UNIDIR

EDITED VOLUME

Unpacking the United Nations Open-Ended Working Group on ICT in the Context of International Security (2021–2025)

SAMUELE DOMINIONI • GIACOMO PERSI PAOLI

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme (SECTEC), which is supported by the Governments of Germany, Italy, the Netherlands, Switzerland, and Microsoft. The editors wish to thank Chimdi Igwe for his contribution to this volume, including his work on data analysis. The editors would like to express their gratitude to the external reviewers who provided invaluable feedback on the chapters, including (in alphabetical order) Allison Pytlak, Chris Painter, Dr. Chen Hui, Elizabeth Kolade, Katherine Prizeman, and two other anonymous reviewers.

About UNIDIR

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

Notes

About the editors

This report was co-edited by Dr Samuele Dominioni, who is a senior researcher in the security and technology programme (UNIDIR), and Dr Giacomo Persi Paoli, who is the head of the security and technology programme (UNIDIR).

Citation

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**.

Cover Image: The eleventh substantive session of the the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 2025.Credit: UN Photo / Loey Felipe.

Acronyms and abbreviations

AI	Artificial intelligence
AU	African Union
APR(S)	Annual Progress Report(s)
ASEAN	Association of Southeast Asian Nations
CB	Capacity-building
CBM(S)	Confidence Building Measure(s)
CERT/	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CI/	Critical infrastructure
CII	Critical information infrastructure
DTG(S)	Dedicated Thematic Group(s)
ECOWAS	Economic Community of West African States
EAC	East African Community
EPT	Existing and potential threats
(THE) FRAMEWORK	The Framework of Responsible State Behaviour in the use of ICTs in the context of international security
GCC	Gulf Cooperation Council
GCSCP	Global Cyber Security Cooperation Portal
GGE(S)	Group(s) of Governmental Experts
GLOBAL MECHANISM	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
ICT(S)	Information and Communication Technology(-ies)
ICRC	International Committee of the Red Cross
IHL	International humanitarian law
IHRL	International human rights law
IL	International law
ILC	International Law Commission
ITU	International Telecommunication Union
LLM(S)	Large language model(s)

NAM	Non-Aligned Movement
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OEWG	Open-ended Working Group
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
OT	Operational technology
PPP(S)	Public-private partnership(s)
POC(S)	Point(s) of Contact
PIF	Pacific Islands Forum
POA	Programme of Action
RID	Regular institutional dialogue
RNP	Rules, Norms and Principles
SADC	Southern African Development Community
SCO	Shanghai Cooperation Organization
UN	United Nations
UNGA	United Nations General Assembly
UNIDIR	United Nations Institute for Disarmament Research
UNITAR	United Nations Institute for Training and Research
UNODA	United Nations Office for Disarmament Affairs
WMD(S)	Weapon(s) of mass destruction

Table of contents

FOREWORD 6

Izumi Nakamizu and Dr Robin Geiss

EXECUTIVE SUMMARY 8

1. INTRODUCTION 10

Dr Samuele Dominioni and Dr Giacomo Persi Paoli

2. EXISTING AND POTENTIAL THREATS 14

Dr Giacomo Persi Paoli, Aamna Rafiq and Chimdi Igwe

3. RULES, NORMS AND PRINCIPLES OF RESPONSIBLE STATE BEHAVIOUR 38

Dr Andraz Kastelic

4. INTERNATIONAL LAW 67

Andrea Gronke and Dominique Steinbrecher

5. CONFIDENCE-BUILDING MEASURES 99

Dr Samuele Dominioni

6. CAPACITY-BUILDING 120

Moliehi Makumane and Dr Ekaterina Martynova

7. REGULAR INSTITUTIONAL DIALOGUE 143

Pavel Mráz and Lenka Filipová

8. CROSS-SECTIONAL ANALYSIS AND CONCLUSIONS 172

Dr Samuele Dominioni and Dr Giacomo Persi Paoli

Foreword

As digital technologies become ever more embedded in societies, economies, critical infrastructure, and military affairs, exploitation of new vulnerabilities and malicious use of these technologies likewise grow in scale, complexity, and consequence. Against this backdrop, the successful conclusion in July 2025 of the Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG 2021–2025) marked an important moment for collective action in tackling these increasing challenges. The OEWG 2021–2025 provided an inclusive forum to strengthen common understandings and advance responsible State behavior in cyberspace.

Under the chairmanship of H. E. Ambassador Burhan Gafoor of Singapore, the OEWG 2021–2025 demonstrated that multilateralism is not a utopian concept, and success is possible. States reached consensus on three Annual Progress Reports (APRs) and a Final Report, which resulted in several institutional innovations, including a Global Intergovernmental Points of Contact Directory and, perhaps most significant, the modalities for a new permanent mechanism on the matter: "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". This agreement initiated the beginning of a new phase for collaborative efforts on this topic.

These concrete achievements were welcomed by UN Secretary General António Guterres, who underscored that even in the most challenging international security environment, collective action remains possible. Indeed, heightened interstate tensions, deepening divisions, and the increasing use of ICT for malicious purposes, including against civilian infrastructure, defined the environment in which the OEWG conducted its work.

This UNIDIR edited volume takes stock of the negotiations that took place throughout the OEWG's mandate with a view to providing a comprehensive and detailed account of the substantive discussions held on the various agenda items across the eleven sessions of the Working Group.

From existing and potential threats to regular institutional dialogue, each chapter of this edited volume unpacks the evolution of the discussions, identifying key milestones, challenges, and negotiation dynamics that led to the successful outcome. It also analyses the wide variety of proposals, ideas, and themes addressed by States during the eleven sessions, including those that did not garner consensus for inclusion in the agreed reports. Last but not least, the volume also identifies cross-cutting themes and consensus-building factors, which facilitated the agreements. The lessons learned can inform not only future work in the area of ICT security but also other disarmament and international security efforts.

The way ahead must build upon the success of the OEWG 2021–2025. The new Global Mechanism offers an opportunity to move from a time-bound process to a permanent forum for dialogue, implementation, and further convergence on ICTs in the context of international security.

Its success will depend on preserving the lessons of the past five years, including the value of gradual progress and inclusive engagement, made possible by the willingness of States to bridge differences even in a difficult geopolitical environment. By carrying forward this institutional memory, the Global Mechanism can build on the OEWG's achievements, address unresolved issues with greater confidence, and help achieve even more ambitious outcomes.

Izumi Nakamitsu
High Representative for Disarmament Affairs

Dr Robin Geiss
UNIDIR Director

Executive summary

This volume examines the United Nations Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (OEWG 2021–2025). Established by General Assembly resolution 75/240, the OEWG 2021-2025 was mandated to continue discussions on existing and potential threats, rules, norms and principles of responsible State behaviour, the application of international law, confidence-building measures, capacity-building and regular institutional dialogue. Throughout its five-year mandate, chaired by Ambassador Burhan Gafoor of Singapore, Member States reached consensus on three annual progress reports and a final report, and agreed that future discussions would continue from 2026 through the 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.

This volume analyses the evolution of discussions across the eleven sessions of the OEWG 2021–2025. It identifies the major themes and trends that emerged and highlights insights that go beyond what was ultimately reflected in the agreed annual progress reports and final report.

On existing and potential threats, the chapter shows that the OEWG 2021-2025 moved beyond simply identifying types of malicious ICT activity. Instead, States increasingly focused on the consequences of such activities, including on how incidents can disrupt critical infrastructure and essential services, spill across borders, involve both State and non-State actors, and affect societies that depend on digital systems. The discussion also linked new and emerging threats, including artificial intelligence and quantum technologies, to broader questions of resilience, cooperation, and capacity-building.

The discussions on rules, norms and principles reaffirmed the centrality of the existing voluntary, non-binding norms of responsible State behaviour. At the same time, they revealed continuing differences among States regarding the future direction of the normative framework. Some States emphasized the implementation of existing commitments, while others called for the development of new norms, rules or legally binding instruments. This divergence did not prevent consensus on the importance of the existing framework, but it limited the extent to which the OEWG 2021-2025 could advance more ambitious normative outcomes.

The OEWG 2021-2025 also confirmed the broad understanding that international law, including the Charter of the United Nations, applies to State use of ICTs. However, Member States continued to differ on how specific rules and principles apply in practice, including sovereignty, non-intervention, the prohibition of the threat or use of force, due diligence, State responsibility and international humanitarian law. The process provided a valuable forum for States to exchange views and develop national positions, while also showing that further work is required to build common understandings on the practical application of international law in the ICT environment.

Confidence-building measures were among the areas in which the OEWG 2021-2025 made the most concrete progress. Discussions moved from reaffirming the value of CBMs to developing practical tools to reduce misunderstanding, misperception and escalation. The establishment and operationalization of the Global Intergovernmental Points of Contact Directory was a particularly significant outcome, providing Member States with a mechanism to facilitate communication and cooperation.

Capacity-building emerged as both a dedicated agenda item and a cross-cutting priority. Member States increasingly treated it not only as technical assistance, but as an enabling condition for the implementation of the entire framework. Discussions addressed national cybersecurity strategies, incident response capacities, critical infrastructure protection, legal and diplomatic expertise, public–private partnerships, coordination of assistance and resource mobilization.

Under regular institutional dialogue, the OEWG 2021-2025 produced one of its most important outcomes. The agreement to establish a permanent Global Mechanism on ICT Security marked the transition from time-bound processes to a standing, inclusive intergovernmental platform under United Nations auspices.

Finally, the volume identifies cross-sectional trends that characterized the OEWG 2021-2025 across its agenda items. These include the movement from reaffirmation to implementation, the shift from general to more grounded discussions, and the conditions that enabled consensus (e.g., a step-by-step approach) and the factors that hampered a more ambitious outcome (e.g., geopolitical tensions).

Altogether, the OEWG 2021–2025 reaffirmed that international cooperation on ICT security is both necessary and possible. Its work underscored the value of dialogue, compromise, and incremental progress in advancing common understandings among States.

