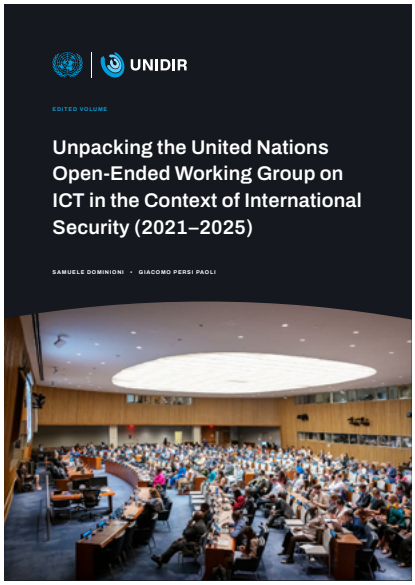
UNIDIR

Chapter title **Confidence-building measures**

Chapter author **Dr Samuele Dominioni**



Extracted from the UNIDIR publication:

Samuele Dominioni and Giacomo Persi Paoli (eds.), *Unpacking the United Nations Open-Ended Working Group on ICT in the Context of International Security (2021–2025)*, (Geneva: UNIDIR, 2026).

Confidence-building measures

Dr Samuele Dominioni

1. Introduction

Confidence-building measures (CBMs) have long been recognized as a useful tool in the context of international security and disarmament efforts. Modern CBMs developed in the context of the Cold War to address military issues, but they have been gradually expanded to non-military domains.[1] In the information and communications technology (ICT) environment, CBMs refer to sets of measures agreed by States that aim to reduce misunderstandings, misperceptions and other sources of tension among States in their use of ICTs.[2] CBMs in this context have been developed by a wide variety of international and regional bodies, including the United Nations, the Organization for Security and Co-operation in Europe (OSCE), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Organization of American States (OAS)[3] and the Economic Community of West African States (ECOWAS).

1.1. The road to the OEWG 2021–2025

Since the inception of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), the United Nations has been playing a crucial role in the development and support for the implementation of global CBMs for ICTs. Practical CBMs have been addressed in each of the consensus reports adopted by the GGEs. For example, in the first consensus report from 2010, the GGE considered it useful to develop CBMs to "address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict".[4]

Subsequent GGEs, building on the success of regional organizations in adopting lists of CBMs for the ICT environment[5] and also on the recommendations of previous GGEs, highlighted how CBMs can be relevant to addressing issues related to States' use of ICTs and can, therefore, increase transparency and cooperation. The 2013 and 2015 consensus reports of the GGEs introduced a list of CBMs, which included "[e]nhanced sharing of information among States on ICT security incidents, [such as] exchanging information on national

1 Samuele Dominioni, "Confidence Building Measures in Cyberspace", in *Elgar Encyclopedia of Cyberspace and International Law*, eds Russell Buchan, François Delerue and Nicholas Tsagourias (Cheltenham: Elgar, forthcoming 2026).

2 Ibid.

3 Camino Kavanagh, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* (Geneva:, UNIDIR, 2017), https://unidir.org/publication/the-united-nations-cyberspace-and-international-peace-and-security-responding-to-complexity-in-the-21st-century/.

4 General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, https://docs.un.org/A/65/201, 2010, paragraph 18(ii).

5 Kavanagh, *The United Nations, Cyberspace and International Peace and Security.*

points of contact [(POCs)]", "the creation of a directory of such contacts",[6] "[e]xchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums,"[7] and "[t]he voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them".[8]

In 2021, two processes dedicated to State use of ICTs in the context of international security produced consensus reports that provided additional understanding on CBMs. The first, agreed by the sixth and final GGE, further elaborated on the list of CBMs recommended by its predecessor group and made a distinction between cooperative measures[9] and transparency measures.[10] The second report, agreed by the first Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG 2018–2021), acknowledged the relevance of the CBMs recommended in the GGE reports and highlighted several measures that required priority attention. These included voluntary information exchanges on different topics (including threats, national approaches to define critical infrastructure, and categorizing ICT incidents); developing a shared understanding of concepts and terminology; and developing scenario-based exercises at the policy, operational, or technical levels between computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs).[11] Additional CBMs were discussed, including establishing a POC network and a repository of CBMs, and the roles and responsibilities of non-State actors.[12]

Discussions on CBMs have progressed from a general appreciation of their applicability to the ICT environment to a substantive body of practical proposals and recommendations. This chapter analyses how the second OEWG (2021–2025) took stock of the legacy of the previous GGEs and OEWG to further develop understanding and operationalization of CBMs. The chapter also looks at how the OEGW 2021–2025 identified key implications for consideration by the permanent Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs, which starts its work in 2026.

---

6 General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, **A/70/174**, 2015, paragraph 16.

7 General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, **A/68/98**, 2013, paragraph 26(c–e).

8 **A/70/174**, paragraph 16(d).

9 Cooperative measures included, for example, a more detailed explanation of the Points of Contact measure. See General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, **A/76/135**, 14 July 2021, paragraphs 76–78.

10 Transparency measures referred, for example, to the use of United Nations resources, such as voluntary reporting to the Secretary-General, and the UNIDIR Cyber Policy Portal. See **A/76/135**, paragraph 86.

11 General Assembly, Report of the Open-ended Working Group on Developments in the field of information and telecommunications in the context of international security, **A/75/816**, 2021, paragraphs 29–32.

12 **A/75/816**, paragraphs 29–32.

2. The evolution of the discussions of the OEWG 2021–2025

Over the course of the OEWG 2021–2025, States' discussions on CBMs evolved from an initial reaffirmation of some of the themes developed in previous processes to a more operational, implementation-oriented outlook. This evolution was characterized by milestones that helped mark out consensus on a few core themes. By examining discussions in the substantive sessions, as well as the multiple documents produced by States, the Chair and the Secretariat, it is possible to unpack the discussions on CBMs into four main phases.

2.1. From reaffirmation to early operationalization

In the early sessions of the OEWG 2021–2025, States widely reaffirmed the value of CBMs as a stabilizing element of State behaviour in the ICT environment. Initial discussions focused on reiterating previously agreed measures, re-emphasizing the importance of regional experiences and practices in the context of ICT CBMs, and signalling the desire for the establishment and operationalization of key measures. These measures included those allowing direct communication between States,[13] such as the proposed POC directory.[14]

At this stage, discussions were mostly exploratory, with many States referring to their national experiences with regional POCs (e.g., in the OSCE, ASEAN, or the OAS).[15] Yet, some States were already addressing practical aspects of CBM operationalization, such as defining typologies of POCs (e.g., diplomatic, legal, technical) and raising the possibility of simulation exercises or ping tests for the POC directory.[16] However, these early operational attempts did not garner significant support from the majority of States. During the third session, when States discussed the first annual progress report (APR), concerns regarding sovereignty, neutrality[17] and misuse of CBMs led to a narrowing of the scope of the discussions, with the operational aspects of establishing the POC directory to be addressed at a later stage.[18]

13 For example, European Union (session 1, meeting 7).

14 For example, Germany on behalf of a group including Serbia and Switzerland (session 1, meeting 7); Russian Federation (session 1, meeting 8); Netherlands (session 1, meeting 8); Jordan (session 2, meeting 7); and Thailand (session 2, meeting 7).

