



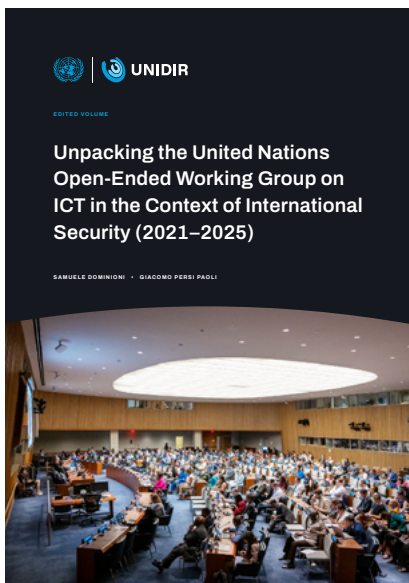
UNIDIR

Chapter title

Capacity-building

Chapter authors

Moliehi Makumane and Dr Ekaterina Martynova



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).



[doi.org/10.37559/SECTEC/26/CR/05](https://doi.org/10.37559/SECTEC/26/CR/05)

# Capacity-building

Moliehi Makumane and Dr Ekaterina Martynova

## 1. Introduction

Cyber capacity-building (CB) constitutes one of the pillars of the United Nations framework for responsible State behaviour in the use of information and communications technologies (ICTs). In the context of the United Nations processes on global ICT security, CB broadly refers to the range of efforts aimed at strengthening the abilities of States to prepare for and respond to malicious ICT activity, as well as to participate meaningfully in international discussions on ICT security, spanning the diplomatic, legal and policy domains. CB thereby serves as an enabling function for the implementation of the other pillars of the normative framework, including compliance with international law and implementation of norms and confidence-building measures (CBMs), while contributing to a more secure and stable ICT environment for all.<sup>1</sup> Unlike traditional technical assistance, CB has increasingly been conceptualized not merely as a development tool but as an essential enabler for the implementation of the broader framework.<sup>2</sup> This means that it encompasses not only the transfer of technical skills but also the building of knowledge and capacity in legal, policy and diplomatic domains.

### 1.1. The road to the OEWG 2021–2025

Capacity-building has long been highlighted as an integral component of the international ICT security agenda. Successive United Nations Groups of Government Experts (GGEs) on developments in the field of ICTs in the context of international security laid the groundwork for recognizing CB as a necessary complement to norms, international law and CBMs. The 2010 GGE report first acknowledged that CB is vital for ensuring global ICT security, assisting developing States in protecting critical infrastructure and bridging the ICT security divide through close international cooperation.<sup>3</sup> The 2013 GGE report then highlighted the importance of cooperation and assistance in strengthening states' abilities to prevent disruptive ICT incidents, and included recommendations on CB measures.<sup>4</sup> The 2015 GGE report explicitly noted that, while normative measures are essential for promoting an open, secure

---

1 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, Annex I, paragraph 54.

2 Giacomo Persi Paoli et al., *Accelerating ICT Security Capacity-Building: Takeaways from the Global Roundtable on ICT Security Capacity-Building* (Geneva: UNIDIR, 2024), <https://unidir.org/publication/accelerating-ict-security-capacity-building-take-aways-from-the-global-roundtable-on-ict-security-capacity-building/>, p. 6.

3 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/65/201](#), 2010, paragraph 17.

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, [A/68/98](#), 2013, paragraphs 30–32.

and stable ICT environment, “their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity”.<sup>5</sup>

The 2021 GGE report reinforced international cooperation and assistance in CB as critical to enabling all States to implement the framework for responsible State behaviour, including by strengthening capacities to detect and respond to threats, protect critical infrastructure, and manage ICT incidents.<sup>6</sup> It underscored the voluntary, politically neutral, mutually beneficial and reciprocal nature of CB,<sup>7</sup> and it encouraged States to adopt a multidisciplinary, multi-stakeholder, modular and measurable approach to cooperation with the United Nations and regional bodies.<sup>8</sup>

The first Open-Ended Working Group (OEWG), in 2019–2021, marked a significant advance in the discussions of CB. Its consensus report articulated a set of guiding principles that frame CB as a sustainable, results-focused and evidence-based process grounded in political neutrality, transparency, accountability and full respect for State sovereignty.<sup>9</sup> This OEWG further underscored that CB should function as a reciprocal endeavour benefiting all participants. It would thereby transform the digital divide into digital opportunities by facilitating the involvement of developing States in relevant discussions and strengthen their resilience through South–South, South–North, triangular and regionally focused cooperation.<sup>10</sup>

These principles and recommendations formed the point of departure for the second OEWG, in 2021–2025. Over four years of deliberations, States moved beyond restating longstanding principles and began engaging in ever more concrete discussions on operationalizing CB. This chapter traces that trajectory, examining the underlying trends and themes that shaped the OEWG negotiations. These include the cross-cutting integration of CB across all pillars of the framework, the persistent operational tensions that arose around centralizing CB coordination within the United Nations, resource mobilization, multi-stakeholder participation, and the boundaries between security-focused CB and broader digital development.

---

5 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 14.

6 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](#), 2021, paragraph 88.

7 [A/76/135](#), paragraph 91.

8 [A/76/135](#), paragraph 92.

9 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, Annex I, paragraph 56.

10 [A/75/816](#), paragraphs 57–58.

## 2. The evolution of the discussions

Discussions on CB during the OEWG 2021–2025 moved through four distinct cycles,<sup>11</sup> from broad reaffirmations of past principles to a focus on implementation tools and delivery methods. For each cycle, this section summarizes the main debates, the negotiating dynamics, and the proposals that States ultimately incorporated into or omitted from the agreed reports.

### 2.1. Establishing the baseline

In the first cycle of the OEWG’s work, States addressed five interconnected issues.

First, some delegations anchored their debates in the principles agreed in 2021 and consistently emphasized “demand-driven, nationally owned and needs-based approaches”.<sup>12</sup>

Second, some States identified priority areas for capacity-building: development of national cybersecurity strategies; establishment of computer security incident response teams (CSIRTs);<sup>13</sup> protection of critical infrastructure;<sup>14</sup> and enhancement of incident response capabilities.<sup>15</sup> The identification of these priorities also raised early questions about where security-focused CB ends and broader digital development begins – a tension that would persist throughout the OEWG 2021–2025.

Third, a few States candidly acknowledged their gaps in ICT or cybersecurity readiness. This included characterization of their capabilities as being at an “infancy stage”,<sup>16</sup> while detailing bilateral partnerships and ongoing negotiations between states’ cybersecurity agencies.<sup>17</sup> This openness about national vulnerabilities enabled productive discussions on matching supply with demand – a principle that would later become central to the OEWG. It also illustrated a broader pattern whereby States increasingly acted simultaneously as both beneficiaries and providers of capacity-building, detailing their own gaps while also showcasing the bilateral partnerships and regional initiatives through which they supported others.<sup>18</sup>

---

11 The analysis divides the OEWG 2021–2025 into four cycles, each running from the substantive sessions through to the negotiation session in which a report was agreed. For further guidance, see the Introduction to this volume.

12 See, for example, Czechia (session 1, meeting 9); Thailand (session 1, meeting 8); El Salvador (session 2, meeting 4); Kenya (session 2, meeting 8); Switzerland (session 2, meeting 8).

13 See, for example, United Kingdom (session 1, meeting 6); Indonesia (session 1, meeting 8); Egypt (session 1, meeting 8); Pakistan (session 2, meeting 8); Brazil (session 2, meeting 9).

14 See, for example, Czechia (session 1, meeting 2); Peru (session 1, meeting 2); India (session 1, meeting 8); Colombia (session 1, meeting 8); Guatemala (session 2, meeting 6); Ghana (session 2, meeting 8).

15 See, for example, Indonesia (session 1, meeting 8); Costa Rica (session 2, meeting 3); India (session 2, meeting 7); Ghana (session 2, meeting 8); Philippines (session 2, meeting 8); Chile (session 3, meeting 8).