Introduction

Dr Samuele Dominioni and Dr Giacomo Persi Paoli

1. Background and purpose of the study

The United Nations has long dealt with the issue of information and communications technology (ICT) and its impact on international security. The General Assembly first addressed this issue in 1998[1] and, starting in 2004, it established six Groups of Governmental Experts (GGEs) and two Open-Ended Working Groups (OEWGs) to study this issue. Four of the GGEs and both OEWGs reached consensus on substantive reports containing conclusions and recommendations that were welcomed by all United Nations Member States. Each group built on the work of its predecessors and generated significant cumulative progress on the issues it considered.[2]

Altogether, these multilateral efforts produced and developed the Framework of Responsible State Behaviour in the Use of ICTs, made up of five pillars: an understanding of existing and potential threats, a set of norms of responsible State behaviour; the affirmation that international law applies in the ICT environment; specific confidence-building measures (CBMs); and cyber capacity-building principles and initiatives. These achievements are the products of decades of intense negotiations among Member States, which, round after round, further advanced their collective understanding of national and international implications of ICTs. In addition, Member States also agreed that starting from 2026, the discussions on these matters will take place in a new permanent forum: the 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.

This edited volume examines the second and last OEWG, which took place between 2021 and 2025. The General Assembly, when establishing the group through resolution 75/240, tasked it with promoting common understandings on rules, norms and principles of responsible State behaviour, existing and emerging threats, how international law applies in the ICT[3] environment, and advancing CBMs and capacity-building.[4] This OEWG (2021–2025) operated under a five-year mandate, a longer duration than is usual for such groups in the area of disarmament and international security; the length of the process enabled more sustained engagement and iterative discussions than previous, shorter processes.

---

1 General Assembly, resolution, 53/70, 1999.

2 Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security", n.d., https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context.

3 Unless otherwise specified, this volume uses the terms "ICT" and "cyber" interchangeably. The use of these terms is in no way intended to convey any normative assessment or value of judgment regarding their nature or scope.

4 General Assembly, resolution 75/240, 2020, paragraph 1.

Throughout the years of negotiations, chaired by Ambassador Burhan Gafoor of Singapore, the Member States reached consensus on three annual progress reports (APRs) and a final report. The OEWG (2021–2025) generated extensive understandings that reflect the perspectives, priorities and concerns of Member States on all aspects of ICTs in the context of international security. Because the OEWG (2021–2025) operated on a consensus basis, not all views could be fully reflected in the agreed APRs or the final report. Nonetheless, the rich discussions held across 11 sessions provided important insights into how States approached each pillar of the Framework of Responsible State Behaviour.

This study analyses these substantive discussions comprehensively. Each of the six chapters focuses on one of the substantive agenda items of the OEWG (2021–2025)'s programme of work: existing and potential threats; rules, norms and principles; international law; confidence-building measures; capacity-building; and regular institutional dialogue. Each addresses three overarching research questions:

I. How did discussions on ICTs in the context of international security evolve throughout the OEWG (2021–2025)'s mandate?
II. What major themes and trends can be observed?
III. What insights emerge from the discussions beyond what was agreed in the APRs and final report?

Each chapter explores the evolution of discussions within the scope of each agenda item, identifies trends and main themes, analyses what drove consensus and what hampered it, assesses the influence of developments in the external international security landscape, and highlights insights applicable beyond the OEWG (2021–2025). The study thus contributes to a comprehensive understanding of how Member States addressed the issue of ICTs and their impact on international security in the OEWG (2021–2025). These findings can help shape future deliberations within the Global Mechanism and beyond.

The primary audience for this study includes diplomats and State representatives engaged in the ICT security discussions. It is also intended for civil society, academia and private-sector actors who, while not always directly involved in the negotiations, seek a deeper understanding of the OEWG (2021–2025) process and its implications for international security, peace and stability.

Participants attending the eleventh substantive session (7-11 July) of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. Credit: UN Photo / Loey Felipe.

2. Structure and methodology

Each of the six thematic chapters in this edited volume follows a defined structure: an introduction; a section that retraces the evolution of the discussion on its agenda item; a section on the main themes and trends that emerged from the discussions; and a concluding section with applicable insights beyond the outcomes of the OEWG (2021–2025). The order of the chapters follows the usual order of the agenda items at meetings of the OEWG (2021–2025).

For analytical purposes, the multi-years mandate has been broken down into smaller segments, named cycles. Each of these cycles started with one or two substantive session(s) and ended with a session in which an agreed text (an annual progress report or the final report) was negotiated (see Figure 1).

FIGURE 1.

Timeline and cycles of the OEWG 2021–2025

Analysis by cycles allows for better retracing of how the discussions evolved and how themes and trends[5] for each agenda item emerged and evolved over time. It also allows for a more accurate comparison of how issues or proposals discussed during the substantive sessions were negotiated and how they were mirrored (or not) in the agreed text at the end of a cycle. This mapping exercise also allowed for the identification of themes and trends across cycles and agenda items.

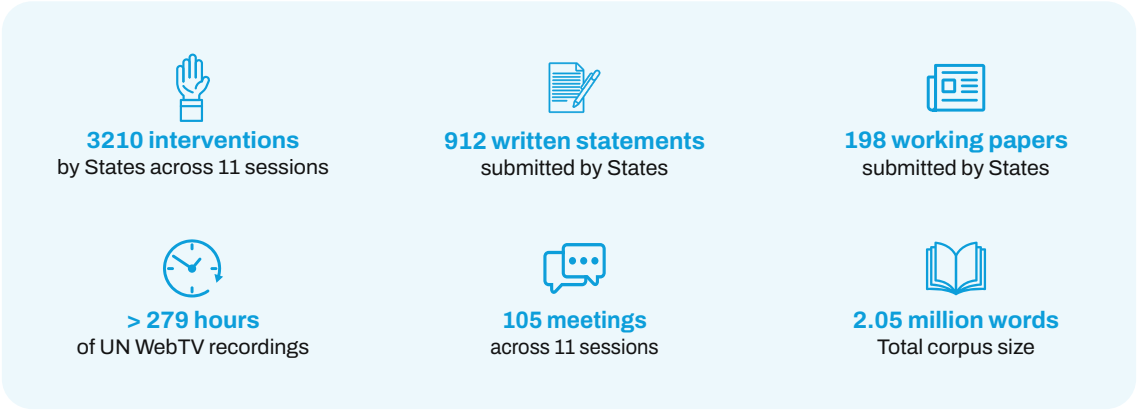
The analysis is based on a broad and diverse corpus of primary and secondary materials. This included 3,210 statements delivered by States; 912 written statements and 198 working papers submitted by States;[6]and official documents, including Chair's letters, annual progress reports and the final report.[7] The analysis also drew on official session recordings

5 "Themes" refer to specific recurring issues debated within each pillar, while "trends" reflect both how Member States understand them over time and other dynamics that were observable across sessions.

6 As the OEWG was a State-led process, the research focused on Member States inputs, and it only partially reflects multi-stakeholder contributions. Nevertheless, given the extreme relevance of the multi-stakeholder community and its expertise on the issues discussed, future research will focus on its contribution to the OEWG process.

7 Available on the Office for Disarmament Affairs Meetings Place, https://meetings.unoda.org/meeting/57871.

available through UN Web TV,[8] amounting to more than 279 hours of material, as well as notes taken by UNIDIR and the Office for Disarmament Affairs and unofficial session transcripts.[9] In total, the corpus analysed exceeded 2 million words.



Given the volume and diversity of the material, the research team adopted a rigorous and systematic methodological approach. First, all relevant data was identified, collected, organized, labelled and reviewed to ensure accuracy, consistency and usability. Second, the material was organized into thematic clusters corresponding to the agenda items set out in the programme of work.[10] Third, the research team conducted a structured content analysis using a combination of manual review and software-assisted coding. This included the use of qualitative analysis tools to identify recurring themes, patterns, and areas of convergence and divergence across the corpus.[11] Fourth, all findings were verified through manual cross-referencing and fact-checking of relevant information against the source material.

Finally, the research team interpreted and synthesized the data in relation to the research questions guiding the study. Following the drafting of each chapter, the report underwent a multilayered quality assurance process. This included two rounds of internal review, followed by feedback from seven external reviewers selected on the basis of their subject-matter expertise, while also taking into account geographical diversity.

8 UN Web TV, "Open-Ended Working Group on Security of and in the Use of ICT", https://webtv.un.org/en/search/categories/meetings-events/general-assembly/subsidiary-organs-general-assembly/open-ended-working-group-security-and-use-ict (last accessed 25 March 2026).

9 Including those available at CyberCapacity, "UN Open-ended Working Group (OEWG) Transcripts", https://cybercapacity.org/resources/oewg-transcripts/.

10 The analysis captured statements made during and pertaining to the agenda items according to the programme of work. Interventions made outside the programme of work or agenda items may not have been captured.

11 Qualitative and quantitative content analysis was supported by a variety of software, including Microsoft Copilot, NotebookLM, ChatGPT-5.2 and Python 3.11.

Existing and potential threats

Dr Giacomo Persi Paoli, Aamna Rafiq and Chimdi Igwe

1. Introduction

The agenda item "Existing and potential threats in the sphere of information security" (EPT) underpins how States recognize, understand, prioritize and respond to the rapidly evolving threat landscape in information and communications technologies (ICT). It was thus a critical pillar of the mandate of the Open-Ended Working Group (OEWG) on security of and in the use of ICTs 2021–2025. Throughout the OEWG 2021–2025, the deliberations on EPT progressed from the identification of a wide range of existing and emerging threats to discussions that, while remaining at the general level, had a narrower focus shaped by observable real-world trends and impacts. These discussions became an important opportunity for States to reflect on both their current experiences dealing with ICT threats and their views on broader trends related to the evolution of the threat landscape.