15 For example, Singapore (session 1, meeting 8); United States (session 2, meeting 7); Costa Rica (session 1, meeting 8).

16 For example, Singapore (session 1, meeting 7); Malaysia (session 1, meeting 8); Costa Rica (session 1, meeting 8; and session 2, meeting 7); El Salvador (session 3, meeting 3); and Estonia (session 1, meeting 8).

17 For example, a few States recalled that CBMs should not be used to impinge on the national sovereignty of States or to interfere in their internal affairs. For example, Nigeria (Session 3, meeting 5); Democratic Republic of the Congo (Session 3, meeting 3).

18 For example, China (session 3, meeting 3); United States (session 3, meeting 4); and Mexico (session 3, meeting 4).

The first cycle[19] concluded with States "taking note" of various proposals with varying levels of support.[20] They agreed to include in the first APR the establishment of the POC directory – as the Global Intergovernmental POC Directory (see Figure 1) – which was explicitly framed as building on regional experiences.[21] Moreover, the Secretariat was tasked with seeking States' views on the POC directory and producing a background paper for discussion in the upcoming sessions.

2.2. Consolidation around the Global Intergovernmental POC Directory

In the lead-up to the fourth substantive session, held in March 2023, the Chair and the Secretariat engaged in focused activities on the Global Intergovernmental POC Directory. In particular, the Secretariat shared a background information paper on the directory,[22] which collected the views of 27 States that submitted their inputs; and the Chair shared a non-paper on elements for the development and operationalization of the directory,[23] and convened dedicated hybrid informal intersessional meetings with States on the directory before and after the session. These initiatives contributed to developing a more detailed understanding of regional experiences and how to operationalize the POC directory, including its guiding principles, management and modalities, and related capacity-building.

During the substantive session, CBM discussions consolidated around a few themes with widespread support. These included the newly created Global Intergovernmental POC Directory, the key role of regional organizations in implementing CBMs, and the need for CBMs to remain voluntary and to respect national sovereignty. At the same time, substantive discussions yielded more operational details for agreed CBMs as well as additional, more technical measures. For example, several States made interventions that discussed the possibility of organizing communication checks, tabletop exercises and drills to operationalize CBMs,[24] which were often framed through regional examples.[25] In parallel, more technical proposals were made referring to cooperation between CSIRTs,[26] coordinated vulnerability disclosure[27] and shared technical standards (e.g., Traffic Light Protocols).[28]

---

19 The analysis breaks down the OEWG 2021–2025 in four cycles, each of which begins with the substantive sessions and ends with the negotiation session where a report was agreed. See the introduction of this volume for further guidance.

20 General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, **A/77/275**, 2022, paragraph 16(a–e).

21 **A/77/275**, 12.

22 UNGA, 2023, A/AC.292/2023/1.

23 Chairperson OEWG 2021–2025, Letter from the Chair, 26 January 2023.

24 For example, European Union (session 4, meeting 6); Singapore (session 4, meeting 6); Ghana (session 4, meeting 6).

25 For example, Brunei Darussalam on behalf of ASEAN (session 4, meeting 6).

26 For example, Mexico (session 4, meeting 6).

27 For example, Kazakhstan (session 4, meeting 6); Czechia (session 4, meeting 6).

28 For example, Malaysia (session 4, meeting 6).

Substantive discussion led the Chair to prepare an initial list of CBMs,[29] which was shared with States ahead of the fifth session, when the second APR was discussed and agreed. This APR added many relevant elements for CBMs, including an appendix detailing procedures for use of the POC directory[30] and an initial list of voluntary global CBMs, which contained four measures (see Table 1 below).

2.3. Operationalization through POC anchoring

After the States agreed on the establishment of the POC directory and its foundational elements[31] – such as its function, structure and management – discussions moved into an even more detailed operational phase. Substantive sessions during the third cycle focused on the practical aspects of the Global Intergovernmental POC Directory, including POC nominations, communication templates, simulation exercises, and the administrative and financial requirements for sustaining the mechanism.[32] Operational details were easier to address through discussion because they were tightly anchored to the directory. In fact, earlier proposals (e.g., on exercises and testing) resurfaced and gained greater support when framed as tools to enhance the functionality of the POCs, rather than as a stand-alone CBMs. At the same time, concerns were raised during the third cycle about the expansion of the POC directory, including the integration of real-time information-sharing platforms and dispute-resolution mechanisms. Some States also objected to the use of the POC directory to conduct a political assessment of other States' actions in the ICT environment.[33] These concerns shaped the language that would later appear in the third APR.

Meanwhile, the establishment of the Global Intergovernmental POC Directory became a reality when the Secretariat invited all States to nominate their POC on 8 January 2024. The official launch took place on 9 May 2024, and the first meeting of the POCs occurred on the same day.[34] A few weeks later, the Secretariat sent the first "ping"[35] test.

---

29 Chair Ambassador Burhan Gafoor (session 4, meeting 6).

30 General Assembly, 'Developments in the field of information and telecommunications in the context of international security', A/78/265, 1 August 2023, Annex A, 'Elements for the development and operationalization of a global, intergovernmental points of contact directory'.

31 **A/77/275**.

32 For example, Russian Federation (session 6, meeting 6 and session 7, meeting 6); Egypt on behalf of the Group of Arab States (session 6, meeting 6); Ghana (session 7, meeting 7); Chair (session 6, meeting 6).