16 Philippines (session 1, meeting 8).

17 See, for example, Republic of Korea (session 1, meeting 8); India (session 1, meeting 8); Paraguay (session 2, meeting 6); Côte d’Ivoire (session 2, meeting 8); Kazakhstan (session 3, meeting 2).

18 See, for example, Malaysia (session 1, meeting 8); Brazil (session 1, meeting 9); Colombia (session 2, meeting 8); Lao PDR (session 2, meeting 8); Chile (session 2, meeting 8). See also the intervention by the African Union Cyber Security Experts Group (session 3, meeting 7).

Fourth, divergent views were expressed between those delegations supporting a stronger coordinating role for the United Nations and those cautioning against duplication of existing regional and multi-stakeholder initiatives.<sup>19</sup>

Finally, several delegations highlighted gender perspectives as a cross-cutting concern.<sup>20</sup>

During the negotiation session, only a subset of these issues shaped the drafting of the first annual progress report (APR). The 2021 principles were restated as a stable foundation for further work on CB. The priority areas informed the concrete “menu” of measures later captured in the APR.<sup>21</sup> However, several elements that States had discussed in substantive sessions were omitted or softened: these included United Nations facilitation mechanisms (e.g., a focal point for dialogue and cooperation or a comprehensive calendar of CB programmes).<sup>22</sup> Instead, the first APR recorded a set of next steps, including encouraging States to survey their capacity needs and to continue discussions on how best to coordinate assistance.<sup>23</sup>

As a result, the first APR, agreed in 2022, captured only part of the first phase of discussion. It reaffirmed the 2021 capacity-building principles, acknowledged the breadth of existing initiatives, and framed the OEWG as a platform for exchanging views and for leveraging, rather than duplicating, ongoing work.<sup>24</sup> The more ambitious institutional proposals and sharper political divergences were filtered out.

## 2.2. Building coordination infrastructure

During the second cycle of the OEWG’s work, States continued to discuss CB principles and also addressed several new issues – some revealing convergence of views, while others proving more contested. Considerable convergence emerged around the principles established in the report of the OEWG 2019–2021, with several delegations reaffirming the principles of needs-based tailoring, non-duplication, multi-stakeholder involvement and gender sensitivity as the baseline for any future work.<sup>25</sup> Remarkable agreement also developed around mainstreaming gender perspectives throughout CB initiatives: a number of

---

19 See, for example, the Netherlands cautioning on duplication (session 1, meeting 8); Thailand (session 1, meeting 8); Cuba (session 2, meeting 8); Costa Rica (session 2, meeting 8).

20 See, for example, Malawi (session 2, meeting 9). See also the intervention by the Organization of American States (session 3, meeting 7).

21 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, Section F, paragraph 17(g).

22 Compare Kenya (session 2, meeting 8); India (session 2, meeting 8); Singapore (session 2, meeting 8) with [A/77/275](#), Section F, paragraph 17.

23 [A/77/275](#), paragraph 17(h).

24 [A/77/275](#), paragraph 17.

25 See, for example, European Union (session 4, meeting 7); South Africa (session 4, meeting 7); Netherlands (session 4, meeting 7); Czechia (session 4, meeting 7); Philippines (session 4, meeting 7); Fiji (session 4, meeting 8); Costa Rica (session 5, meeting 4).

delegations praised the Women in Cyber Fellowship programme,<sup>26</sup> and States broadly supported development of tools for incorporating gender dimensions into CB strategies.<sup>27</sup>

On concrete next steps, a Secretariat mapping exercise to inventory CB programmes “within and outside” the United Nations at the global and regional levels gained traction without significant opposition, as did needs-assessment surveys.<sup>28</sup> In contrast, the proposal for a centralized “global cybersecurity cooperation portal” as a coordination hub<sup>29</sup> drew differing views on its scope.<sup>30</sup> Several delegations also urged that it be kept in the descriptive paragraphs of the report until its purpose and relationship to existing platforms were better understood<sup>31</sup> – a cautious approach that would carry into the negotiations.

On other issues, views diverged more sharply. Some delegations advocated for a well-funded permanent United Nations mechanism or dedicated fund for CB.<sup>32</sup> This position remained a minority view in relation to support for coordinating and leveraging existing initiatives. Similarly, although many States proposed references to existing organizations (e.g., the Global Forum on Cyber Expertise), some contested those references, arguing instead for “non-discriminatory” approaches that did not privilege specific entities.<sup>33</sup> These States also pushed for stronger language in the report on fair and non-discriminatory approaches in CB, the principle of “common but differentiated responsibilities” and an explicit prohibition of unilateral coercive measures (e.g., the limiting or blocking of IP addresses, restrictions on the registration of domain names, and the removal of applications from digital marketplaces) that could restrict technology transfer and undermine the ability of developing States to build ICT capacity.<sup>34</sup>

In negotiating the second APR, States addressed these divergences through deliberate choices about what to include, how to phrase it and what level of commitment to assign. The 2021 CB principles were “locked in” as Annex C to the second APR, reinforcing them as the baseline for subsequent discussion on their implementation.<sup>35</sup> The coordination role of the United Nations was consolidated around a set of relatively uncontroversial functions:

---

26 See, for example, Canada (session 4, meeting 7); United Kingdom (session 4, meeting 7); Colombia (session 4, meeting 8); Botswana (session 4, meeting 8); North Macedonia (session 4, meeting 8); Philippines (session 4, meeting 7); Chile (session 4, meeting 7).

27 See, for example, Canada (session 4, meeting 7); Albania (session 4, meeting 7); Costa Rica (session 4, meeting 7); El Salvador (session 4, meeting 7).

28 See, for example, El Salvador (session 4, meeting 7); United Kingdom (session 4, meeting 7); Malawi (session 4, meeting 8); Estonia (session 4, meeting 7).

29 India (session 4, meeting 7).

30 See, for example, Chile (session 4, meeting 7); Russian Federation (session 4, meeting 7); Singapore (session 4, meeting 7).

31 See, for example, New Zealand (session 5, meeting 4); United States (session 5, meeting 4).

32 See, for example, Iran (Islamic Republic of) (session 4, meeting 7); Pakistan (session 4, meeting 7); Syria (session 4, meeting 8).

33 See, for example, Russian Federation (session 4, meeting 7; session 5, meeting 4); Cuba (session 5, meeting 4); Iran (Islamic Republic of) (session 5, meeting 4).

34 See, for example, Cuba (session 4, meeting 7); Iran (Islamic Republic of) (session 4, meeting 7); Nicaragua (session 4, meeting 8); Syria (session 4, meeting 8).

35 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 C; Section F, paragraph 44.

a Secretariat mapping exercise to survey CB programmes at the global and regional levels,<sup>36</sup> and broader United Nations coordination functions to take stock of needs, identify gaps through tools and surveys, and facilitate access.<sup>37</sup> The second APR also introduced practical implementation-support tools, including voluntary checklists and questionnaires to help States identify gaps and to mainstream the agreed principles and gender perspectives into national CB strategies, an updated Cyber Diplomacy e-learning course, and the convening of a global round table to bring together practitioners and stakeholders from both State and non-State backgrounds.<sup>38</sup>

On contested issues, States employed compromise formulations. The portal proposal was retained but with its institutional weight moderated: it was framed as a topic for “continuing discussion” and possible synergy with existing portals, rather than as an agreed deliverable.<sup>39</sup> Several delegations explicitly recommended keeping the portal only in descriptive paragraphs (for ideas still under discussion), rather than elevating it to the “recommended next steps” section (for ideas ready for commitment).<sup>40</sup>

Finally, delegations handled politically charged framings through careful drafting. Some delegations sought to insert language specifying that CB should be “fair, equitable, and unconditionally available”.<sup>41</sup> The final text preserved the underlying concern (about digital divide) while omitting the more prescriptive formulations.<sup>42</sup> Similarly, divergence over whether to name specific non-United Nations coordination platforms was resolved through generalization: the second APR retained the concept of synergy with other existing portals without naming particular entities, stating that “further discussions could take place on how to synergize this portal with other existing portals as appropriate”.<sup>43</sup>

The second APR thus marked a significant step in discussions on the operationalization of CB. While the earlier phase had established what CB should be, this phase focused on what the OEWG and the United Nations system should do next: mapping, convening, developing tools and facilitating coordination. This shift towards operationalization also revealed deeper governance tensions between those favouring centralized United Nations control over CB and those advocating for coordination with existing multi-stakeholder platforms.