The work of the OEWG was influenced by several real-world events that occurred during or shortly before the process began, which had an impact on States' perception of the threat landscape and thus influenced the direction of the discussions. These events included:

- Incidents involving the use of ICTs in the context of the conflict in Ukraine[1]
- Incidents involving the explosion of personal communications devices across Lebanon and Syria[2]
- Several cases of ransomware and distributed denial of service (DDoS) attacks against national governments, institutions and digital infrastructure (e.g. in Albania, Costa Rica, Sudan, Montenegro, the United Kingdom, Malawi and Vanuatu)[3]
- Several high-profile cybersecurity incidents – due to severity of impact, geographical scope or novelty – that occurred in the lead up to or during the OEWG (e.g. SolarWinds, Colonial Pipeline, Microsoft Exchange exploit, "Ghostwriter" campaign)[4]
- Accelerated adoption of artificial intelligence (AI), particularly following the release of ChatGPT in November 2022, and growing concerns over quantum computing

---

1 For example, Netherlands (session 2, meeting 1); Germany (session 2, meeting 4); Russian Federation (session 2, meeting 10; session 7, meeting 3; session 10, meeting 1); Canada (session 4, meeting 2); Romania (session 4, meeting 2); Latvia (session 7, meeting 2); Switzerland (session 8, meeting 3); United Kingdom (session 10, meeting 1).

2 UN News, "UN Appeals for Restraint after Further Devices Explode across Lebanon", 18 September 2024, https://news.un.org/en/story/2024/09/1154486.

3 For example, United Kingdom (session 1, meeting 5; session 10, meeting 1); Ireland (session 2, meeting 4); Costa Rica (session 4, meeting 2); Vanuatu (session 4, meeting 2); Albania (session 4, meeting 3); Sudan (session 6, meeting 2); Montenegro (session 7, meeting 2); Malawi (session 10, meeting 1).

4 For example, Japan (session 1, meeting 3); United Kingdom (session 1, meeting 5); Germany (session 4, meeting 1); Belgium (session 6, meeting 2)

1.1. The road to the OEWG 2021–2025

Since the first-ever draft United Nations General Assembly resolution on "Developments in the field of information and telecommunications in the context of international security" was introduced in 1998,[5] the misuse and exploitation of ICTs with potential impacts on international peace and security have formed the basis of deliberations over the course of more than two decades. General Assembly resolution 53/70 called upon the Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security.

The EPT pillar remained at the centre stage in all six Groups of Governmental Experts (GGE) on ICT security. Although the first GGE could not agree a consensus report in 2004, its extensive deliberations touched on a wide range of EPT issues, including the use of ICTs for the generation and dissemination of disruptive online content and weaponization of ICTs by states. In 2010, the final report of the second GGE highlighted the increasing use of ICTs as instruments of terrorism, in connection with armed conflict and for the conduct of intelligence operations. It also noted attacks on critical infrastructure (CI) and critical information infrastructure (CII) and disruption of ICT supply chains by States and non-State actors, including criminal organizations and terrorist groups acting as proxies.[6] Deliberations of the third GGE and its final report in 2013 successfully carried forward all existing and potential threats highlighted by the previous GGE, along with the introduction of new themes, such as the risk of mistaken attribution, unintended escalation and intersection with other emerging technologies (e.g. botnets and cloud computing).[7]

As with each new GGE process, several new themes emerged during the deliberations of the fourth GGE in 2014–2015. These included the development of ICTs for military purposes; and malicious use of ICT that directly harms the socioeconomic development of States and the lives and property of ordinary citizens. The final report of the fourth GGE also reflected more on the use of ICTs for terrorist purposes and to spread ICT attacks on CI/CII. Following the failure of the fifth GGE to reach consensus in 2017, the process split into parallel GGE and OEWG processes. The final report of the final GGE in 2021 comprehensively summed up the deliberations of all previous GGEs by reaffirming that "serious ICT threats identified in previous reports persist".[8]

Following the discussion on threats during the first OEWG, both the final consensus report[9] and the Chair's summary provided useful insights into how States' perception of the threat landscape had evolved. Conducting its work against the backdrop of the global Covid-19 pandemic, the OEWG 2019–2021 highlighted the potentially devastating security, economic,

---

5 General Assembly, resolution **53/70**, 1998, p. 2.

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/65/201**, 2010, Section II, paragraphs 4–11.

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, paragraphs 5–10.

8 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, paragraphs 6–14.

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.

Ambassador 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, 2025. Credit: UN Photo / Manuel Elías.

social and humanitarian consequences of malicious ICT activities on the CI/CII that support essential services to the public. These included risks to specific critical sectors such as healthcare and public health systems, energy grids, water supplies, and others.[10] The OEWG also brought attention to the proliferation of harmful ICT tools and vulnerabilities, including the rise of ransomware, and raised concerns over the increasing frequency and sophistication of ICT operations executed or sponsored by States.[11] The Chair's summary of the first OEWG is a useful resource to capture some of the nuances around the consensus text.[12] It shows how some threat-related themes were either fully excluded from the final report or significantly toned down. For example, threats deriving from disinformation, interference with electoral processes or vulnerability stockpiling were generalized or framed exclusively as technical measures in the consensus report but had been the subject of a much richer debate during the OEWG's deliberations.[13]

Unlike other substantive issues discussed by the first OEWG – including the pillars of the framework of responsible State behaviour in cyberspace – the final report did not include any clear recommendation on the topic of existing and potential threats for States to take on in future negotiations. This choice possibly had an impact on how the EPT theme was taken forward in the second OEWG: that is, as a more dynamic context within which to anchor all other discussions, rather than as an agenda item with a clear pathway for development.

10 A/75/816, Annex I, Section A, paragraphs 3–5, 20

11 A/75/816, Annex I, Section B, paragraphs 15–23

12 A/75/816, Annex II, Section B

13 Compare A/75/816, Annex I, Section B, paragraph 18, with Annex II, Section B, paragraph 7.

2. Evolution of the discussions

Over the course of the OEWG 2021–2025, discussions under the agenda item on existing and potential threats evolved in four main cycles.[14] This section takes a longitudinal approach to State interventions in the EPT pillar, particularly in how they contextualize further proposals, positions and negotiations within other thematic discussions.

2.1. Mapping the threat landscape

Just as the Covid-19 pandemic shaped State interventions during earlier discussions on existing threats in cyberspace, a similar dynamic emerged during the first cycle of the second OEWG. States explicitly noted the criticality of ICT systems to their social, economic and political stability and continuity.[15] Similarly, increasing geopolitical tensions and outbreaks of regional conflict led delegations to both denounce military actions by States – both offline and online – and reflect on the increasing potential for conflict to extend into the ICT domain.[16]

Alongside increasing concerns around the militarization of the ICT domain – framed primarily as an encroachment on sovereignty and territorial integrity[17] – States noted the credible threats to international and national security posed by non-State actors such as criminal, terrorist and politically motivated hacktivist groups.[18] To some States, these concerns were exacerbated by what they viewed as potential legal "grey areas" – particularly the view that ambiguities over State responsibility afforded States a degree of deniability and freedom from culpability under existing international law.[19]

Among the most salient of State concerns was protection of CI/CII. Across this initial cycle, delegations underscored the centrality of this issue to their engagement with the second OEWG process, with many using their interventions to emphasize their concerns through anecdotal experiences.[20] Despite universal agreement on the criticality of CI/CII protection,

---

14 Consistent with the rest of this volume, this analysis divides the OEWG 2021–2025 into four cycles, with each incorporating the substantive and outcome negotiation sessions before negotiation of the annual progress report (APR). On this approach, see also the introduction to this volume.

15 For example, Czechia (session 1, meeting 2); Bangladesh (session 1, meeting 2); Pakistan (session 1, meeting 2); Côte d'Ivoire (session 1, meeting 3); Ireland (session 1, meeting 3); Kenya (session 1, meeting 4); Argentina (session 1, meeting 5).

16 For example, Cuba (session 1, meeting 2); Ukraine (session 2, meeting 1).
On cyber conflict more generally, see, for example, Syria (session 1, meeting 3); Ukraine (session 2, meeting 1); European Union on behalf of 36 States (session 2, meeting 3); Venezuela (session 2, meeting 4).

17 For example, Indonesia on behalf of the Non-Aligned Movement (session 1, meeting 2); Syria (session 1, meeting 3); Ethiopia (session 1, meeting 4); Iran (Islamic Republic of) (session 1, meeting 4).

18 For example, Peru (session 1, meeting 2); Côte d'Ivoire (session 1, meeting 3); Guatemala (session 1, meeting 3); South Africa (session 1, meeting 4); India (session 1, meeting 4); South Africa (session 1, meeting 4); France (session 1, meeting 5); Brazil (session 1, meeting 5); Pakistan (session 2, meeting 4).

19 For example, Belarus (session 1, meeting 2); India (session 1, meeting 6). For further examination of the legal dimensions of the deliberations, see the chapter on international law in this volume.

20 For example, Czechia (session 1, meeting 2); Peru (session 1, meeting 2); United States (session 2, meeting 3); United Kingdom (session 2, meeting 3); Ghana (session 2, meeting 4); Ukraine (session 2, meeting 5).

differing understandings of the term itself prompted a proposal that it be delineated[21] – an initiative which itself was met with contestation within the chamber.