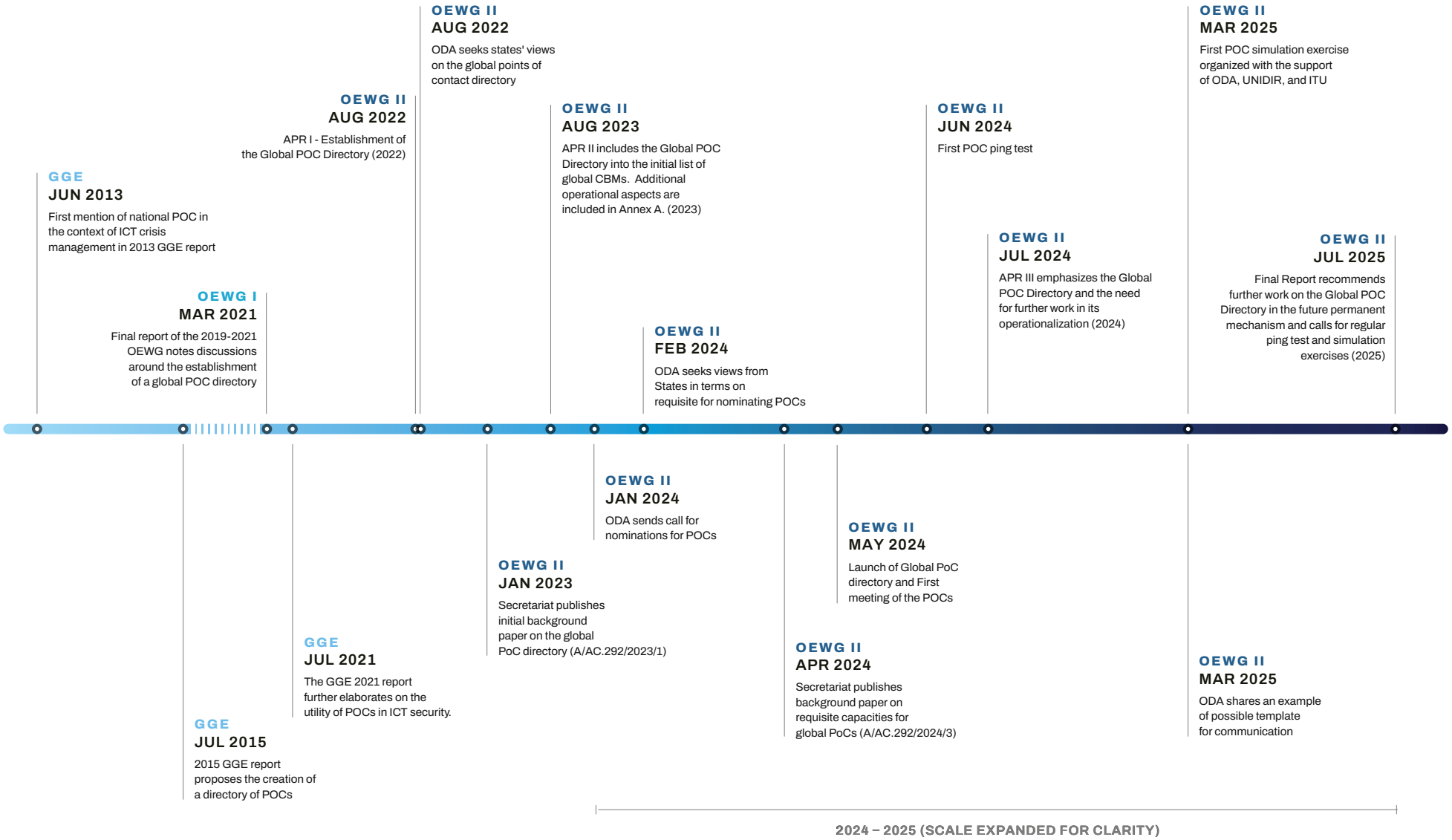
33 For example, Russian Federation (session 6, meeting 6); Thailand (session 8, meeting 3); European Union (session 8, meeting 4); United Kingdom (session 8, meeting 3); New Zealand (session 8, meeting 3).

34 As of 9 May 2024, 92 States had nominated a POC. See Office for Disarmament Affairs, "The Global Intergovernmental Points of Contact Directory as Established by the OEWG ICT security", Presentation, 9 May 2024, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/9_May_2024_1st_meeting_POCs_Demo-overview-ping_test.pdf**.

35 The Office for Disarmament Affairs sent an email to POCs registered in the directory, requesting a response confirming the receipt of that message within 24 hours.

FIGURE 1.

Timeline of the establishment and operationalization of the Global Intergovernmental POC Directory



As States' discussions entered a phase of practical operationalization, capacity-building also emerged as an essential component for engaging in and implementing CBMs.[36] The States continued to reaffirm the vital role of regional and subregional organizations in developing and implementing CBMs, including by sharing practical examples.[37] Additionally, States continued to discuss transparency-focused CBMs. In this context, different proposals received varying levels of support, including the sharing of national views on technical ICT terms or of national approaches to classifying ICT incidents.

The third APR acknowledged the important developments concerning the POC directory and explicitly endorsed the "step-by-step" approach for its operationalization. Moreover, the Secretariat was tasked with developing a communications template for voluntary use by POCs at their discretion. For the first time, States also agreed to continue the development of the POC directory in "the forthcoming sessions of the OEWG and subsequently under the auspices of the future permanent mechanism".[38] Moreover, four additional CBMs were adopted, expanding the initial list of voluntarily global CBMs (see Table 1) and reflecting a growing consensus across a broader range of themes. These included recognizing the importance of cooperation between States to strengthen capacity in ICT security, the protection of critical infrastructure and critical information infrastructure, and the key role of private–public partnerships.

2.4. Late-stage operationalization and closure

In the last cycle, CBM discussions can be largely categorized into two layers. In one, there were more discussions that converged on the operationalization of key CBMs, such as the Global Intergovernmental POC Directory; and in the other were proposals – still exploratory – concerning possible new measures.

In terms of operationalizing the POC directory, it became broadly accepted to engage in ping tests and simulation exercises,[39] to consider developing voluntary communication templates, and to address capacity-building and implementation challenges.[40] In particular, capacity-building was increasingly framed not merely as an enabler but as essential to meaningful participation and implementation in CBMs, especially for maximizing participation in the POC directory.[41]

---

36 For example, Ghana (session 6, meeting 6); Cuba (session 6, meeting 6); Canada (session 7, meeting 7); Mexico (session 7, meeting 7); and Argentina, on behalf of a group of Latin American States (session 6, meeting 7).

37 For example, Cross-Regional Confidence-Builder Group, "Cyber CBMs in Action", Working paper, 12 December 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Working_Paper_CBMs_in_Action.pdf.

38 General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/79/214, 2024. See also the chapter on Regular Institutional Dialogue in this volume.

39 The first simulation exercise for the POC directory was conducted in March 2025 by the Office for Disarmament Affairs, UNIDIR and the International Telecommunication Union (ITU).

40 For example, Russian Federation (session 9, meeting 6); Thailand (session 10, meeting 5); Tonga on behalf of the Member States of the Pacific Islands Forum (session 10, meeting 5); Indonesia (session 9, meeting 7).