---

36 [A/78/265](#), Section F, paragraph 46.

37 [A/78/265](#), paragraph 43(d).

38 [A/78/265](#), paragraphs 48–50.

39 [A/78/265](#), paragraphs 43(f), 47.

40 See, for example, New Zealand (session 5, meeting 4); United States (session 5, meeting 4); Japan (session 5, meeting 4); Australia (session 5, meeting 4).

41 See, for example, Pakistan (session 4, meeting 7; session 5, meeting 4); Cuba (session 4, meeting 7; session 5, meeting 4); Nicaragua (session 5, meeting 4).

42 [A/78/265](#), Section F, paragraphs 43(c–d).

43 Compare Iran (Islamic Republic of) (session 5, meeting 4) with [A/78/265](#), Section F, paragraph 47. See also Egypt (session 5, meeting 1; session 5, meeting 4); Russian Federation (session 5, meeting 4).

## 2.3. Designing operational tools

As the OEWG moved into its third cycle, States engaged with increasing specificity on the design, functionality and some of the administrative arrangements of capacity-building in the context of United Nations processes.

Several delegations acknowledged the efforts of the Secretariat in a mapping exercise to survey the landscape of CB programmes and initiatives.<sup>44</sup> Other delegations proposed structuring the exercise document by listing assistance providers (including states, intergovernmental organizations, regional and subregional organizations, and the private sector) alongside the forms of assistance they offer (e.g., seminars, research and development, training, technology transfer, and other activities).<sup>45</sup>

A notable milestone was the inaugural Global Roundtable on ICT Security Capacity Building on 10 May 2024, which was convened by the OEWG Chair and featuring a video message from the United Nations Secretary-General.<sup>46</sup> The event brought together a number of high-level representatives, experts and stakeholders from over 50 states. It emphasized the urgent need for action, the importance of moving from principles to implementation, and the necessity of inclusive, multi-stakeholder cooperation.<sup>47</sup> The Global Roundtable succeeded in focusing attention on these issues; that said, the limited time available for the meeting constrained its scope for practical matchmaking between stakeholder initiatives and states' needs.

On the design of operational tools, several delegations advanced concrete but diverging proposals: one delegation presented a proposal for a comprehensive United Nations-hosted portal comprised of a capacity-building calendar and an assistance mapping function.<sup>48</sup> Another State proposed establishing a needs-based catalogue as a possible component of the future portal.<sup>49</sup> These differing visions – of a fully specified platform versus a more limited matching tool – reflected an underlying tension between those delegations favouring a centralized United Nations hub and those preferring a lighter coordination function for the United Nations. This debate would sharpen during the APR negotiations.

---

44 See, for example, Kenya (session 6, meeting 7); Bangladesh (session 6, meeting 8); Portugal (session 6, meeting 8); Brazil (session 6, meeting 8); Czechia (session 6, meeting 8); Australia (session 7, meeting 8).

45 See, for example, United States (session 7, meeting 8); Australia (session 7, meeting 8); Bangladesh (session 6, meeting 8); Russian Federation (session 7, meeting 8). The final mapping exercise document is General Assembly, "Mapping Exercise to Survey the Landscape of Capacity-Building Programmes and Initiatives within and outside the United Nations and at the Global and Regional Levels", [A/AC.292/2024/2](#), 2024.

46 United Nations, "Secretary-General's Video Message to the Global Roundtable on Information and Communications Technologies Security Capacity-Building", 10 May 2024, <https://www.un.org/sg/en/content/sg/statements/2024-05-10/secretary-generals-video-message-the-global-roundtable-information-and-communications-technologies-security-capacity-building>.

47 UNIDIR, "Inaugural Global Roundtable on ICT Security Capacity Building: Recap and Key Highlights", 16 May 2024, <https://unidir.org/inaugural-global-roundtable-on-ict-security-capacity-building-recap-and-key-highlights/>.

48 See the intervention by India (session 6, meeting 7).

49 See the intervention by Philippines (session 7, meeting 8).

Differences of view also arose on other issues. Thus, while most delegations supported the inclusion of gender and youth dimensions in the mapping exercise,<sup>50</sup> one delegation characterizing these as “controversial” and calling for a “radical revision” of the structure of the exercise.<sup>51</sup>

During the APR negotiation session, States appeared to filter these proposals through concerns about feasibility, duplication and institutional sustainability. On feasibility and funding, several delegations argued that establishing a United Nations voluntary trust fund was “premature” and should be reframed as something to consider or further discuss once there was more clarity, including on the avoidance of overlap with existing mechanisms.<sup>52</sup> Other duplication concerns also surfaced: some delegations questioned whether a United Nations platform would duplicate existing portals, while others suggested incorporating new functions into the already-launched Global Intergovernmental Points of Contact (POC) Directory to reduce costs.<sup>53</sup> Several delegations sought to anchor portal and fund decisions explicitly in the future permanent mechanism to ensure continuity;<sup>54</sup> others cautioned against deciding timing and modalities before that mechanism was settled.<sup>55</sup>

As a result, States translated substantive proposals into agreed text in the third APR through several compromise formulations. They consolidated the portal and catalogue proposals into a single operational package called the Global ICT Security Cooperation and Capacity-Building Portal, conceived as a Member State-driven, modular platform with an initial role as the official website and practical information hub of the future permanent mechanism, and with an evolution pathway for adding modules over time.<sup>56</sup> The needs-based CB catalogue was retained as a complementary tool, framed to reduce overlap and duplication, with potential integration into the portal.<sup>57</sup> The regular Global Roundtable format was linked to the permanent mechanism, with parameters for equitable geographic representation and support for attendance by developing states.<sup>58</sup> On the voluntary fund – the most debated issue – States did not create the fund but instead used the third APR to mandate the Secretariat to prepare an initial report on design features, management, eligibility, monitoring and evaluation, and avoidance of duplication.<sup>59</sup> Throughout, the third APR emphasized “optimizing

---

50 See, for example, Italy (session 7, meeting 8); United Kingdom (session 7, meeting 8); South Africa (session 7, meeting 8); Australia (session 7, meeting 8).

51 See the intervention by the Russian Federation (session 7, meeting 8).

52 See, for example, New Zealand (session 8, meeting 3); European Union (session 8, meeting 4); Italy (session 8, meeting 4); United States (session 8, meeting 4); Switzerland (session 8, meeting 5); Mexico (session 8, meeting 5); Canada (session 8, meeting 5).

53 Compare, for example, Switzerland (session 8, meeting 5) and Republic of Korea (session 8, meeting 4) with 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, Section F, paragraph 52. See also the chapter on confidence building measures (CBMs) in this volume.

54 See, for example, Argentina (session 7, meeting 9); Australia (session 8, meeting 4); Netherlands (session 8, meeting 4); European Union (session 8, meeting 4); United States (session 8, meeting 4); Germany (session 8, meeting 5); Thailand (session 8, meeting 5).

55 See, for example, Switzerland (session 8, meeting 5); Russian Federation (session 8, meeting 4); Republic of Korea (session 8, meeting 4); Mexico (session 8, meeting 5).

56 [A/79/214](#), Section F, paragraph 52.

57 Ibid.

58 [A/79/214](#), paragraph 53.

59 [A/79/214](#), paragraph 54.

synergies and avoiding duplication” without choosing a concrete operational pathway for how to achieve this.<sup>60</sup>

## 2.4. Consolidating for continuity

In the final cycle’s substantive sessions, States continued to generate increasingly detailed operational proposals while several differences of view sharpened.