While concerns were raised over threats such as disinformation campaigns[22] and cyber surveillance via spyware,[23] ransomware attacks were highlighted by many delegations as a pre-eminent threat to their social and political welfare.[24] This was underlined by its increasing commercial availability, such as "as-a-service" models.[25] Subsuming economic and developmental fears over the interconnected nature of the global ICT supply chains – and their emergent fragility to ICT incidents – delegations also noted the generation of multiple points of vulnerability for both hardware and software products as a result of their inherent complexity. In this regard, they referenced incidents such as the SolarWinds' Orion platform and the Apache Log4j vulnerability.[26]

Although data security is explicitly mentioned in the second OEWG's mandate on existing and potential threats,[27] discourse on the topic, while present, took on a peripheral role in the cycle's deliberations. Informing this discussion was the proposal for a Global Data Security Initiative,[28] which, among other aims, sought to regulate cross-border data flows with the question of State sovereignty. Disagreement both over the proposal and the OEWG's remit in this regard[29] meant that the first annual progress report (APR) reflected minimal progress on the topic.[30]

Alongside substantive debate, interventions also highlighted procedural and institutional concerns. Disagreements over non-standardization of terminology led to a deliberation on the necessity for a common glossary of cyberthreat terminology.[31] In a similar vein, debate

---

21 For example, Colombia (session 2, meeting 4); Ecuador (session 2, meeting 4); Russian Federation (session 2, meeting 7); European Union (session 3, meeting 1); Australia (session 3, meeting 2); United States (session 3, meeting 4).

22 For example, Switzerland (session 1, meeting 2); Pakistan (session 1, meeting 5); Syria (session 1, meeting 5); Russian Federation (session 2, meeting 3); Iran (Islamic Republic of) (session 2, meeting 3); Cameroon (session 3, meeting 2).

23 For example, China (session 1, meeting 4); Costa Rica (session 1, meeting 5); Venezuela (session 2, meeting 4); Czechia (session 3, meeting 2).

24 For example, Romania (session 1, meeting 3); Israel (session 1, meeting 3); Ireland (session 1, meeting 3); Singapore (session 1, meeting 4); South Africa (session 1, meeting 4); Canada (session 2, meeting 3); Ghana (session 2, meeting 4); Costa Rica (session 3, meeting 1).

25 For example, Singapore (session 1, meeting 4); Israel (session 1, meeting 5); Denmark (session 1, meeting 5); France (session 2, meeting 4).

26 For example, Singapore (session 1, meeting 4; session 2, meeting 3); United Kingdom (session 1, meeting 5); Nigeria (session 1, meeting 5); Denmark (session 1, meeting 5); France (session 1, meeting 5); Pakistan (session 2, meeting 4).

27 General Assembly, resolution **75/240**, 2021, operative paragraph 1.

28 See "Global Initiative on Data Security", Submitted by China, 1 December 2021, **https://documents.unoda.org/wp-content/uploads/2022/03/Position-paper-Global-Initiative-on-Data-Security-submitted-by-China.pdf**.

29 For statements in favour of the proposal, see, for example, Syria (session 1, meeting 5; session 2, meeting 4); Russian Federation (session 2, meeting 3). For interventions critical of its inclusion, see, for example, European Union (session 3, meeting 1); United Kingdom (session 3, meeting 4).

30 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, Annex, Section B, paragraph 13.

31 For interventions in support of common terminology, see, for example, Cuba (session 1, meeting 5; session 2, meeting 3; session 3, meeting 2); Iran (Islamic Republic of) (session 1, meeting 4); Russian Federation (session 1, meeting 6); Syria (session 2, meeting 6). For more critical perspectives, see, for example, Australia (session 1, meeting 7); United States (session 3, meeting 2); European Union (session 3, meeting 3); United Kingdom (session 3, meeting 4).

emerged over potential scope creep of the second OEWG's mandate, given the wide range of State concerns in the ICT domain – such as Internet fragmentation,[32] cybercrime[33] and terrorism via cyber means.[34] Some States referred to processes lying beyond the mandate of the second OEWG and the General Assembly's First Committee at large, such as the ongoing Ad Hoc Committee on Cybercrime.[35]

2.2. The advent of AI

Where interventions on emerging threats in the first cycle were broad in scope, in the second cycle States approached the EPT discussion with increased clarity and focus, building on common understanding established in the first session.

While concerns around CI/CII and established threats such as ransomware continued to feature heavily, a greater focus on emerging technologies started to take root. Where the first APR noted the increase in the attack surface due to "new and emerging technologies", the conversation deepened during the second cycle following the release of consumer-facing products based on large language models (LLMs) such as OpenAI's ChatGPT in November 2022.[36] Interventions reflected not only on the potential for LLMs to exacerbate conventional cybercrime[37] and misinformation,[38] but also on novel threats through autonomous decision-making[39] and the impact of bias in LLM training data sets.[40] While concerns were widespread, support for discussions on the topic was not universal; a number of like-minded States raised concerns over an overstep of the OEWG's mandate into the work of other United Nations processes.[41]

As in the first cycle,[42] many States – particularly in the Global South – brought up differences in cyber capacities and capabilities both as a threat multiplier and as a threat to global ICT

---

32 For example, Spain (session 1, meeting 4); Netherlands (session 1, meeting 5); France (session 1, meeting 5); China (session 1, meeting 4; session 3, meeting 1).

33 For example, United Kingdom (session 1, meeting 5; session 3, meeting 4); China (session 3, meeting 1); European Union (session 3, meeting 1); Netherlands (session 3, meeting 2); United States (session 3, meeting 2); Jordan (session 3, meeting 3); Brazil (session 3, meeting 2).

34 For example, Côte d'Ivoire (session 1, meeting 3); Australia (session 1, meeting 5); Syria (session 1, meeting 3); Iraq (session 1, meeting 5); Indonesia on behalf of NAM (session 2, meeting 3); Jordan (session 3, meeting 3).

35 For example, Australia (session 3, meeting 2); European Union (session 3, meeting 1); Netherlands (session 3, meeting 2).

36 For example, El Salvador (session 4, meeting 1); Germany (session 4, meeting 1); Singapore (session 4, meeting 2); Mauritius (session 4, meeting 3); Kenya (session 4, meeting 1).

37 For example, El Salvador (session 4, meeting 1); France (session 4, meeting 2); Ireland (session 5, meeting 2).

38 For example, Bangladesh (session 4, meeting 2); Kenya (session 5, meeting 1); Mauritius (session 4, meeting 3).

39 For example, El Salvador (session 4, meeting 1); Germany (session 4, meeting 1); Czechia (session 4, meeting 1); Japan (session 4, meeting 2); France (session 4, meeting 2).

40 For example, Germany (session 4, meeting 1); Australia (session 4, meeting 2).

41 For example, China (session 4, meeting 2; session 5, meeting 2); Russian Federation (session 5, meeting 1); Nicaragua on behalf of a like-minded group of States (session 5, meeting 1).

42 For example, India (session 1, meeting 2; session 2, meeting 3); Peru (session 1, meeting 2); Slovenia (session 1, meeting 3); South Africa (session 1, meeting 8); Indonesia (session 1, meeting 8); Egypt (session 1, meeting 8).

security in itself.[43] A number evoked a "weakest link" analogy to emphasize this perspective.[44] In this vein, a proposal on a voluntary United Nations cyberthreat repository – submitted in a draft working paper[45] – saw much interest from Member States across the sessions.[46] Despite the proposal not being included in the second APR because of concerns over potential politicization,[47] the underlying discussion was reflected by the inclusion of capacity considerations within the threats section.[48] This demonstrated the increasingly cross-cutting impact of capacity-building considerations on the process.[49]

Considerations of marginalized identities within threat perspectives were a significant undercurrent of the discussions, such as disproportionate technology-facilitated abuse and discrimination.[50] While discussions around gender perspectives on threats in the ICT domain were included in the second APR,[51] States went further in their considerations of other marginalized identities, such as considering youth, disabled populations and certain professions (e.g., journalists) as targets of ICT malfeasance.[52]

2.3. Electoral and institutional resilience

The third APR cycle occurred against the backdrop of a flurry of democratic activity in 2024, which some referred to a "super year" for elections – a period in which over 70 States conducted national electoral processes.[53] Accordingly, during discussions States explicitly signposted the potential for election interference through disinformation and other content-related activities.[54] These concerns were positioned within wider, more established concerns about possible erosion of trust in public institutions.[55] Concurrently, outbreak of

---

43 For example, Vanuatu (session 4, meeting 2); Malawi (session 4, meeting 5).

44 For example, Israel (session 4, meeting 2); Brazil (session 4, meeting 2); Kenya (session 4, meeting 9); Timor-Leste (session 5, meeting 4); Venezuela (session 5, meeting 4).

45 See, "Updated Draft Working Paper on the Establishment of a Threat Repository within the United Nations", Submitted by Kenya, 21 July 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated18July23Kenya_Draft_Working_Paper_Threat_Repository.pdf; also Kenya (session 4, meeting 1).

46 For example, Philippines (session 4, meeting 1); Argentina (session 4, meeting 1); India (session 4, meeting 2); Ghana (session 4, meeting 2); Belgium (session 4, meeting 2); Ecuador (session 4, meeting 3); Spain (session 4, meeting 6); Germany (session 5, meeting 1); Republic of Korea (session 5, meeting 1); Chile (session 5, meeting 2); Czechia (session 5, meeting 2); Ireland (session 5, meeting 2).

47 For example, Nicaragua (session 5, meeting 1); Philippines (session 5, meeting 2); China (session 5, meeting 2); Cuba (session 5, meeting 2); Kenya (session 5, meeting 7).

48 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, Section B, paragraphs 18–20.

49 For further discussion of the cross-cutting nature of capacity-building within the OEWG discussions, see the chapter on capacity-building in this volume.

50 For example, Sri Lanka (session 4, meeting 1); Chile (session 4, meeting 1); Australia (session 4, meeting 2); Costa Rica (session 4, meeting 7).

51 A/78/265, Annex, Section B, paragraph 18.

52 For example, Kenya (session 4, meeting 1; session 5, meeting 1); Costa Rica (session 4, meeting 7; session 5, meeting 2); Nigeria (session 5, meeting 5).

53 United Nations Development Programme. "A 'Super Year' for Elections", 2024, https://www.undp.org/super-year-elections.

54 For example, United Kingdom (session 6, meeting 1); Canada (session 6, meeting 1); Japan (session 6, meeting 2); European Union (session 7, meeting 2); Brazil (session 7, meeting 3).