41 For example, El Salvador (session 9, meeting 6); South Africa (session 9, meeting 6); Lao People's Democratic Republic (session 10, meeting 5); India (session 10, meeting 6).

While progress was demonstrated on the agreed CBMs, in particular the Global Intergovernmental POC Directory, additional proposals for new CBMs or extensions of existing ones were frequently met with caution. Several delegations urged the prioritizing of the implementation of the eight agreed CBMs (see Table 1), warning that additional proposals risked diluting progress and that an expanded list of unimplemented measures could undermine the effectiveness of existing CBMs.[42] For example, proposals linking CBMs to market access and other briefly discussed additions encountered explicit resistance from some States, with multiple delegations criticizing them and calling for their deletion during the negotiation session.[43]

The final report of the OEWG 2021–2025 institutionalized the Global Intergovernmental POC Directory and frames its ongoing operationalization within the context of the Global Mechanism on ICT Security. The agreed text also noted that the POC directory could become a tool to support CBMs in general. Moreover, the final report mandates regular simulation exercises and ping tests. Finally, it embeds CBMs within a voluntary, step-by-step, incremental approach that focuses primarily on implementing existing CBMs.

TABLE 1.

Initial list of voluntary global CBMs

INITIAL LIST OF VOLUNTARY GLOBAL CBMS (AS PER ANNEX, A/78/265)	
CBM 1	Nominate national points of contact to the global POC directory, and operationalize and utilize the global POC directory.
CBM 2	Continue exchanging views and undertaking bilateral, subregional, regional, cross-regional and multilateral dialogue and consultations between States.
CBM 3	Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and best practices.
CBM 4	Encourage opportunities for the cooperative development and exercise of CBMs.
ADDITIONAL VOLUNTARY GLOBAL CBMS (AS PER ANNEX B, A/79/214)	
CBM 5	Promote information exchange on cooperation and partnership between States to strengthen capacity in ICT security and to enable active CBM implementation.
CBM 6	Engage in regular organization of seminars, workshops and training programmes on ICT security.
CBM 7	Exchange information and best practice on the protection of critical infrastructure and critical information infrastructure, among other things, including through related capacity-building.
CBM 8	Strengthen public–private sector partnerships and cooperation on ICT security.

42 For example, France (session 11, meeting 3); New Zealand (session 11, meeting 3); Netherlands (session 11, meeting 5); Ukraine (session 11, meeting 5); Republic of Korea (session 11, meeting 5); and South Africa (session 11, meeting 5).

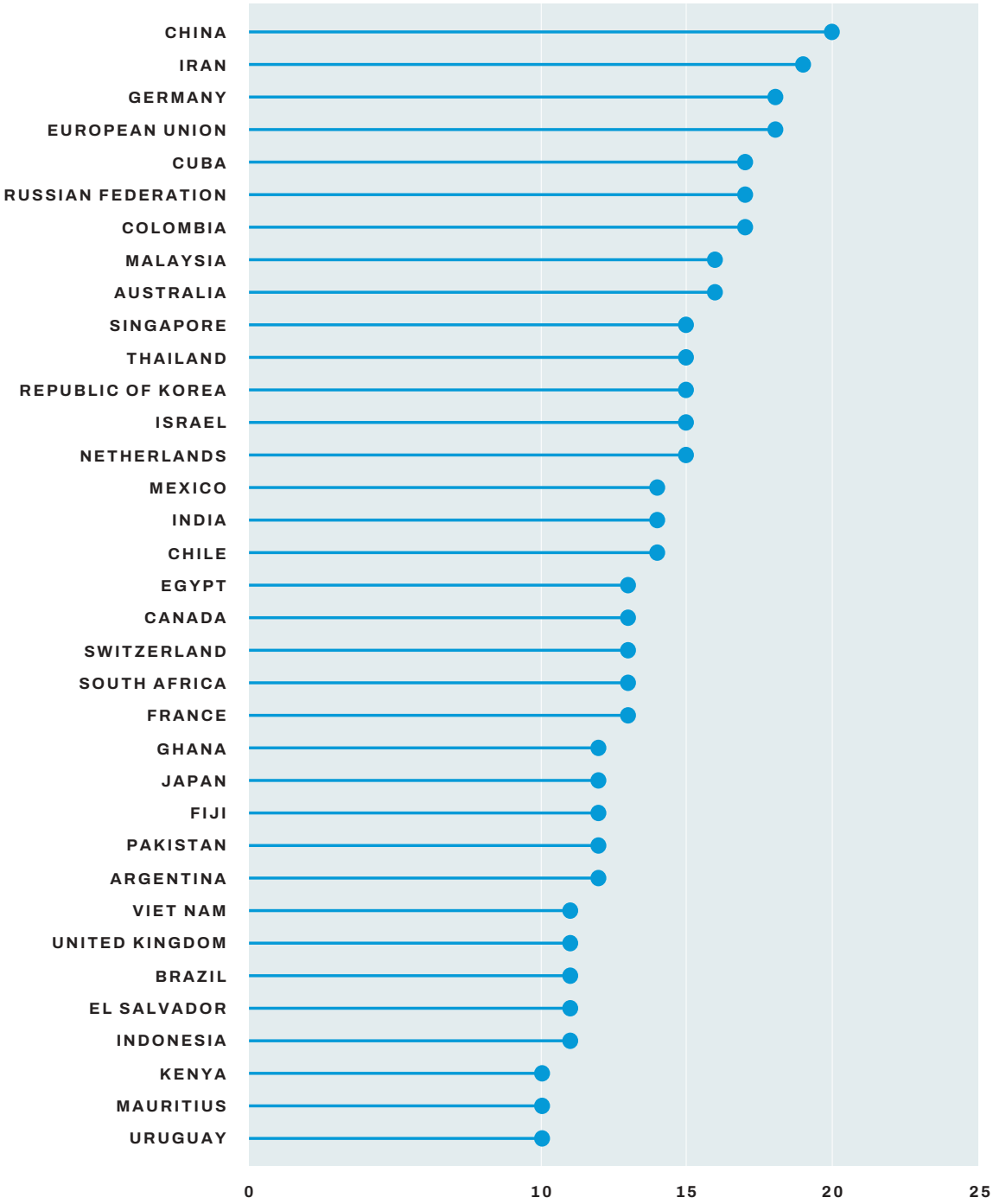
43 For example, United States (session 11, meeting 3); United Kingdom (session 11, meeting 5); Netherlands (session 11, meeting 5).

Overall, the CBM discussions over the years produced concrete outcomes for reducing misunderstandings, misperceptions and other sources of tension among States in their use of ICTs. The establishment of the Global Intergovernmental POC Directory, its operationalization and implementation, including the development of dedicated capacity-building initiatives and the outline of an initial list of CBMs, are among the results States achieved through substantive discussions throughout the sessions.