One delegation introduced a proposed digital tool to operationalize implementation of the 11 voluntary norms by integrating existing checklists, enabling progress tracking and optional sharing of obstacles and achievements, with potential integration into the broader portal.<sup>61</sup> The Chair also explicitly re-situated CB as cross-cutting – linking threat understanding, norm implementation and international law capacity – and positioned it as a practical connector across pillars, rather than a standalone activity.<sup>62</sup>

At the same time, differences of view sharpened on the issue of financing, particularly during the negotiations on the final report. Some delegations argued that the proposed United Nations voluntary fund was essential to ensure equitable participation and to meet the needs of developing states.<sup>63</sup> Others pointed to United Nations budgetary constraints, the risk of duplicating existing sponsorship schemes (notably the Women in Cyber Fellowship), and their reluctance to commit to new operational United Nations roles without clearer evidence that such a fund would add value.<sup>64</sup>

Moreover, in the final report negotiations, it appeared that States filtered proposals through practical criteria: available financial resources and budgetary constraints,<sup>65</sup> non-duplication of existing mechanisms, best practices and lessons learned, gender dimensions of ICT security, and demonstrated maturity of debate. As a result, the final report consolidated a package of concrete enabling instruments: a regular Global Roundtable format, the Global ICT Security Cooperation and Capacity-Building Portal, and continued work on a voluntary fund.<sup>66</sup> Duplication safeguards were explicitly embedded: the fund should maximize leveraging of existing initiatives and avoid duplication.<sup>67</sup> The final report also captured how CB became increasingly tied to implementation of the other pillars of the United Nations

---

60 [A/79/214](#), paragraph 52.

61 Statement by the delegation of Kuwait (session 9, meeting 7).

62 See Chair’s comments (session 9, meeting 7).

63 See, for example, Uruguay (session 9, meeting 8); Kiribati (session 9, meeting 9); Nigeria on behalf of the African Group (session 11, meeting 3); Brazil (session 11, meeting 3); Iran (Islamic Republic of) (session 11, meeting 3); Egypt (session 11, meeting 8).

64 See, for example, United States (session 11, meeting 3); European Union (session 11, meeting 3); Canada (session 11, meeting 3); Vanuatu (session 11, meeting 3); France (session 11, meeting 3).

65 The broader United Nations liquidity crisis at the time, with 760 million USD in unpaid assessments by the end of 2024 and significant budget cuts under way, is likely to have reinforced the reluctance of several delegations to support new funds or expanded operational roles. See, for example, UN News, “UN Chief Warns Unpaid Dues Near \$1.6 Billion, As Budget Cuts Deepen”, 1 December 2025, <https://news.un.org/en/story/2025/12/1166480>.

66 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, Section F, paragraphs 55–58.

67 [A/80/257](#), paragraph 53(h).



Ambassador Burhan Gafoor, Permanent Representative of the Republic of Singapore to the United Nations, chairs the eleventh substantive session of the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 2025. Credit: UN Photo / Loey Felipe.

framework for responsible State behaviour in cyberspace. This was reflected in proposals for a needs-based CB catalogue and a digital tool for national implementation of voluntary norms and checklists, with potential integration into the portal.<sup>68</sup>

However, this consolidation package did not resolve the deeper governance tensions that had surfaced across the four cycles. The portal's design left open whether it would centralize CB coordination under the auspices of the United Nations or would coordinate among existing initiatives; the voluntary fund's future remained conditioned on further study without resolving the question of private sector participation; the broader tension between multilateral and multi-stakeholder governance persisted despite compromise formulations; and the boundary between security-focused capacity-building and digital development remained ambiguous. These unresolved questions constitute the principal challenges that the dedicated thematic group (DTG) on capacity-building of the Global Mechanism will inherit.<sup>69</sup>

The final report thus marked the culmination of the CB trajectory of the OEWG 2021–2025. What had begun as a reaffirmation of principles in the first cycle, moved to coordination infrastructure in the second and developed into operational tools in the third became consolidated into a more comprehensive operational package. The portal, round table and voluntary fund workstreams, having been narrowed, conditioned and anchored in the Global Mechanism, represented the agreed handover. The result balanced the demand for concrete deliverables with the political realities of divergent positions, financial constraints on the United Nations and the need to demonstrate added value in relation to existing initiatives.

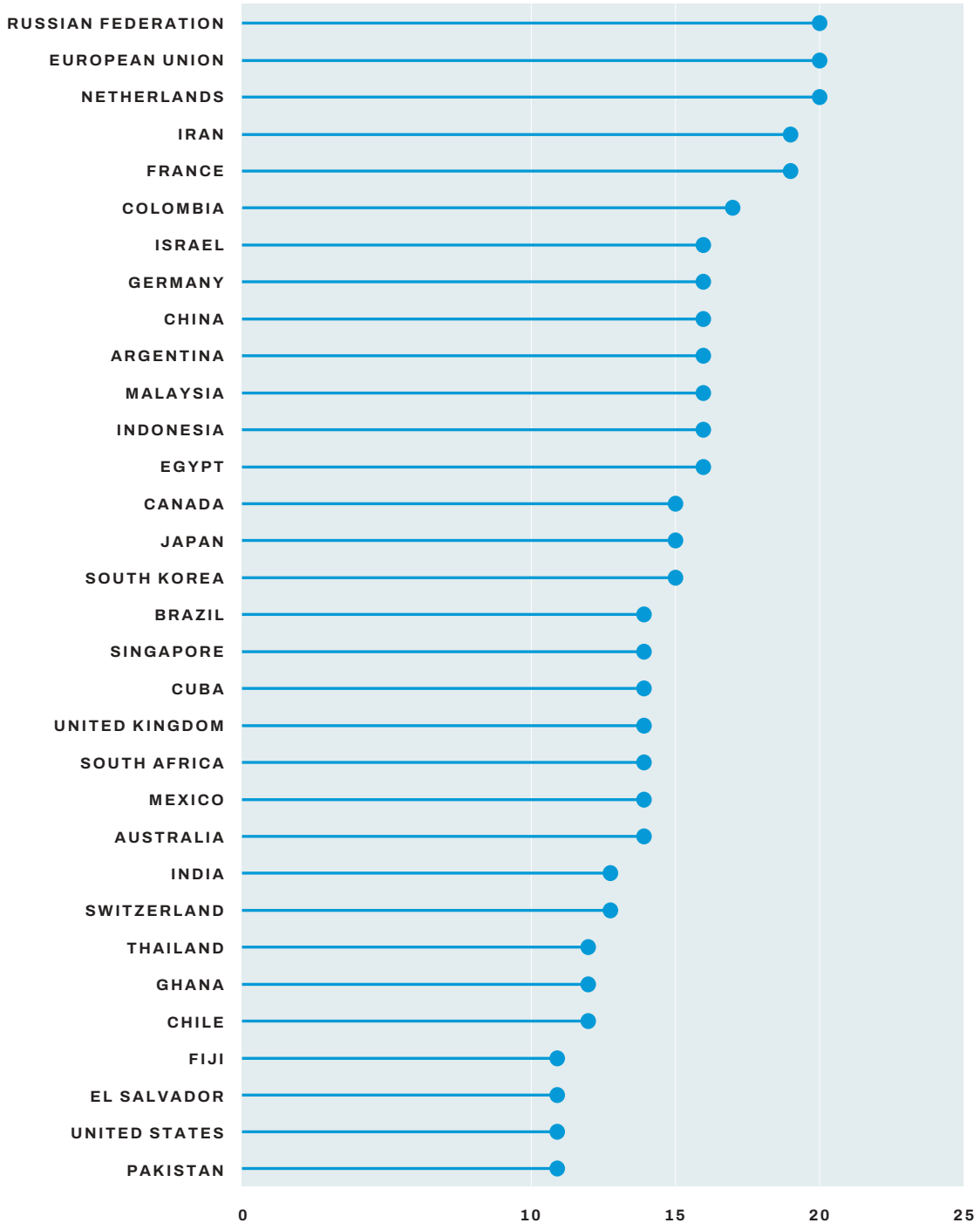
---

68 [A/80/257](#), paragraph 53(f–g).