55 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, Annex, Section B, paragraph 15.

new conflict prompted States to take a multi-level approach to threats and risks. In addition to widespread concerns about the spillover effects on civilians[56] and international humanitarian organizations[57] of the hybridized ICT–kinetic operations of modern warfare, several delegations supported consideration of a real-world victim-centric framing of harm. This led to a proposal put forward for a Committee on Victim Assistance within the future permanent mechanism.[58] However, this proposal did not garner broad support among the majority of delegations in the negotiation phase.[59]

A noticeable evolution in the discourse that emerged in the third APR was the framing of critical infrastructure. Notably, the negotiated text of the third APR distinguishes "critical infrastructure" from "critical information infrastructure",[60] although this operational distinction was neither clarified nor defined. Even more notably, discussions elaborated the distinct vulnerabilities of core technical systems: for example, core international ICT infrastructure such as subsea cables and orbit (satellite) communications systems;[61] and operational technology (OT) and the wider Internet of Things (IoT).[62]

While ransomware continued to dominate State concerns regarding threat vectors, the third APR reflected a shift in the discourse to consider other threat types, such as "wiper malware and trojans, and techniques such as phishing, man-in-the-middle and distributed denial-of-service (DDoS) attacks".[63] In parallel, discussions began to mature on the role and nature of financially motivated cybercrime – particularly those involving cryptocurrencies – within the wider international peace and security landscape. While some States, as in previous cycles, noted the link between ransomware, State-sponsored activities and money laundering via cryptocurrencies,[64] the final report of the 1718 Sanctions Committee in March 2024[65] provided some delegations with a link between such activities and the development of weapons of mass destruction (WMD).[66] In this vein, various States remarked on the wider

---

56 For example, European Union (session 7, meeting 2); Canada (session 6, meeting 1); Netherlands (session 6, meeting 1); Croatia (session 6, meeting 2).

57 A/79/214, Annex, Section B, paragraph 17.

58 See "Working Paper on a Victim-Based Approach", Submitted by Belgium, 6 March 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20240304_Belgium_-_Working_Paper_on_a_victim-based_approach.pdf.

59 For interventions supportive of the proposal, see, for example, Belgium (session 6, meeting 10; session 7, meeting 10); Finland (session 8, meeting 3); New Zealand (session 8, meeting 3); Fiji (session 8, meeting 4); Uganda (session 8, meeting 5). For statements more critical of its inclusion, see, for example, Egypt (session 8, meeting 7); Syria (session 8, meeting 7).

60 A/79/214, Annex, Section B, paragraph 14.

61 For example, Pakistan (session 7, meeting 2); Ireland (session 7, meeting 2); Antigua and Barbuda (session 8, meeting 5).

62 A/79/214, Annex, Section B, paragraph 25.

63 A/79/214, Annex, Section B, paragraph 20.

64 For example, Japan (session 6, meeting 2); Israel (session 6, meeting 2); Estonia (session 6, meeting 2); European Union (session 7, meeting 2); Portugal (session 8, meeting 2); Croatia (session 8, meeting 3); Australia (session 8, meeting 7).

65 Security Council, Final Report of the Panel of Experts Submitted Pursuant to resolution 2680 (2023), S/2024/215, 2024.

66 For example, Republic of Korea (session 6, meeting 1; session 7, meeting 2; session 8, meeting 1); Japan (session 7, meeting 2; session 8, meeting 2); Australia (session 7, meeting 2); United States (session 8, meeting 1).

consequences of criminal and conflict usage of cryptocurrency;[67] this resulted in its eventual inclusion in the third APR[68] – although this was not without criticism of scope creep.[69]

2.4. Towards the Final Report

In the last cycle, the substantive discussions under the EPT pillar progressed towards a more refined scope and characterization of existing and potential threats compared with earlier cycles. During the ninth and tenth substantive sessions, the majority of States reaffirmed their support for consolidating a set of stable, mature and high-impact themes, including ransomware,[70] CI/CII,[71] the military use of ICTs,[72] supply chain risks due to embedded backdoors and undeclared capabilities,[73] blurring boundaries between non-State and State-sponsored activities[74], and emerging technologies (AI and quantum) as a threat multiplier.[75] As discussions progressed to the negotiation phase, ransomware-as-a-service not only re-emerged as a core area but was also elevated and further expanded by connecting with CI/CII and illicit financing, thereby explicitly recognizing the cascading cross-border effects.[76] There were strongly divergent views on framing the blurring lines between the capabilities of State and non-State actors as an issue of international peace and security, rather than a criminal activity.[77] In tandem, AI and quantum shifted from being perceived primarily as threat multipliers to being framed as neutral technologies with dual-use implications.[78]

Various national ICT incidents, explicitly mentioned in delegations' statements, provided context for these convergences and divergences. These included the ransomware attack

---

67 For example, India (session 6, meeting 1); Israel (session 6, meeting 8); Mexico (session 7, meeting 2); Czechia (session 7, meeting 3); Japan (session 8, meeting 2);

68 A/79/214, Annex, Section B, paragraph 20.

69 For example, Russian Federation (session 8, meeting 1); Democratic People's Republic of Korea (session 8, meeting 3); Nicaragua on behalf of Belarus, Burundi, China, Cuba, Democratic People's Republic of Korea, Eritrea, Iran, Nicaragua, Russia, Syria, Venezuela and Zimbabwe (session 8, meeting 7).

70 For example, European Union (session 9, meeting 1); Republic of Korea (session 9, meeting 1); Portugal (session 9, meeting 1); Pakistan (session 10, meeting 1); United States (session 10, meeting 1).

71 See also, European Union (session 9, meeting 1); Nigeria on behalf of the African Group (session 10, meeting 1); Pakistan (session 10, meeting 1); El Salvador (session 9, meeting 1); Estonia (session 10, meeting 2).

72 For example, Egypt (session 9, meeting 1); Viet Nam (session 9, meeting 2); China (session 10, meeting 1); United Kingdom (session 10, meeting 1); Uruguay (session 10, meeting 1).

73 For example, European Union (session 9, meeting 1); Iran (Islamic Republic of) (session 9, meeting 1); Egypt (session 9, meeting 1); El Salvador (session 9, meeting 1); Russian Federation (session 10, meeting 1); Kazakhstan (session 10, meeting 1); Iran (Islamic Republic of) (session 10, meeting 2).

74 For example, Portugal (session 9, meeting 1); Japan (session 10, meeting 2); Australia (session 10, meeting 2); European Union (session 11, meeting 1).

75 For example, Singapore (session 9, meeting 1); Republic of Korea (session 9, meeting 1); Egypt (session 9, meeting 1); Pakistan (session 10, meeting 1); El Salvador (session 10, meeting 1); Italy (session 10, meeting 2); Nigeria on behalf of the African Group (session 11, meeting 1).

76 For example, Singapore (session 9, meeting 1); Italy (session 9, meeting 1); New Zealand (session 9, meeting 2); European Union (session 11, meeting 1); Republic of Korea (session 11, meeting 2).

77 For example, Republic of Korea (session 9, meeting 1); Japan (session 10, meeting 2); Switzerland (session 11, meeting 1); Iran (Islamic Republic of) (session 11, meeting 1); Russian Federation (session 11, meeting 1); Belarus (session 11, meeting 5).

78 For example, Republic of Korea (session 9, meeting 1); Italy (session 9, meeting 1); Nigeria (session 10, meeting 1); Pakistan (session 10, meeting 1); Brazil (session 10, meeting 2); Mauritius (session 11, meeting 1); Argentina (session 11, meeting 7).

on Slovakia's land registry offices (2025),[79] retrospective mention of the 2021 ransomware attack on Ireland's public health services,[80] a cyberattack on Albania's critical healthcare infrastructure (ongoing since 2022 and detected in November 2024),[81] DDoS attacks on Germany's critical infrastructure, which resulted in the disruption of healthcare, child benefits and pension services to 1.7 million citizens (2024),[82] exploding communication devices in Lebanon (September 2024),[83] DDoS and phishing attacks on the voter-registration system during the presidential elections in Moldova (November 2024),[84] and cyberattacks during the 2024 Paris Olympics.[85]

States also increasingly situated ICT threats within a broader geopolitical context and evolving conflict dynamics at the regional level, reflecting a visible rise in conflict-related language.[86] Accordingly, these discussions were further refined to reframe the role of ICT operations in connection with armed conflicts.[87]

The Final Report reflected a maturing and progressively structured approach to the EPT pillar. This served as a context-setting foundation for framing the environment within which other pillars were discussed. Building on earlier cycles, the report consolidated a broad spectrum of threats articulated consistently and repeatedly by delegations. At the same time, the report adopted a measured and carefully calibrated tone, with threat characterizations framed in a manner that facilitates consensus while avoiding politically sensitive characterizations.

79 For example, Slovakia (session 9, meeting 3); European Union (session 10, meeting 1).

80 For example, Ireland (session 9, meeting 2).

81 For example, Albania (session 10, meeting 2).

82 For example, Germany (session 9, meeting 1).

83 For example, Iran (Islamic Republic of) (session 9, meeting 1); Egypt (session 9, meeting 1); China (session 9, meeting 2); Russian Federation (session 9, meeting 2).