Burhan Gafoor (on screen), Permanent Representative of the Republic of Singapore to the United Nations, chairs the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 2024. Credit: UN Photo / Eskinder Debebe.

FIGURE 2.

Number of times delegations took the floor on CBMs in the OEWG 2021-2025.[44]



44 This chart shows the delegations that took the floor at least 10 times during the sessions. The full list of interventions is provided in Annex A.

3. Trends and major themes addressed during the mandate

States' negotiations under the agenda item on CBMs addressed multiple themes and included discussions of several proposals that span a wide range of issues – from general considerations regarding the importance of voluntariness to the detailed outlining of concrete technical cooperation measures. Overall, the breadth and depth of the discussions indicate that the delegations were meaningfully engaged in the sessions and eager to share national or regional and subregional examples, thereby enriching the understanding of concrete CBMs.

The following is a non-exhaustive list of some of the themes that were discussed during the OEWG 2021–2025 under the CBM agenda item. Some were included in the agreed text, whereas others were not retained during the negotiation process. Nevertheless, they constitute an important source of knowledge for appraising how States understood CBMs during the last OEWG on ICT security.

3.1. Establishment and operationalization of the Global Intergovernmental POC Directory

As outlined in Section 2, the Global Intergovernmental POC Directory became the central anchor for CBM discussions during the OEWG sessions. Over time, and despite initial hesitation raised by a few States on different issues (e.g., United Nations capacity, budget, its role in relation to existing networks and regional POC directories, and the respect of sovereignty),[45] a step-by-step approach meant that a compromise was possible, and it gave way to broader acceptance of the establishment of the POC directory. Discussions thus shifted from endorsing the importance of the directory to discussing how POCs should function in practice, including ping tests, meetings, simulations and exercises, and communication templates. These operational and technical details were seemingly more widely acceptable because they were anchored within the framework of the POC directory, rather than in separate, standalone CBMs.

The agreed texts strongly reflect the deliberations during the substantive sessions. Yet, the OEWG 2021–2025 did not address or resolve all issues related to the POC directory; practical operationalization work is needed for the Global Intergovernmental POC Directory to operate effectively, including agreement on a voluntary, standard communication template, which remains an open question for the Global Mechanism.

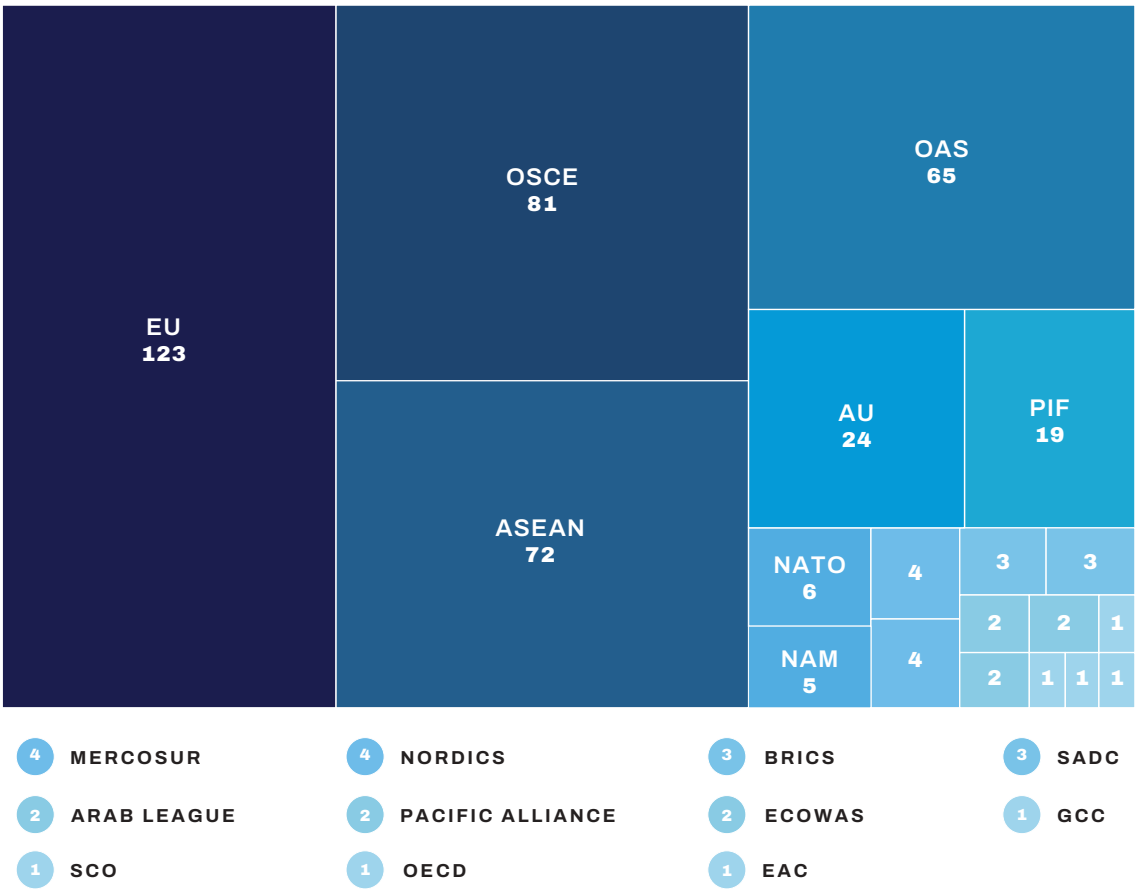
45 For example, United States (session 2, meeting 7; session 3, meeting 4); China (session 3, meeting 3).

3.2. Regional organizations and cross-regional cooperation

Throughout the sessions, States repeatedly referenced regional and subregional experiences (see Figure 2), both as sources of learning from existing practices and as additional examples for addressing and fostering cooperation in the context of CBMs. Cross-regional cooperation was also frequently cited as an important factor in building confidence. Over time, the emphasis of the interventions shifted from general praise for regional and cross-regional activities to a more functional focus on the role of regional and subregional organizations in operationalizing and implementing global and regional CBMs, including contributions to or alignment with the Global Intergovernmental POC Directory.[46] The APRs recognize the value of regional and subregional efforts, especially as an opportunity for States to further engage in cooperative exercises.[47]

FIGURE 3.

Mentions of regional and subregional organizations and other State groupings in States' statements during the CBM sessions of OEWG 2021–2025



46 For example, Brunei Darussalam on behalf of ASEAN (session 4, meeting 6); European Union (session 6, meeting 6); Dominican Republic (session 10, meeting 6).