69 The dedicated thematic group of the global mechanism on accelerating ICT security capacity-building was proposed by a group of 15 delegations in early 2024 and subsequently reflected in the Chair's discussion papers and the OEWG final report as the primary forum for taking forward the capacity-building agenda, including the operationalization of the Global Portal, the voluntary fund and the regular Global Roundtable.

FIGURE 1.

## Number of times delegations took the floor on CB in the OEWG 2021–2025<sup>70</sup>



70 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

This section captures a selected, non-exhaustive list of trends and themes raised in discussions on capacity-building during the OEWG 2021–2025. Some were ultimately reflected in the text of the agreed reports, while others were set aside over the course of negotiations. Taken together, however, they offer useful insight into how States framed, interpreted and prioritized capacity-building within the OEWG process on ICT security.

### 3.1. Donors, recipients and dual roles

Analysis of national statements reveals a model of CB in which States increasingly occupy dual roles as both beneficiaries and providers, moving beyond rigid donor–recipient categories. States took on multiple roles depending on the thematic area, regional context and delivery phase. This approach reflected a shift from passive receipt of assistance towards more active leadership in regional and thematic CB efforts.

Donor States described their role as extending beyond the mere provision of funds: they emphasized commitments to needs-based, demand-driven and sustainable approaches and positioned capacity-building as mutual learning.<sup>71</sup> Recipient States also transformed their interventions – moving from requests for assistance to demonstrations of active engagement in CB activities and leadership roles in their regions; they explicitly identify themselves as both recipients and providers within cooperation arrangements. Examples include the ASEAN–Japan Cyber Security Capacity Building Centre in Bangkok, which trains government officials and critical infrastructure operators regionally, which Thailand hosts while simultaneously benefitting “immensely” from OEWG-related capacity programmes to build its national understanding of international law.<sup>72</sup> Similarly, Montenegro hosts the Western Balkans Cyber Capacity Centre while benefiting from projects offered by the European Commission.<sup>73</sup> Gender-focused programming also featured prominently in the OEWG 2021–2025, with States showcasing mentorship programmes such as HerCyberTracks and the Women in Cyber Fellowship.<sup>74</sup>

---

71 See, for example, Egypt (session 2, meeting 8); European Union (session 2, meeting 8); South Africa (session 10, meeting 7); Tonga (session 10, meeting 7).

72 See, for example, Thailand (session 7, meeting 8; session 11, meeting 3); Japan (session 10, meeting 7).

73 See, for example, Montenegro (session 7, meeting 2).

74 See, for example, European Union (session 7, meeting 8); Germany (session 9, meeting 8); Canada (session 10, meeting 7); Australia (session 10, meeting 7). See also the intervention by the Organization of American States (session 10, meeting 8).

## 3.2. Capacity-building as a cross-cutting dimension of the framework for responsible State behaviour

Several States and regional groups used their interventions during the sessions to specifically link capacity-building to the other pillars of the framework for responsible State behaviour in cyberspace.

In relation to threats, certain delegations argued that CB should form part of discussions on a common understanding of threats and the ability to respond to them.<sup>75</sup> Particular emphasis fell on how emerging technologies (e.g., artificial intelligence, blockchain and deepfakes) would alter the dynamics of future cyberthreats, requiring continuous acquisition of technical knowledge.<sup>76</sup>

On norms, several States advanced the position that CB is a prerequisite for the effective implementation of the 11 voluntary norms, with proposals to list the specific capacities required for implementation of each norm.<sup>77</sup> Another proposal called for a dedicated digital tool to assist States in tracking their implementation of the norms and identifying specific capacity gaps.<sup>78</sup>

On international law, Member States consistently framed CB as a fundamental prerequisite for equal participation in global ICT security discussions.<sup>79</sup> There was widespread recognition that a State unable to articulate its legal position cannot meaningfully contribute to or shape the rules and norms that will eventually bind it.<sup>80</sup> Across sessions, this translated into concrete demands: assistance in developing national position papers, training on the applicability of international law, and regional exercises designed to close the gap between legal theory and operational practice.<sup>81</sup>

On confidence-building measures, several States underscored that CB is a “CBM in itself” because it fosters trust and international cooperation.<sup>82</sup> Some States linked CB directly to the Global Intergovernmental POC Directory, proposing tabletop exercises and “onboarding” tutorials to help States utilize the directory as a practical CBM.<sup>83</sup>

---

75 See, for example, Nigeria on behalf of the African Group (session 10, meeting 6). See also the chapter on existing and potential threats in this volume.

76 See, for example, Dominican Republic (session 4, meeting 7); Uruguay (session 7, meeting 3); Argentina on behalf of 14 States (session 9, meeting 7); Nigeria (session 9, meeting 8)

77 See, for example, Colombia (session 4, meeting 8); Singapore (session 5, meeting 4; session 11, meeting 3). See also the chapter on norms, principles and rules in this volume.

78 See, for example, Kuwait on behalf of Arab Group (session 10, meeting 6); India (session 10, meeting 7).

79 See, for example, Singapore (session 11, meeting 3); Mozambique (session 11, meeting 3). See also the chapter on international law in this volume.

80 See, for example, Tonga (session 10, meeting 7); Mozambique (session 11, meeting 3); Malawi (session 11, meeting 3); Lao PDR (session 11, meeting 4).

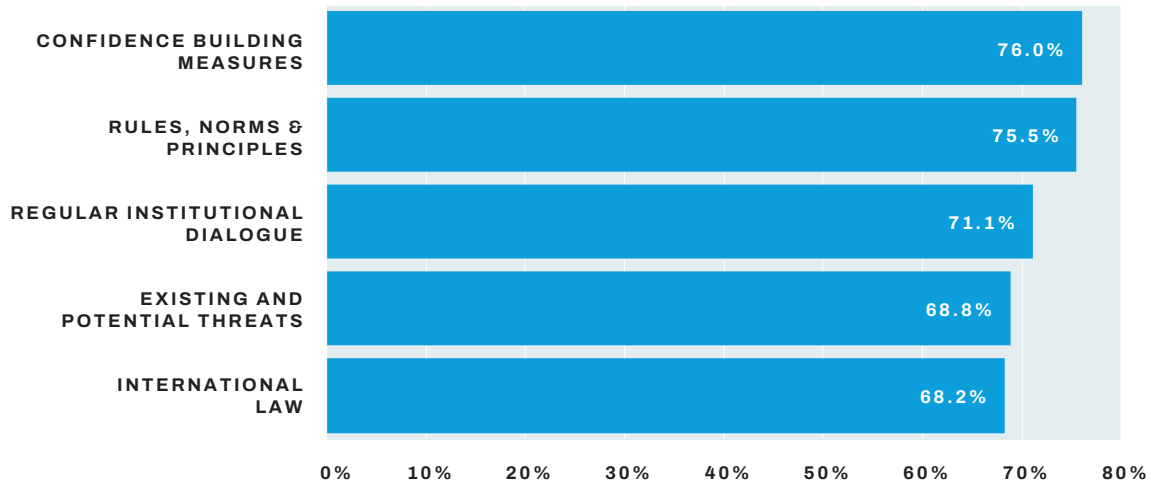
81 For example, Estonia (session 8, meeting 3); Colombia (session 10, meeting 3); Malawi (session 11, meeting 3); Singapore (session 11, meeting 3).

82 See, for example, Argentina on behalf of Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Mexico, Paraguay, Peru, Dominican Republic and Uruguay (session 5, meeting 4); India (session 6, meeting 7); Greece (session 7, meeting 8).