84 For example, Moldova (session 9, meeting 2).

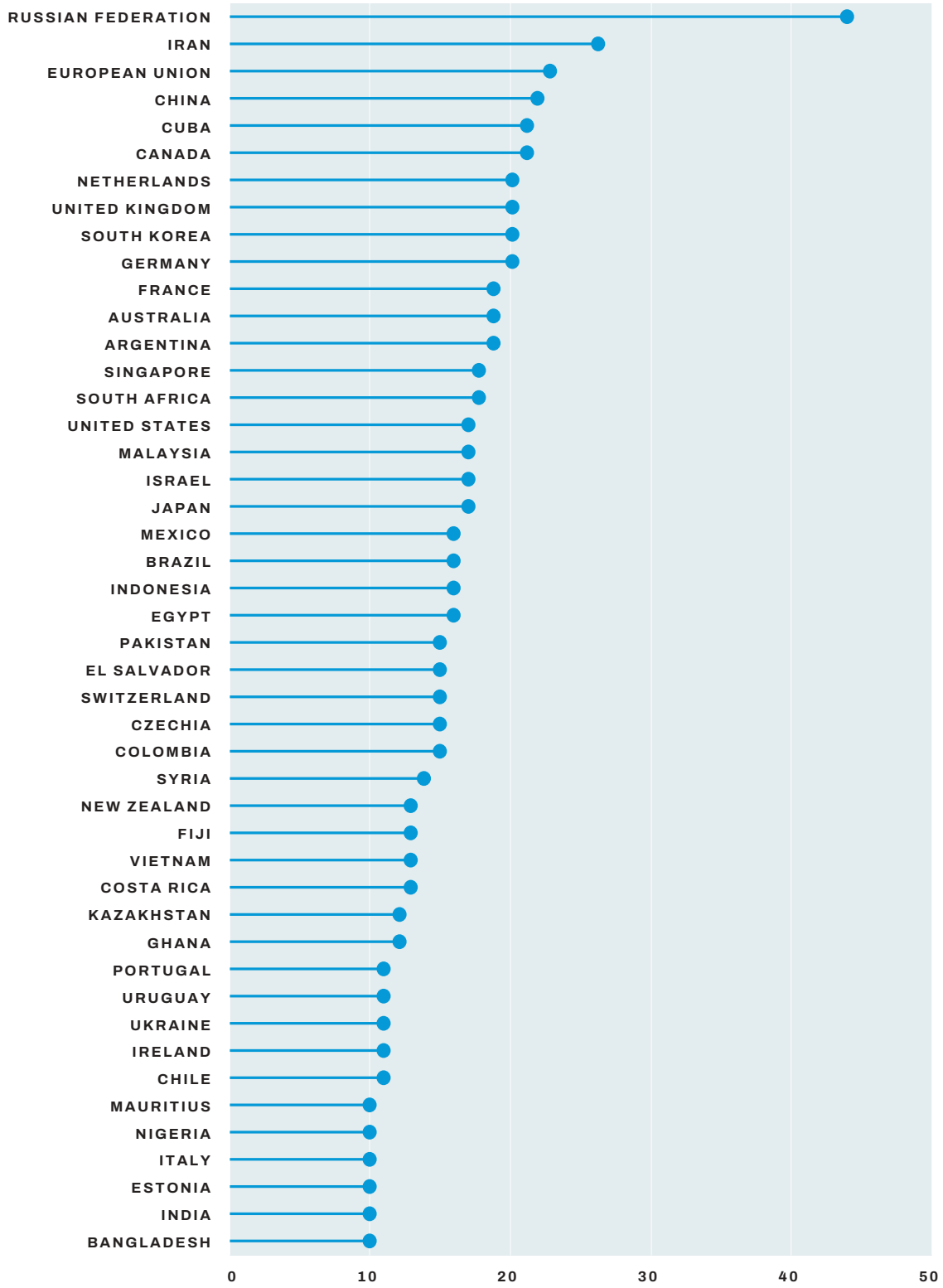
85 For example, France (session 9, meeting 1).

86 For example, Iran (Islamic Republic of) (session 9, meeting 1); China (session 9, meeting 2); Lebanon (session 9, meeting 4); United States (session 10, meeting 1); United Kingdom (session 10, meeting 1); Democratic Republic of the Congo (session 10, meeting 3); Russian Federation (session 10, meeting 1); Egypt (session 11, meeting 1); Albania (session 11, meeting 2); Cuba (session 11, meeting 8).

87 For example, Viet Nam (session 9, meeting 2); Ukraine (session 9, meeting 2); United States (session 11, meeting 1); Mexico (session 11, meeting 3).

FIGURE 1.

Number of times delegations took the floor on EPT in the OEWG 2021–2025[88]



88 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

To complement the chronological analysis above, this section presents the discussions in the OEWG 2021–2025 along three dimensions: threat types, targets and effects, and the role of new and emerging technologies. This approach is intended to provide a more integrated view of how existing and potential threats were understood over the course of the OEWG mandate.

This approach reflects an evolution observed across the OEWG's work. Over time, discussions moved away from a focus on who conducts malicious activity towards a more effects-based understanding of how threats manifest and where their impacts are felt. Questions related to threat actors – whether States or non-State actors, including terrorists and criminal groups – were present throughout, but were more limited in scope.[89] Emphasis was placed on the increasing sophistication of capabilities accessible to non-State actors (including via a growing market of commercially available ICT intrusion capabilities[90]) and on the risk that ICT criminal activity would increase in scale and severity to the point of impacting international peace and security. In addition, a consistent theme remained the extent to which States were integrating ICT capabilities in military operations. Particularly in this regard, a visible division emerged between some States advocating for a complete non-militarization of ICTs[91] and those more openly acknowledging that military ICT capabilities were already being developed and used.[92]

The categories below are introduced as an analytical tool to synthesize the discussions. They do not correspond to formal OEWG classifications, but reflect recurring patterns in delegations' interventions and in the ways these were taken up, partially or fully, in the APRs and Final Report.

3.1. Threat types

Over the course of the OEWG mandate, discussions on threat types evolved from relatively broad listings towards a more focused set of priority threats, shaped both by practical relevance and perceived impact and by breadth of political support. Among these, ransomware emerged as the most consistently emphasized and operationally significant threat.

---

89 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, Annex, Section B, paragraph 16.

90 A/80/257, paragraph 25.

91 For example, Ecuador (session 1, meeting 3); Venezuela (session 2, meeting 4); Pakistan (session 3, meeting 2); Cuba (session 6, meeting 2); Burkina Faso (session 9, meeting 4); Nicaragua on behalf of Belarus, Venezuela, China, Cuba, Eritrea, Iran, Niger, Russia, Sudan, Zimbabwe (session 11, meeting 8).

92 For example, Denmark (session 1, meeting 5); Australia (session 1, meeting 5); Ghana (session 2, meeting 6); Czechia (session 2, meeting 6); Nigeria (session 6, meeting 5); Switzerland (session 7, meeting 3); Viet Nam (session 9, meeting 2). On this point it is interesting to note that similar, potentially related, tensions emerged also in the context of the discussions on international humanitarian law (IHL). Some States argued that emphasizing the applicability of IHL could be seen as legitimizing the use of cyber capabilities in conflict, Others supported the argument that cyber capabilities could be used in conflict, provided that IHL is respected. For a more detailed discussion on this dynamic, see the chapter on international law in this volume.

Delegations increasingly framed ransomware not as isolated criminal activity, but as a growing threat to critical infrastructure and essential services, with frequency, scale and severity that may have an impact on international peace and security.[93]

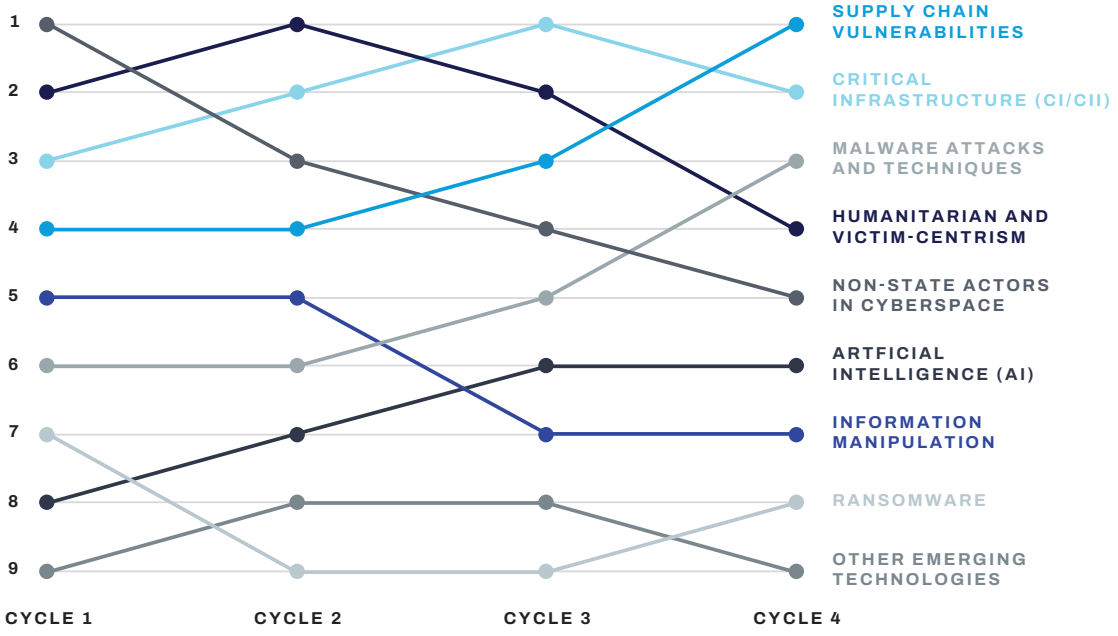
In parallel, discussions highlighted supply chain vulnerabilities, including risks associated with compromised products, hidden functions and dependencies on external providers. Over time, these concerns were increasingly articulated in technical and life cycle approaches, with emphasis on product integrity and "security-by-design",[94] rather than broader geopolitical narratives.

Other threat types (e.g. ICT-enabled information manipulation) appeared more intermittently and with divergent views. While some delegations emphasized their destabilizing potential, others expressed caution regarding scope and framing. This resulted in their eventual inclusion in narrow and carefully bounded terms in the Final Report.[95]

Across these discussions, a broader shift was observable: rather than categorizing threats primarily by the identity of the actor, delegations increasingly focused on the nature of the activity and its potential impact. This allowed for a degree of convergence despite differing views on attribution and responsibility.