47 A/77/275,12; General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, 2023, Annex B.

Moreover, cross-regional cooperation was recognized as a CBM in the initial list of voluntary global CBMs (CBM 2; see Table 2), underscoring that cross-regional exchanges are a crucial opportunity for sharing lessons learned and best practices.[48] However, while reference to the contribution of regional and cross-regional cooperation was consistently reflected, regional and cross-regional discussions were not elaborated in detail in any of the agreed texts.

3.3. Capacity-building for CBMs

Capacity-building has become an increasingly central theme for CBMs and their effective implementation. In this context, States particularly referred to the crucial importance of capacity-building for the implementation of the Global Intergovernmental POC Directory.[49] As the operationalization of the directory progressed, an increasing number of delegations emphasized that effective participation depends on training and resources, particularly for developing countries and small States.[50]

This practical emphasis on capacity-building and CBMs is well reflected in the official outcomes of the OEWG. For example, Annex A of the second APR includes a dedicated section on capacity-building for the development and operationalization of the POC directory, which outlines concrete actions to be undertaken by the Secretariat.[51]

3.4. Transparency and information-sharing

Transparency and information-sharing often featured as a topic of discussion during State interventions. Statements on transparency and information-sharing routinely mentioned voluntary exchanges of national approaches, doctrines and relevant information to reduce misinterpretation and enhance predictability. States also often referred to practical tools that could be used for this purpose. For example, the UNIDIR Cyber Policy Portal was frequently cited in the context of CBMs as a resource that supports transparency, and it was included as supporting text for CBM 3 (see Table 1).[52] Additionally, some delegations advocated for repositories or portals to make information accessible and comparable.[53]

Overall, the agreed texts, including CBM 3 on information-sharing, outlined transparency and information-sharing elements in voluntary, non-prescriptive terms, avoiding language that would have created more specific or demanding expectations.[54]

---

48 A/78/265, Annex B.

49 For example, Chile (session 2, meeting 7); Iran (Islamic Republic of) (session 5, meeting 4); Fiji on behalf of the Cross-Regional Confidence Builders Group (session 5, meeting 4); Egypt on behalf of the Group of the Arab States (Session 6, meeting 6); Sri Lanka (Session 6, meeting 6); Czechia (session 6, meeting 7); Russian Federation (session 7, meeting 7); Thailand (session 10, meeting 5).

50 For example, Tonga on behalf of the Member States of the Pacific Islands Forum (session 10, meeting 5); Laos DPR (session 10, meeting 5); Ghana (session 10, meeting 5); Australia (session 6, meeting 6).

51 A/78/265, Annex A, paragraph 13.

52 A/78/265, Annex B, 26.

53 For example, India's presentation on a proposed global cybersecurity co-operation portal (GCSCP) (session 6, meeting 7); Croatia (session 3, meeting 3); Kenya (session 5, meeting 4); Singapore (session 10, meeting 5).

54 For example, a few States proposed transparency measures regarding States' cyber capabilities; however, this understanding of transparency did not receive additional support.

3.5. Technical cooperation (including CSIRT/CERT cooperation)

Technical cooperation, especially through CSIRT/CERT cooperation, was repeatedly framed as a practical complement to more political and diplomatic measures. Indeed, cooperation among incident-response teams (CSIRTs and CERTs) was described as a useful channel for voluntary information exchange and collective incident response.[55] Throughout the sessions, some States explored the possibility of establishing a new CBM on technical cooperation,[56] drawing also on regional examples. Other statements framed technical cooperation as a tool to reinforce existing CBMs, including in the context of the Global POC Intergovernmental Directory.[57]

In agreed texts, the idea of CSIRT/CERT cooperation is preserved primarily with respect to the POC directory; in particular, the directory is framed as a tool that States may harness "where appropriate", taking into account existing CSIRT/CERT directories.[58] Notwithstanding this, technical cooperation, including in its CSIRT/CERT form, has not been framed as a standalone CBM.

3.6. Protection of critical infrastructure and critical information infrastructure

Under the CBM agenda item, States generally addressed the protection of critical infrastructure and critical information infrastructure through practical proposals (e.g., sharing information, lessons learned and good practices) to reduce risks to this infrastructure and to support cooperative incident prevention and response.[59] Compared with other themes, discussions on the protection of critical infrastructure and critical information infrastructure remained marginal yet at a consistent level across the sessions.

This theme is, nevertheless, clearly institutionalized in the APRs,[60] which explicitly frame the exchange of information on infrastructure protection as a confidence-building measure. The final report emphasizes the importance of implementing the "Initial List of Voluntary Global CBMs" in Annex B of the third APR, thereby carrying forward infrastructure as part of the agreed CBM set.[61]

---

55 For example, Thailand (session 6, meeting 6); Pakistan (session 6, meeting 6); Mauritius (session 7, meeting 7).

56 For example, Ghana (session 7, meeting 7); Colombia (session 7, meeting 7); Mexico (session 7, meeting 7)

57 For example, Singapore (session 2, meeting 7); Thailand (session 7, meeting 7); Argentina (session 7, meeting 7); Russian Federation (session 10, meeting 5).

58 A/78/265, Annex A, paragraph 12.

59 For example, Mauritius (session 3, meeting 5); Switzerland (session 4, meeting 6); Malaysia (session 7, meeting 7); Sierra Leone (session 11, meeting 3).

60 A/79/214, Annex B, 37.

61 General Assembly, Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/80/257, 2025, paragraph 47(g).

3.7. Shared terminology for ICT terms

The possibility of developing a shared terminology of common ICT terms emerged as a recurring yet isolated proposal during the OEWG cycles.[62] Discussions on developing a common glossary took place in parallel under both the agenda item on "Rules, norms and principles"[63] and that on CBMs. In the latter, a few States supported the idea of developing a shared terminology or glossary as a relevant measure to increase cooperation and reduce misunderstandings. This proposal was challenged by other delegations, which voiced explicit opposition and concerns, such as that it would be time-consuming and unsuccessful.[64]

Overall, under the agenda item on CBMs, broader support did not develop, and negotiations resulted in a softer reference in the reports to the voluntary sharing of national views on technical terms, rather than in developing a common understanding of the terms.