83 See, for example, Czechia (session 4, meeting 7); Antigua and Barbuda (session 6, meeting 9); Indonesia (session 7, meeting 9); Democratic Republic of the Congo (session 8, meeting 3); Thailand (session 11, meeting 3). See also the chapter on confidence-building measures in this volume.

FIGURE 2.

## Proportion of interventions referencing CB across other agenda items



This convergence had a direct institutional consequence. In early 2024, a group of 15 delegations formally proposed that CB should have a “thematic group focused exclusively on this matter” within the future permanent mechanism.<sup>84</sup> The proposal emphasized that CB should not merely be a “standing item” on other agendas but required its own dedicated space and coordinator.<sup>85</sup> The Chair reflected this view in his discussion papers, and his recommendation for the establishment of a dedicated thematic group on accelerating ICT security capacity-building received strong support from states.<sup>86</sup> The final report and the Chair’s element papers added specific content to this DTG to ensure that it remained action-oriented and focused on measurable results.<sup>87</sup>

### 3.3. The portal proposal: centralization versus coordination

The proposal for a Global ICT Security Cooperation and Capacity-Building Portal under United Nations auspices triggered intense debate over whether the United Nations should centralize CB coordination or should instead facilitate coordination among existing initiatives. This debate evolved across the OEWG’s four cycles: from initial proposals for a United Nations coordination hub in the first cycle, through the compromise formulation in the second APR that retained the portal as a topic for “continuing discussion”, to the agreement in the third APR to establish the Global Portal as a Member State-driven, modular platform.

84 See Argentina on behalf of a group of 15 States (session 10, meeting 7).

85 Ibid.

86 See, for example, the Chair’s Discussion Paper on Dedicated Thematic Groups of the Future Permanent Mechanism, 4 April 2025, [https://docs-library.unoda.org/Open-Ended\\_Working\\_Group\\_on\\_Information\\_and\\_Communication\\_Technologies\\_-\\_2021/Letter\\_from\\_OEWG\\_Chair\\_4\\_April\\_2025.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Letter_from_OEWG_Chair_4_April_2025.pdf). See also Iran (Islamic Republic of) (session 10, meeting 7); India (session 10, meeting 7); Indonesia (session 10, meeting 7); Brazil (session 11, meeting 4); Lao PDR (session 11, meeting 4); South Africa (session 11, meeting 4).

87 On the Global Mechanism see also the chapter on regular institutional dialogue in this volume.

States advocating for centralization argued that the United Nations should function as a “one-stop shop” or “central repository” to match needs with resources.<sup>88</sup> These delegations positioned a United Nations-anchored platform as providing a neutral space where developing States could access assistance without political pressure.<sup>89</sup> They emphasized that fragmentation across multiple platforms created barriers for developing States that lack the capacity to navigate complex ecosystems, and that only a mechanism centralized in the United Nations could ensure equitable access free from donor conditionality or commercial interests.<sup>90</sup>

States in favour of coordination over centralization warned against “reinventing the wheel”.<sup>91</sup> These delegations insisted that any United Nations portal must complement, not duplicate, existing multi-stakeholder platforms which already hosted thousands of documents and projects. Creating parallel United Nations infrastructure, they argued, would waste limited resources while undermining successful multi-stakeholder platforms that already provided the functionality that centralists sought.<sup>92</sup>

The Secretariat’s mapping exercise revealed extensive existing programmes both within and outside the United Nations system, documenting dozens of CB initiatives, platforms and coordination mechanisms.<sup>93</sup> This raised fundamental questions of whether coordination challenges stemmed from genuine gaps or from insufficient utilization of available resources. The first APR’s call for States to strengthen coordination provided conceptual guidance, yet States held divergent views about what coordination versus centralization meant in practice.<sup>94</sup> The final report recommended that the future permanent mechanism continue to strengthen coordination and cooperation between States and other interested parties, including businesses, non-governmental organizations and academia.<sup>95</sup> However, how the Global Portal will relate to the mechanism’s coordination functions (and how “strengthening coordination” will operate in practice) remains to be clarified.

### 3.4. Financing capacity-building

Discussions on the voluntary fund proposal revealed a spectrum of views, ranging from support for multi-stakeholder financing to insistence on strict intergovernmental control.

States advocating for multi-stakeholder donation models argued that the fund should benefit from contributions from the ICT private sector, philanthropic foundations and other

---

88 See, for example, Brazil (session 7, meeting 8; session 10, meeting 7); India (session 10, meeting 7).

89 See, for example, Sri Lanka (session 6, meeting 7); Philippines (session 7, meeting 8).

90 Ibid.

91 See, for example, Canada (session 4, meeting 7); United Kingdom (session 6, meeting 8); Australia (session 6, meeting 9); Netherlands (session 10, meeting 7); Samoa (session 10, meeting 8); United States (session 11, meeting 3).

92 Ibid.

93 [A/AC.292/2024/2](#).

94 [A/77/275](#), Section F, paragraphs 17(e), (h).

95 [A/80/257](#), Section F, paragraph 53(k).

stakeholders to ensure diverse and sustainable financing.<sup>96</sup> These delegations characterized such approaches as pragmatic responses to resource constraints that could mobilize significantly greater resources than State contributions alone.<sup>97</sup> Other States expressed strong reservations about private sector financing. They argued that companies and the States backing them might exert pressure on recipient States to influence their national approaches to international information security.<sup>98</sup>

From a different perspective, some delegations characterized a United Nations-managed fund as necessary to ensure that developing States could participate without the political pressure that is inherent in bilateral or stakeholder sponsorship. They positioned the fund as a tool for “equal footing”.<sup>99</sup> Yet, some other States expressed scepticism about new United Nations institutionalization, questioning the operational role of the United Nations. These States noted that successful multi-stakeholder sponsorship programmes (e.g., the Women in Cyber Fellowship) already existed, cautioning that a new United Nations fund might create additional overhead with minimal added value.<sup>100</sup>

A middle ground proposal suggested that the United Nations function as a “clearing house” to link existing initiatives, rather than acting as direct provider.<sup>101</sup> The final report’s consensus that the fund should “maximally leverage on existing initiatives” while remaining under United Nations management represented a compromise.<sup>102</sup> It maintained State control while acknowledging resource-mobilization realities. However, it left two questions unresolved: how to incorporate stakeholder expertise and resources without compromising State decision-making prerogatives, and how the fund’s administrative demands on the Secretariat would be resourced given the broader financial constraints facing the United Nations system – a concern that cut across all thematic areas of the second OEWG’s work.

### 3.5. Multilateral versus multi-stakeholder capacity-building governance

The question of who should design, deliver and coordinate capacity-building generated persistent tensions throughout the OEWG 2021–2025. Beginning at the organizational session in June 2021, the OEWG engaged in recurring negotiations on modalities for stakeholder participation. The adoption of formal modalities providing for participation in meetings for both “relevant non-governmental organizations in consultative status with the Economic and Social Council” and “other interested non-governmental organizations

---

96 See, for example, Argentina (session 10, meeting 7); Mauritius (session 10, meeting 7); Mexico (session 10, meeting 7); Nigeria (session 10, meeting 7).

97 See, for example, Nigeria on behalf of the African Group (session 10, meeting 6); Vanuatu (session 10, meeting 7).

98 See, for example, Russian Federation (session 10, meeting 8); Nicaragua (session 11, meeting 4).

99 See, for example, El Salvador (session 10, meeting 6); Brazil (session 11, meeting 3).

100 See, for example, United States (session 11, meeting 3); France (session 11, meeting 3).

101 See, for example, Singapore (session 1, meeting 8); Japan (session 4, meeting 7); France (session 10, meeting 8).

102 [A/80/257](#), paragraph 53(h).

relevant and competent to the scope and purpose of the OEWG”, along with written submissions, dedicated briefings and informal consultations, did not settle the matter.<sup>103</sup> The tension between multilateral and multi-stakeholder approaches constituted a major area of divergence among Member States.