FIGURE 2.

Relative prominence of selected EPT themes across all State interventions by OEWG cycle.[96]



93 A/80/257, paragraph 24. See also Singapore (session 1, meeting 4); European Union (session 1, meeting 4); Israel (session 3, meeting 2); Costa Rica (session 4, meeting 2); Canada (session 5, meeting 2); Australia (session 8, meeting 7); Nigeria on behalf of the African Group (session 11, meeting 1).

94 A/80/257, paragraph 23. See also Costa Rica (session 2, meeting 3); Malaysia (session 2, meeting 3); France (session 6, meeting 3).

95 A/80/257, paragraph 22.

96 Rankings reflect the relative frequency of State interventions per cycle matched against keyword dictionaries for derived EPT themes.

3.2. Threat targets and effects

As just noted, a central feature of the OEWG's work under the EPT pillar was the progressive shift towards an effects-based framing of threats, with particular emphasis on targets and consequences.

Critical infrastructure and critical information infrastructure emerged early as a shared concern and, over time, became one of the core organizing elements of the EPT pillar. Delegations consistently highlighted the risks posed to essential services, including energy, healthcare, finance and communications (including undersea cables, communications satellites and cloud infrastructure), and the potential for disruption to have wide-ranging societal and economic consequences.[97] As discussions evolved, greater attention was given to interdependencies between systems;[98] the potential for cascading failures;[99] and the cross-border nature of impacts, particularly in relation to globally connected infrastructure such as undersea cables and space-based communications systems.[100] This evolution is reflected in the Final Report, which explicitly recognized both direct and indirect effects, including spillovers across sectors and jurisdictions.[101]

The emphasis on targets and effects also provided a practical way to address particularly divisive issues. For instance, debates on whether certain forms of malicious activity perpetrated by non-State actors fall within the scope of international peace and security were often reframed in terms of scale, severity and systemic impact, rather than legal classification. This allowed delegations to acknowledge that certain activities – regardless of who conducts them – may have consequences relevant to international peace and security.[102]

At the same time, the discussion also reflected how the impact of ICT threats is not limited to systems or infrastructure but extends to a range of actors. In addition to States and public institutions, the Final Report made explicit reference to risks affecting, among others, international and humanitarian organizations as well as individuals, including those in vulnerable situations. This broadened the understanding of targets beyond purely technical or institutional categories.

---

97 For example, Czechia (session 1, meeting 2); Peru (session 1, meeting 2); Türkiye (session 2, meeting 4); France (session 4, meeting 2); Republic of Korea (session 5, meeting 1); Guatemala (session 6, meeting 2); Pakistan (session 7, meeting 2); European Union (session 11, meeting 1); Nigeria on behalf of the African Group (session 11, meeting 1).

98 For example, Switzerland (session 1, meeting 5); El Salvador (session 2, meeting 5); Australia (session 4, meeting 2); Slovakia (session 7, meeting 5).

99 For example, Thailand (session 1, meeting 2); United States (session 4, meeting 1); India (session 5, meeting 4); Venezuela (session 8, meeting 1); Mauritius (session 8, meeting 1); China (session 9, meeting 2).

100 For example, United States (session 2, meeting 3); Djibouti (session 2, meeting 7); Brazil (session 7, meeting 3); Ireland (session 9, meeting 2); Kazakhstan (session 10, meeting 1).

101 **A/80/257**, Section B, paragraphs 17–19.

102 **A/80/257**, Section B, paragraph 16.

3.3. Role of new and emerging technologies

The role of emerging technologies in the EPT pillar evolved from general concern about future risks to a more precise and integrated analysis of how these technologies shape both the threat landscape and the solution landscape.[103]

In earlier stages, technologies such as AI and quantum computing were often referenced in forward-looking terms. With the contemporaneous emergence of commercial, multimodal large language models, these discussions became more concrete in their formulations.[104] Delegations identified specific ways in which these technologies could:

- Introduce and exploit new vulnerabilities (e.g. security of AI systems)[105]
- Lower the barriers to entry for undertaking malicious activities[106]
- Increase the scale and speed of malicious activity (e.g. AI malware generation)[107]
- Enhance deception and influence operations (e.g. deepfakes)[108]
- Undermine existing security mechanisms (e.g. impact of quantum computing on encryption)[109]

In parallel to the discussions on risks and threats emerging from new technologies, a second discussion thread highlighted the potential of these technologies to strengthen ICT security and resilience. They could do this by improving threat detection and response;[110] enhancing network monitoring and anomaly detection;[111] and supporting more proactive and adaptive defensive measures.[112] This dual perspective is reflected in the Final Report, which reaffirmed the neutrality of technologies and their inherit potential to both expand development opportunities and make the threat landscape more complex.[113]

As discussions matured, emerging technologies were therefore less frequently treated as stand-alone categories of concern and more often understood as “threat multipliers” and “capability enablers” operating across the threat landscape. This framing proved more resilient to negotiation dynamics, as it allowed delegations to acknowledge both risks and benefits without adopting deterministic or alarmist positions.[114]

---

103 A/80/257, paragraphs 26–27. Cf. A/77/275, Annex, Section B, paragraph 11.

104 A/80/257, paragraph 26.

105 For example, El Salvador (session 4, meeting 1); Kenya (session 4, meeting 1); United Kingdom (session 6, meeting 1).

106 For example, Malaysia (session 4, meeting 2); Germany (session 7, meeting 3); Portugal (session 9, meeting 1).

107 For example, Japan (session 4, meeting 2); El Salvador (session 4, meeting 1); Croatia (session 7, meeting 3).

108 For example, Bangladesh (session 4, meeting 2); Ghana (session 6, meeting 2).

109 For example, Canada (session 4, meeting 2); Mauritius (session 4, meeting 3); El Salvador (session 6, meeting 1).

110 For example, Malaysia (session 4, meeting 2); United States (session 6, meeting 1; session 9, meeting 1); Israel (session 6, meeting 2); South Africa (session 9, meeting 1).

111 For example, Uruguay (session 7, meeting 2); Switzerland (session 7, meeting 3); Albania (session 10, meeting 2).

112 See, for, example, El Salvador (session 4, meeting 1); Latvia (session 7, meeting 2); Malaysia (session 8, meeting 1).

113 A/80/257, Section B, paragraph 26.

114 Compare the language in A/80/257, Section B, paragraph 26, to A/78/265, Section B, paragraph 17.

4. Insights beyond the official outcomes

A notable feature of the OEWG's thematic discussion on existing and potential threats was the progressive broadening and deepening of participation by delegations. This was particularly visible in the later stages of the mandate, where a large number of delegations used the EPT discussion to share national and regional threat experiences, identify priority risks, and propose practical areas for future work.

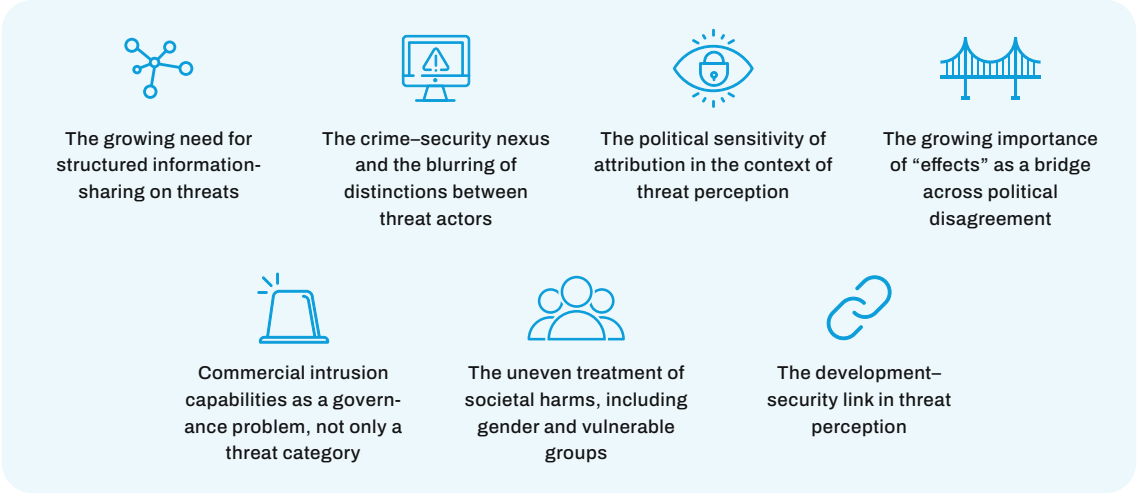
More significantly, the quality and technical depth of interventions increased over time. Earlier discussions often referred to broad categories of concern, such as malicious ICT activity, ransomware, critical infrastructure and emerging technologies. Later interventions were more likely to identify specific threat mechanisms (e.g. ransomware-as-a-service, AI-generated malware, deepfakes and post-quantum cryptography), affected sectors and technical dependencies (e.g. industrial control systems, operational technology, cloud services and undersea cables) and mitigation measures (e.g. security-by-design and cooperation among computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs)). This suggests that the OEWG served not only as a negotiating forum, but also as a space for building a more technically informed understanding of the evolving ICT threat landscape.

This qualitative deepening is reflected in the Final Report, whose EPT section contained a considerably more detailed account of the threat landscape than earlier outputs, while still preserving consensus language.[115] Although the result is a negotiated text that may only partially capture the deliberative richness of the process, it nevertheless showed how sustained engagement, supported by the many stakeholder contributions, helped move the discussion from broad threat awareness towards more operationally grounded common understandings.

While the APRs and the Final Report provided an important record of consensus, they did not necessarily capture the full analytical richness of the OEWG's deliberations under the EPT pillar. Several themes emerged repeatedly in discussions but were either only partially reflected in negotiated outcomes, were reframed in more general language or were omitted. These themes are analytically significant because they reveal the breadth of concerns raised by States, which could be useful to inform negotiations in the Global Mechanism on ICT security.