3.8. Vulnerability disclosure as a CBM

Some States supported the inclusion of vulnerability disclosure, or responsible reporting of vulnerabilities, as a global CBM.[65] Some of the statements supporting this theme included references to existing regional CBMs on this matter.[66] Certain States framed the proposal as a practical way to strengthen trust in ICT products and services and reduce uncertainty and escalation risks during ICT incidents.[67]

However, in the annual progress reports, vulnerability disclosure did not resolve into a standalone CBM. Instead, references on this matter were included in the second APR in the list of proposals with varying levels of State support, along with the possibility of holding further discussion on the topic during the OEWG 2021–2025.[68] Yet, the third APR and the final report did not include any further text on vulnerability disclosure and instead prioritized the implementation of the agreed global CBMs. In contrast, a more detailed understanding of vulnerability disclosure policy was captured under norm-implementation guidance in the "Rules, norms and principles" pillar, in line with the norm on vulnerability disclosure.[69]

---

62 For example, Argentina (session 1, meeting 8); Iran (Islamic Republic of) (session 2, meeting 7); session 4, meeting 6; session 6, meeting 7); Kazakhstan (session 7, meeting 7); Paraguay (session 9, meeting 7).

63 On this discussion, see the chapter on "Rules, norms and principles" in this volume.

64 For example, the discussions during the third and fifth sessions of the OEWG, when disagreement emerged on including text referring to the development of a common understanding on a glossary in the agreed texts.

65 For example, China (session 10, meeting 5); Netherlands (session 7, meeting 6); Czechia (session 7, meeting 7); Singapore (session 7, meeting 7).

66 For example, Kazakhstan (session 4, meeting 6); Netherlands (session 2, meeting 7); Romania (session 4, meeting 6).

67 For example, China (Session 10, meeting 5).

68 A/78/265, paragraph 37(d).

69 A/79/214, Annex A, Norm j, paragraphs 1–6.

3.9. Multi-stakeholder and private–public partnerships

Throughout the sessions, there was frequent debate on the theme of the multi-stakeholder approach and public–private partnerships. States frequently framed these approaches as practical enablers of CBMs.

Several States acknowledged that, in many instances, non-State actors play a key role in ICT, including the operation of critical infrastructure and in incident response and management.[70] Several States' interventions, therefore, emphasized structured engagement with the private sector, academia, civil society and the technical community to support CBM development and implementation. This would include increasing preparedness and response to ICT threats and protecting the integrity and availability of critical infrastructure and critical information infrastructure.[71]

In contrast, some States emphasized that CBMs should remain State-driven.[72] Therefore, proposals to develop CBMs that addressed specific roles or functions for non-governmental actors – such as ensuring supply chain integrity or establishing dedicated private-sector POCs – were met with caution.[73]

This balance of views regarding the role of non-State actors is reflected in the reports, which frame their involvement in two ways: first, as a CBM (number 8), which stresses the importance of private–public partnerships and cooperation on ICT security; second, in terms of non-State actor engagement in certain aspects of CBMs ("as appropriate").[74] This outcome underscored the widely held view of the primary role of States – a role that, where appropriate, includes contributions by non-State actors to CBM-related activities.

3.10. Inclusivity and gender-sensitive CBMs

Inclusivity and gender issues emerged in the discussions under the CBM agenda item. Many States praised the Women in International Security and Cyberspace Fellowship,[75] which was itself considered to be a CBM.[76] In addition, States also discussed the importance of inclusivity in terms of implementing CBMs. As such, several delegations emphasized that women

---

70 For example, Switzerland on behalf of Switzerland, Serbia and Germany (session 1, meeting 7); Italy on behalf of a group of States (Session 6, Meeting 6); European Union (session 1, meeting 7); India (session 2, meeting 7); Spain (session 4, meeting 6); Georgia (session 8, meeting 3); Ethiopia (session 10, meeting 5); Denmark (session 11, session 4)|

71 See Belgium on behalf of Austria, Belgium, Estonia, Finland, Italy and Sweden (session 4, meeting 6).

72 For example, Russian Federation (session 3, meeting 4).

73 For example, China (session 3, meeting 3); United States (session 3, meeting 4).

74 The latter possibility is listed in the third APR and final report among the list of proposals with varying levels of support. See A/79/214, paragraph 42(g); A/80/257, paragraph 47(i).

75 The Women in International Security and Cyberspace (WIC) Fellowship (or Women in Cyber Fellowship) is an initiative to increase women's representation in United Nations negotiations on cyberspace. The fellowship was coordinated by the Global Forum of Cyber Expertise in partnership with the United Nations Institute for Training and Research (UNITAR) and UNIDIR and sponsored by the Governments of Australia, Canada, Germany, the Netherlands, New Zealand, the United Kingdom and the United States.

76 For example, Albania (session 10, meeting 5); Malaysia (session 10, meeting 5); South Africa (session 10, meeting 5); Fiji (session 10, meeting 6).

should have meaningful opportunities to take part in CBM processes, including in national delegations, technical roles and capacity-building activities that support implementation.[77] Although there were a few references to the possibility of developing new CBMs with a gender focus,[78] these suggestions did not gain enough support, and thus did not develop into a standalone CBM.

3.11. Supply chain security

States addressed supply chain security only marginally in the CBM sessions, primarily in terms of security risks that may undermine trust among States. In general, they discussed this theme with references to the related norm,[79] rather than as a standalone CBM. Limited support was recorded for the proposal to establish an additional CBM specifically addressing supply chain security and market access.[80]

Overall, the list of themes outlines a broad and diverse set of issues that States considered relevant to address in CBM discussions. Some themes were repeatedly raised and discussed throughout the sessions, including the establishment of the Global Intergovernmental POC Directory, the relevance of regional and subregional organizations, and the importance of transparency in building trust in an opaque environment such as cyberspace. Others were raised or discussed in a more limited fashion, such as supply chain security or a common glossary for ICT terms. Nevertheless, the breadth of proposals discussed, including those not ultimately agreed on, remains analytically valuable. It reveals how States interpreted "confidence" in the ICT environment in a specific period of time. Therefore, this record offers both a picture of the relevant issues within a specific timeframe (the early to mid-2020s) and a forward-looking legacy that the Global Mechanism may choose to incorporate into its upcoming sessions.

77 For example, Canada (session 4); Costa Rica (session 4); China (session 3, meeting 5).

78 For example, Argentina (session 4, meeting 6); Germany (session 4, meeting 6).

79 For example, France (session 9, meeting 7).

80 For example, Iran (Islamic Republic of) (session 9, meeting 6); Russian Federation (session 10, meeting 5).

4. Insights beyond the official outcomes

The analysis of the evolution of the discussions and the themes addressed during the OEWG 2021–2025 provides a useful reference for identifying additional insights that can be drawn beyond the OEWG's reports. This section identifies some trends in discussions that supported consensus, as well as reasons why other topics were not successfully consolidated into specific CBMs. These insights may be useful for both the upcoming Chair of the Global Mechanism on ICT Security and the delegations of States that will address some of the legacies of the last OEWG.