Some States viewed CB as potentially creating dependencies that donors could exploit for geopolitical advantage.<sup>104</sup> Other States viewed private sector partnerships as pragmatic necessities in a domain where non-State actors often possess superior technical capabilities.<sup>105</sup> They also pointed to the vast number of CB programmes being delivered by stakeholders outside the United Nations – a fact documented by the Secretariat’s mapping exercise. These tensions surfaced concretely in two debates examined above: whether the Global Portal should centralize CB coordination or should coordinate existing initiatives; and whether the voluntary fund should accept private sector contributions or should remain strictly intergovernmental.

The final report achieved consensus by accommodating both perspectives. It commended specific donor-funded initiatives that were working well, satisfying the donor community, while placing institutional developments (e.g., the Global Portal and the voluntary fund) under the direct management of the United Nations to ensure State control, satisfying those concerned about sovereignty.<sup>106</sup> The commitment to establish mechanisms “via a step-by-step modular approach” and to leverage existing initiatives represented formulations that enabled consensus.<sup>107</sup>

### 3.6. Capacity-building and digital development: where the boundaries lie

In their interventions, some States increasingly connected capacity-building to the Sustainable Development Goals (SDGs), arguing that secure digital transformation and development are inseparable.<sup>108</sup> It could be argued that the reasoning was pragmatic: SDG frameworks bring more funding, broader institutional networks and greater political reach than international security processes alone. Connecting CB to development goals made practical sense, but it also blurred the lines between digital development and cybersecurity.

Some States advocated for mainstreaming cybersecurity into the United Nations digital development agenda across the United Nations system. They saw an opportunity to leverage existing funding and coordination mechanisms, rather than creating parallel systems.<sup>109</sup>

---

103 [A/77/275](#), Section II, paragraph 7.

104 See, for example, China (session 10, meeting 6); Venezuela (session 10, meeting 8); Nicaragua (session 11, meeting 7).

105 See, for example, Sri Lanka (session 4, meeting 7); Slovenia (session 4, meeting 7); Vanuatu (session 10, meeting 7); Croatia (session 11, meeting 1).

106 [A/80/257](#), paragraph 56.

107 Ibid.

108 See, for example, the Netherlands (session 7, meeting 8); Rwanda (session 10, meeting 7); Brazil (session 10, meeting 7). See also the Chair remarks (session 8, meeting 3).

109 See, for example, Syria (session 1, meeting 8); Czechia (session 1, meeting 9); Lao PDR (session 2, meeting 8); Fiji on behalf of the Pacific Islands Forum (session 2, meeting 9). See also the intervention by the African Union Cyber Security Experts Group (session 3, meeting 7).

However, such integration would blur the line between security-focused CB and broader digital development. Certain States insisted that the OEWG's scope was to consider ICTs in the context of international security and that it was neither a forum for all ICT issues nor an operational entity.<sup>110</sup> The tension surfaced clearly when CB discussions touched on other aspects of ICTs such as cybercrime (including ransomware affecting non-critical infrastructure) or general digital literacy initiatives. Some States argued that these topics warranted OEWG attention when they reached thresholds affecting international peace and security; others insisted that they belonged in different United Nations processes, such as the Ad Hoc Committee on Cybercrime or development-focused forums.<sup>111</sup> Overall, it appears that linking CB to norms, international law and CBMs had an unintended effect: it expanded the scope of CB beyond international security and into broader development objectives.

The acknowledgement in the final report on integrating capacity-building with SDG frameworks while maintaining focus on "ICTs in the context of international security" represented compromise language – it both preserved flexibility and acknowledged boundary concerns.<sup>112</sup> What served as a workable compromise in the OEWG 2021–2025 will require greater definition as the Global Mechanism on ICT Security moves from principles to practice.

## 4. Insights beyond the official outcomes

The preceding sections trace what States agreed on capacity-building across the OEWG's four cycles. This section steps back to examine how that agreement was reached, what obstacles stood in its way and what remains unresolved. It addresses three sets of insights: the procedural practices that helped build consensus; the definitional and institutional challenges that hampered it; and the legacy issues that the Global Mechanism's dedicated thematic group on capacity-building will inherit.

### 4.1. Procedural practices

The OEWG's procedural design played a decisive role in shaping the CB outcomes documented in Sections 2 and 3. Without it, CB discussions risked becoming a record of statements, rather than a genuine exchange. The Chair, Ambassador Burhan Gafoor, addressed this directly. His use of targeted guiding questions gave delegations a shared focus and moved the conversation forward. Under his direction, the OEWG introduced

---

110 See, for example, European Union (session 4, meeting 7); United States (session 11, meeting 3). The Chair frequently reinforced this boundary, noting that while national cyber strategies do not exist in a vacuum, the OEWG must remain focused on the perspective of the General Assembly's First Committee to ensure that it does not take on developmental burdens regarding the digital divide that it cannot effectively discharge. See the Chair's statements (session 8, meeting 3).

111 On different United Nations processes, see, for example, Nicaragua on behalf of Belarus, Burundi, China, Cuba, Democratic People's Republic of Korea, Eritrea, Iran (Islamic Republic of), Nicaragua, Russian Federation, Syria, Venezuela and Zimbabwe (session 8, meeting 5). On the thresholds for international peace and security see, for example, Austria (session 3, meeting 7); Israel (session 3, meeting 7); Nigeria on behalf of the African Group (session 10, meeting 6).

112 [A/80/257](#), paragraphs 9, 12.

two interlocking tools. First, guiding questions issued ahead of each substantive session shifted debate from declaratory positions towards operational specifics. Second, a phased, incremental approach to proposals helped build convergence, avoid deadlock and keep the process action-oriented despite deep geopolitical divisions. The Chair explicitly framed this as a deliberate strategy, noting that proceeding step-by-step was necessary to achieve concrete progress. He warned against moving too fast and “leaving people behind”.<sup>113</sup> As such, States were invited to discuss not whether to build capacity, but how, for whom and through what mechanisms, and they did so at a pace that kept agreement within reach.

The result was visible in the progress of discussions themselves, from broad reaffirmations in the first cycle to operational tools in the third. By asking about mechanisms for contributing to capacity-building, the Chair prompted States to consider concrete structures (e.g., partnerships for training and research), rather than principles alone. This led States to acknowledge that non-State actors were already playing an important role in delivering CB results, such as incident response training and maturity assessments.<sup>114</sup> Concrete examples of successful partnerships gave the discussion a practical foundation that moved it forward.

Ahead of the March 2023 session, the Chair shared a number of guiding questions, including on concrete topics such as public–private partnerships.<sup>115</sup> The debate shifted from whether stakeholders should participate in capacity-building to how they can participate effectively. The May 2024 Global Roundtable brought ministerial-level engagement and domestic political weight to the process. That momentum supported the conditions in which a proposal for a dedicated capacity-building thematic group in the permanent mechanism became a natural next step.

The Chair’s step-by-step approach also facilitated consensus through gradual commitment. The portal and voluntary fund evolved iteratively: conceptual introduction, detailed State proposals, Secretariat’s technical reports and, finally, a compromise language that enabled consensus while deferring implementation details. This phased approach succeeded because it separated decisions on institutional architecture from decisions on governance authority. States could endorse establishing the portal without definitively resolving whether it would centralize or coordinate CB efforts. Yet the same approach that built consensus also revealed the limits of what that consensus could sustain. When States later turned to implementation, they discovered that they did not always agree on what the terms they had accepted actually meant, nor on where the OEWG’s authority ended and other institutions’ mandates began.

---

113 See Chair’s statement (session 6, meeting 7).

114 See, for example, Saudi Arabia (session 3, meeting 6); United Kingdom (session 3, meeting 6); Canada (session 8, meeting 5); Vanuatu (session 10, meeting 7); Denmark (session 11, meeting 4)

115 See Chair’s letter, 3 March 2023, [https://docs-library.unoda.org/Open-Ended\\_Working\\_Group\\_on\\_Information\\_and\\_Communication\\_Technologies\\_-\\_\\_\(2021\)/Chair's\\_Letter\\_3\\_March\\_2023\\_pdf.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__(2021)/Chair's_Letter_3_March_2023_pdf.pdf), Annex B, “Chair’s Guiding Questions for Focused Discussions, Taking into Account General Assembly Resolution 75/240 and the First Annual Progress Report (A/77/275)”.

