- **Location of the portal:** It would be relevant to further specify the location of the directory. This report suggests that it would be recommended to host the directory on a specific, restricted, and protected section of a pre-existing website (such as the UNODA website).
- **The interface of the portal:** For online directories, the user-friendly design of the platform is key; the analysis of existing online directories reveals that it is an asset when users can easily navigate the directory and retrieve the required information. It could be considered to share the draft design of the digital platform with States for feedback before implementing it.

In regard to directory accessibility, the following additional element may be further considered for discussion:

- **Login credentials:** Some directories feature personal credential policies (for example, only PoC staff can access the directory, and each person has their individual credentials); others adopt the 'one State–one password' policy, and thus login details can be shared among selected offices or institutions of the State.

In terms of updates,[23] this research recommends that to keep the directory updated, it would be useful to task the secretariat with the responsibility of sending scheduled reminders to all participants (preferably not using the same contact details of the PoC).

5.3 Additional Recommendations

Finally, this report identifies three general and key foundational aspects that should be taken into consideration for the effective functioning of any PoC directory.

- A clear understanding of PoC functions and roles. If these aspects are covered and detailed from the outset, Member States might have a better sense of where to structure it and of the capacities needed to equip the PoC at the domestic level.
- A clear mandate and resources for the secretariat, especially concerning its responsibilities and duties regarding the key and sensitive tasks of receiving States' nominations or updates for their PoC (including verifying such information), and assisting Member States with capacity-building.
- A clear understanding of how often and for what purposes Member States use the PoC directories. The research for this project revealed that often secretariats do not have data to assess if the directory they maintain is used by members. Having such information would be important for improving the efficiency of this confidence-building measure.

[21] "The directory will be hosted online on a secure password-protected website"; ibid., para. 4(b).

[22] "States may request login credentials for the website from UNODA through their Permanent Missions in New York"; ibid., para. 4(c).

[23] "States may provide updates to information contained in the directory on a rolling basis in the event of changes to their submitted information"; ibid., para. 4(d).

Annex 1. List of States that Responded to the Survey

(In alphabetical order).

Albania
Australia
Austria
Canada
Chile
Colombia
Costa Rica
Czechia
Denmark
Ecuador
Estonia
France
Germany
Holy See
Honduras
Hungary
Ireland
Israel
Italy
Jordan
Latvia
Malawi
Mauritius
Mexico
Monaco
Montenegro
Netherlands
Norway
Philippines
Portugal
Qatar
Republic of Korea
Russian Federation
Singapore
Slovakia
South Africa
Spain
Switzerland
Timor-Leste
Türkiye
United Kingdom