With respect to how the Chair and the States managed to find and keep consensus on the initial list of CBMs, as well as how they further developed the CBMs, the following considerations can be made:

1. **Focus on high-feasibility outputs.** The choice to focus the discussions, from the beginning, on themes with a higher degree of feasibility – such as the establishment of the Global Intergovernmental POC Directory,[81] which matured over the course of the GGEs and OEWGs – helped States transition quickly from general statements to more tangible, outcome-oriented discussions. In fact, discussions began early to elaborate on the establishment and subsequent operational aspects of the POC directory.

2. **Anchor the discussion before expanding it.** Throughout the cycles, the Chair and the States managed to preserve consensus on a narrow core, particularly the POC directory, which anchored subsequent discussions. This approach enabled States to be more proactive and to participate in substantive discussions on a range of detailed topics. Discussion of those details would probably have proven more difficult if there were no consensus (i.e., the POC directory proposal) on which to anchor them. With universal support for a directory, States from across the geographic and geopolitical spectrum could more easily engage in, and sometimes converged on, concrete implementation activities such as simulation exercises and communication templates.

3. **Create space for exploratory deliberations.** Overall, the experience of establishing the Global Intergovernmental POC Directory indicates that it may take considerable time for a theme or proposal to gain traction and ultimately be adopted by consensus. It is therefore crucial to leave space for exploratory ideas to circulate and possibly mature. Throughout the cycles, States had opportunities to explore a broad range of proposals for new CBMs, including measures on State transparency regarding their cyber capabilities and on gender-sensitive CBMs. These proposals were not included in the reports, but they may be considered further in future deliberations.

---

81 For example, two of the five guiding questions that the Chair shared before the first substantive session addressed the topic of the points of contact. See Chairperson OEWG 2021–2025, Letter from the Chair, 15 November 2021, https://documents.unoda.org/wp-content/uploads/2021/11/OEWG-2021-2025_Chairs-letter_final.pdf.

As the analysis of the themes that emerged across the cycles indicates, there was a range of issues on which States did not achieve consensus. By looking at States' deliberations on CBMs throughout the cycles, it is possible to observe two trends concerning what hampered agreement on additional CBMs and related measures:

1. **Aversion to intrusive CBMs.** States appeared more reluctant to engage in and agree to "intrusive" CBM – that is, measures considered to impinge upon the voluntary nature of CBMs or perceived as infringing on State sovereignty. Proposals regarding transparency requirements for States' cyber capabilities, mandatory communication templates, and an attribution council[82] did not gain widespread support. In fact, several delegations stressed that CBMs must fully respect State sovereignty and remain voluntary and State-driven, with each State retaining control over the information it shares and the manner in which it implements measures.
2. **Caution on expanding CBMs.** Once States had agreed on the Global Intergovernmental POC Directory and an initial list of CBMs, they appeared to opt for operationalizing existing measures in a step-by-step approach, rather than agreeing to expand them or introduce new ones. Several reasons were cited to justify this preference, including practical constraints (e.g., time, resources and the risk of overburdening States' capabilities). Moreover, it is plausible that States preferred to avoid engaging in additional proposals that could have been politically divisive or technically demanding.

In general, proposals that did not gain support were excluded during the text negotiation sessions. States directly criticized a proposal from another State on only a few occasions. More frequently, proposals that were not favourably received were framed as ideas for future consideration.

In conclusion, States' discussions on CBMs during the OEWG 2021–2025 were shaped from the outset by the early identification of a feasible measure: the establishment of the Global Intergovernmental POC Directory. Its inclusion in the first annual progress report provided an immediate and practical anchor that structured and affected much of the subsequent substantive discussions. At the same time, the process revealed some limits on what could be achieved. Proposals seen as intrusive, politically sensitive, or expanding the scope of CBMs too quickly tended to receive limited support, with delegations repeatedly emphasizing voluntariness, sovereignty, and a step-by-step approach.

Overall, the OEWG discussions on CBMs leave a substantive legacy, both in the agreed measures and the additional inputs, that will inform and support the mandate of the Global Mechanism.

82 For example, Ghana (session 2, meeting 7).

Annex A. Number of times delegations took the floor on CBMs in the OEWG 2021-2025

STATE	COUNT	STATE	COUNT
China (the People's Republic of)	20	Brazil	11
Iran (Islamic Republic of)	19	El Salvador	11
European	18	Indonesia	11
Germany	18	United Kingdom of Great Britain and Northern Ireland	11
Colombia	17	Viet Nam	11
Cuba	17	Kenya	10
Russian Federation	17	Mauritius	10
Australia	16	Uruguay	10
Malaysia	16	Costa Rica	9
Israel	15	Czechia	9
Netherlands (Kingdom of the)	15	New Zealand	9
Singapore	15	United States of America	9
Republic of Korea	15	Kazakhstan	8
Thailand	15	Dominican Republic	7
Chile	14	Italy	7
India	14	Nigeria	7
Mexico	14	Syrian Arab Republic	7
Canada	13	Estonia	6
Egypt	13	Philippines	6
France	13	Albania	5
South Africa	13	Austria	5
Switzerland	13	Bangladesh	5
Argentina	12	Botswana	5
Fiji	12	Ecuador	5
Ghana	12	Lao People's Democratic Republic	5
Japan	12	Nicaragua	5
Pakistan	12	Ukraine	5

STATE	COUNT	STATE	COUNT
Venezuela, Bolivarian Republic of	5	Greece	2
Denmark	4	Kiribati	2
Djibouti	4	Kuwait	2
Finland	4	Lebanon	2
Ireland	4	Morocco	2
Jordan	4	North Macedonia	2
Latvia	4	Poland	2
Paraguay	4	Saudi Arabia	2
Romania	4	Senegal	2
Uganda	4	Sierra Leone	2
Belgium	3	Slovakia	2
Bosnia and Herzegovina	3	Timor-Leste	2
Côte d'Ivoire	3	Algeria	1
Croatia	3	Antigua and Barbuda	1
Hungary	3	Armenia	1
Iraq	3	Belarus	1
Malawi	3	Cambodia	1
Republic of Moldova	3	Cameroon	1
Peru	3	Chad	1
Portugal	3	Georgia	1
Spain	3	Guatemala	1
Sri Lanka	3	Madagascar	1
Sweden	3	Mozambique	1
Vanuatu	3	Democratic People's Republic of Korea	1
Zimbabwe	3	Papua New Guinea	1
Benin	2	Qatar	1
Brunei Darussalam	2	Serbia	1
Burkina Faso	2	Sudan	1
Democratic Republic of the Congo	2	Tonga	1
Ethiopia	2	Tunisia	1