## 4.2. Definitional and institutional challenges

The parallel negotiations within the Ad Hoc Committee on Cybercrime created persistent boundary friction, hampering resolution of the questions raised above (in Section 3.6). The Ad Hoc Committee was an intergovernmental body mandated to elaborate a comprehensive international convention to combat the misuse of ICTs for criminal purposes.<sup>116</sup> States repeatedly debated whether ransomware and law enforcement cooperation belonged in OEWG capacity-building or the cybercrime process.<sup>117</sup> Some States argued that ransomware warranted OEWG attention when it crossed the threshold of international security. This position was conceptually coherent (the same capacities serve both purposes) but operationally difficult to apply, as States could not agree on where the OEWG's mandate ended and the Ad Hoc Committee's began.<sup>118</sup> This boundary contestation directly hampered consensus on where the scope of CB ended, and other processes began.

A second obstacle to consensus was definitional ambiguity around core principles. States did not always agree on what the principles they had endorsed actually meant in practice. “Politically neutral”, for example, meant different things to different delegations. For States of the Non-Aligned Movement (NAM), it meant avoiding references to specific organizations, to prevent privileging some over others. For others, acknowledging successful initiatives was not political bias<sup>119</sup> – it was transparency.<sup>120</sup> When the portal proposal prompted suggestions for making reference to existing multi-stakeholder platforms, the same ambiguity resurfaced: was citing them an act of transparency or of privilege?

The wording “without conditions” similarly generated divergent interpretations, hampering consensus on the voluntary fund. Some States read it as prohibiting donor governments from attaching political strings. Others read it more broadly, objecting to proposals that would condition access to the fund on adopting the voluntary checklist or implementing agreed norms. For these delegations, linking financing to implementation benchmarks was itself a condition.<sup>121</sup> This definitional impasse kept the voluntary fund proposal at the level of “continue discussions”.

---

116 See United Nations Office on Drugs and Crime, “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”, [https://www.unodc.org/unodc/en/cybercrime/ad\\_hoc\\_committee/home](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home).

117 On different United Nations processes see, for example, New Zealand (session 3, meeting 3); Czechia (session 3, meeting 4, at 02:16:08); Brazil (session 5, meeting 2); Cuba (session 8, meeting 5; session 11, meeting 1)

118 On the thresholds for international peace and security see, for example, Austria (session 3, meeting 7); Israel (session 3, meeting 7); Nigeria on behalf of the African Group (session 10, meeting 6).

119 See, for example, Egypt (session 5, meeting 4); Russian Federation (session 5, meeting 4).

120 See, for example, Australia (session 7, meeting 8); European Union (session 8, meeting 4).

121 On no political strings, see Syria (session 7, meeting 9); South Africa (session 10, meeting 7). On strict governmental control, see, for example, Iran (Islamic Republic of) (session 10, meeting 7); Russian Federation (session 8, meeting 3).

### 4.3. Legacy issues for the Global Mechanism’s dedicated thematic group

The CB dedicated thematic group of the Global Mechanism inherits three major unresolved issues. First, States will have to decide how to manage the role of the United Nations, specifically with respect to the Global Portal. Coordination has merit in that States can leverage multi-stakeholder resources, yet concerns about political neutrality cannot be dismissed. Second, limited resources and the constantly evolving threat landscape, which makes it difficult to identify and keep pace with the types of capacity States need, remain an open question: should the Global Mechanism accept private sector contributions or maintain strict intergovernmental financing? Third, the boundary between broader digital development, cybercrime and cybersecurity requires definition. States will have to define where one ends and the other begins, or establish working arrangements with relevant bodies. The tension between creating visible new United Nations mechanisms that demonstrate multilateral control and strengthen existing multi-stakeholder platforms while avoiding duplication will require continued diplomatic attention as the permanent mechanism operationalizes its coordination and financing functions.

One shift is worth noting: the line between donors and recipients has blurred. States that once received capacity-building are now delivering it. This is precisely the reciprocal model that the OEWG 2019–2021 envisioned. The Global Mechanism inherits this progress and should build from it.

Across the four cycles of the OEWG 2021–2025, discernible patterns emerged along Global North and Global South lines, although not uniformly. Developing countries, particularly those in the African Group and NAM, consistently advocated for stronger United Nations institutional mechanisms (including a dedicated voluntary fund and a centralized coordination portal) as essential tools to ensure equitable access to capacity-building free from donor conditionality. Their interventions emphasized principles of political neutrality, non-discrimination and the avoidance of unilateral coercive measures that could restrict technology transfer. Conversely, Western States and other traditional donor countries cautioned against duplicating existing multi-stakeholder platforms, expressed reservations about new United Nations institutionalization given budgetary constraints, and favoured coordination over centralization. These divergent perspectives were not static; middle-ground positions emerged, with some developing States acting simultaneously as both beneficiaries and providers of capacity-building, and some donor States emphasizing demand-driven, needs-based approaches. The compromise formulations in the agreed reports (anchoring the portal and voluntary fund within the United Nations while embedding duplication safeguards and mandating further study) reflected an effort to bridge this North–South divide.

The effectiveness of the CB thematic group will depend on whether it can develop operational practices that move past these disputes, or whether persistent disagreements over centralization versus coordination, private sector financing, and the boundaries between security and development will stall implementation despite five years of hard-won progress.

## Annex A. Number of times delegations took the floor on CB in the OEWG 2021–2025

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

| STATE                             | COUNT | STATE                                 | COUNT |
|-----------------------------------|-------|---------------------------------------|-------|
| Croatia                           | 6     | Uganda                                | 3     |
| Vanuatu                           | 5     | Slovakia                              | 3     |
| Malawi                            | 5     | Republic of Moldova                   | 3     |
| Paraguay                          | 5     | Bosnia and Herzegovina                | 2     |
| Venezuela, Bolivarian Republic of | 5     | Burkina Faso                          | 2     |
| New Zealand                       | 5     | Algeria                               | 2     |
| Botswana                          | 5     | Papua New Guinea                      | 2     |
| Lao People's Democratic Republic  | 5     | Sweden                                | 2     |
| Portugal                          | 5     | Romania                               | 2     |
| Greece                            | 5     | Jordan                                | 2     |
| Slovenia                          | 5     | Hungary                               | 2     |
| Saudi Arabia                      | 5     | Antigua and Barbuda                   | 2     |
| Sri Lanka                         | 5     | Qatar                                 | 2     |
| Morocco                           | 4     | Oman                                  | 1     |
| Latvia                            | 4     | Mali                                  | 1     |
| Djibouti                          | 4     | Sierra Leone                          | 1     |
| Kiribati                          | 4     | Türkiye                               | 1     |
| Ireland                           | 4     | Haiti                                 | 1     |
| Austria                           | 4     | Cambodia                              | 1     |
| Rwanda                            | 3     | Sudan                                 | 1     |
| Tonga                             | 3     | Timor-Leste                           | 1     |
| Zimbabwe                          | 3     | Montenegro                            | 1     |
| Mozambique                        | 3     | Brunei Darussalam                     | 1     |
| Democratic Republic of the Congo  | 3     | Democratic People's Republic of Korea | 1     |
| Samoa                             | 3     | Spain                                 | 1     |
| Finland                           | 3     | Georgia                               | 1     |
| Denmark                           | 3     | Armenia                               | 1     |
| Senegal                           | 3     | Madagascar                            | 1     |
| North Macedonia                   | 3     | Benin                                 | 1     |
| Belgium                           | 3     | Chad                                  | 1     |
| Peru                              | 3     | Ethiopia                              | 1     |