115 **A/80/257**, Section B, paragraphs 14–30.

These include:



4.1. The growing need for structured information-sharing on threats

An insight from the discussions of the OEWG 2021–2025 was the perceived need for more structured ways to share information on existing and potential threats. As discussions became more technically detailed, several delegations moved beyond identifying threat categories and began to ask how States could maintain a shared understanding of a rapidly evolving threat landscape. This was particularly relevant for threats such as ransomware, supply-chain compromise, emerging technologies and attacks on CI, where information is essential for timely awareness and practical mitigation.

The clearest expression of this need was the proposal for a voluntary, non-attributional cyber-threat repository under the United Nations. The proposal envisaged a centralized platform through which States could share information on common threats, threat vectors, indicators of compromise and, where appropriate, mitigation practices. The repository was framed as a tool to deepen common understanding and support preparedness, rather than as an attribution mechanism.[116]

While the proposal was ultimately not reflected in any of the consensus reports, the discussions around it are nevertheless analytically important. Some delegations expressed openness to considering the idea further, while others suggested that it might be better placed under the agenda item on confidence-building measures or connected to existing CERT-to-CERT and technical information-sharing channels.[117]

---

116 "Updated Draft Working Paper", Submitted by Kenya.

117 France (session 5, meeting 2; session 6, meeting 9), for example, indicated openness to discussing "the objectives and potential modalities" of a repository of threats, particularly within the future mechanism, while the United States (session 5, meeting 1; session 6, meeting 8) supported threat information-sharing but cautioned that any new mechanism would need to account for existing technical forums, including CERT-to-CERT channels and public threat advisories.

The fact that the repository proposal did not feature in the APRs or the Final Report should not be read as the resolution of the underlying issue. Rather, it reflects the difficulty of institutionalizing the sharing of threat information in a consensus setting, especially where States may differ on questions of neutrality, attribution, and the appropriate relationship between diplomatic and technical channels and may have significant reservations about sharing threat and vulnerability information, much of which would be classified.

This reveals an important lesson beyond the official outcomes: as the EPT discussion became more operational, delegations increasingly recognized that shared threat awareness is itself a form of capacity-building and confidence-building. The challenge for the Global Mechanism will be to preserve space for practical exchange of threat information while avoiding duplication of existing technical channels and managing sensitivities around attribution and politicization.

4.2. The crime–security nexus and the blurring of distinctions between threat actors

A further insight from the deliberations was that the boundary between the criminal use of ICTs and their use in ways relevant to international peace and security was becoming increasingly difficult to maintain in practice.

This was particularly visible in discussions on ransomware. Several delegations argued, explicitly or implicitly, that the scale, severity and systemic effects of an incident should determine its relevance to the OEWG, rather than the formal classification of the actor as criminal or State-linked. This effects-based framing was especially important for developing a shared basis for discussing ransomware without requiring agreement on attribution or State responsibility (see Subsection 4.4).

Closely related to this was a second, more operational ambiguity: the increasingly blurred landscape of actors involved in malicious ICT activity. Delegations referred to situations involving State actors, non-State actors, criminal groups, proxies, hacktivists and commercially enabled actors, sometimes operating in ways that are difficult to distinguish. Some delegations emphasized the direct or indirect tolerance of non-State actors by States, the operation of cybercriminals from national territory, and the use of commercially available capabilities by both State and non-State actors. While some delegations regretted the exclusion of language on the "blurred lines" between State, non-State and criminal actors,[118] other delegations resisted formulations that could imply attribution or State responsibility.[119]

The Final Report preserved only a cautious version of these discussions. It noted that ICT criminal activity could increase in scale and severity such that it seriously disrupts governments and international organizations and could potentially affect international peace and security. It also noted that malicious use of ICTs by State and non-State actors is increasing

118 For example, European Union (session 11, meeting 1); Switzerland (session 11, meeting 7).

119 For example, Russian Federation (session 11, meeting 1); Cuba (session 11, meeting 1); China (session 11, meeting 2).

and that some non-State actors have capabilities previously available only to States. However, it did not fully capture the operational ambiguity discussed in the room: how to address cybercriminal ecosystems, proxy relationships and commercially enabled capabilities when their effects may reach the level of national or international security threats. This suggests that the crime–security nexus, and the associated blurring of threat actors, may require additional exploration in the Global Mechanism, while leveraging possible synergies and avoiding duplication with the deliberations under the United Nations Convention against Cybercrime.[120]

4.3. The political sensitivity of attribution in the context of threat perception.

Attribution was a recurring undercurrent of the EPT discussions, but it remained largely outside the consensus outputs. Alongside statements attributing ICT incidents to various groups – including other States – delegations also raised increasing State-linked activity, false-flag risks or the need for evidence-based attribution.[121] In addition, warnings against politicized accusations or "false narratives" were raised by others during the discussions.[122] This revealed a persistent tension: attribution is often central to how States understand threats, but it is too politically sensitive to institutionalize in negotiated language.

As a result, the APRs and the Final Report avoided any attribution-specific language, focusing instead on categories of activity, effects and cooperative measures. This produced a more consensual text, at the cost of much of the deliberative texture around how States assess responsibility, risk escalation and appropriate responses.

This disconnect matters for the Global Mechanism because attribution disputes are unlikely to disappear. They may simply re-emerge in more indirect forms, for example in discussions on incident response, confidence-building, points of contact or critical infrastructure protection.

4.4. The growing importance of "effects" as a bridge across political disagreement

An important insight from the deliberations was that States increasingly used effects-based reasoning to bridge disagreement. Rather than resolving disputes over who was responsible, whether conduct was criminal or State-sponsored, or which legal framework applied, delegations often focused on the consequences of malicious ICT activity: disruption of essential

120 United Nations Office on Drugs and Crime, "UNCC: United Nations Convention against Cybercrime", https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

121 For example, Iran (Islamic Republic of) (session 1, meeting 2); Ukraine (session 2, meeting 1); United States (session 4, meeting 1); Russian Federation (session 6, meeting 1); Democratic Republic of the Congo (session 10, meeting 3).

122 For example, Nicaragua (session 1, meeting 4); China (session 2, meeting 5); Iran (Islamic Republic of) (session 9, meeting 1); Russian Federation (session 10, meeting 1).

services, harm to civilians, loss of trust in institutions, cascading failures or cross-border impacts.[123]

Whether this was the result of a deliberate negotiating choice or the natural evolution of the discussion, this approach helped make progress possible. It allowed discussions on ransomware, critical infrastructure and ICT-enabled disruption to advance even when attribution and legal characterization remained sensitive. The Final Report reflected effects-based language throughout the EPT section, including references to cascading national, regional and global effects, disruption of essential services, and potential impacts on international peace and security.

Beyond descriptiveness, this effects-based framing functioned as a way to sustain convergence under conditions of political disagreement. This might be a useful consideration as the Global Mechanism, given its permanent nature, will inevitably face periods of varying geopolitical tension.

4.5. Commercial intrusion capabilities as a governance problem, not only a threat category

Although commercially available ICT intrusion capabilities featured in the Final Report, the deliberations suggest that this issue was a broader and more difficult one than is conveyed in the final text. Delegations did not only identify these tools as a threat; they also raised questions about markets, proliferation, oversight, safeguards, access, lawful use and the role of private actors.

The breadth of this governance dimension was particularly visible in the later sessions of the OEWG, also influenced by the emergence of external processes on commercial intrusion capabilities (e.g. the Pall Mall Process),[124] which allowed for more focused discussion that then fed back into the OEWG. Where some delegations supported stronger language on commercial intrusion capabilities,[125] others resisted references that could imply new regulatory obligations or could constrain lawful access by developing countries.[126]

The Final Report reflected the theme but carefully balanced concern with safeguards. It noted both the risk of illegitimate and malicious use and the need not to limit the ability of States, particularly developing countries, to access and use ICT tools for purposes consistent with

---

123 For example, the Belgian victim assistance proposal: "Working Paper on a Victim-Based Approach", Submitted by Belgium, 6 March 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20240304_Belgium_-_Working_Paper_on_a_victim-based_approach.pdf.

124 French Ministry of Foreign Affairs, "Pall Mall Process: Code of Practice for States to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities", 23 July 2025, https://www.diplomatie.gouv.fr/en/presse-et-ressources/decouvrir-et-informer/actualites/processus-de-pall-mall-code-de-bonnes-pratiques-a-destination-des-etats-pour-lutter-contre-la.

125 For example, United Kingdom (session 9, meeting 3; session 10, meeting 1); Ghana (session 11, meeting 1); France (session 11, meeting 1); Australia (session 11, meeting 1).

126 For example, Brazil (session 7, meeting 3); Iran (Islamic Republic of) (session 11, meeting 1; meeting 3); Russian Federation (session 11, meeting 1).

international law. What is less visible in the final text is the underlying debate over whether this is merely a threat to be monitored or an emerging governance challenge requiring sustained attention.

4.6. The uneven treatment of societal harms, including gender and vulnerable groups

The deliberations also show that societal harms were unevenly integrated into the EPT theme. Harm to civilians, public trust, democratic institutions and vulnerable populations appeared at different points, but not all of these dimensions consolidated equally.

Gender was the clearest example. While gender-related concerns appeared in the OEWG record, they were largely framed through participation, digital divides, inclusion and capacity-building rather than as a distinct threat dimension. During the later sessions of the process, references to gender in the threat section were explicitly contested by some delegations.[127] The Final Report retained gender language, but in cross-cutting terms: participation, the gender digital divide and risks faced by persons in vulnerable situations, rather than gender-based ICT threats as such.[128]

The insight beyond the official outcomes is that some social and societal dimensions were acceptable when framed as inclusion or capacity issues, but not when framed as threat categories. This distinction is important for the Global Mechanism because it suggests that certain societal and social elements of harm may be better integrated in cross-thematic discussions, rather than treated as stand-alone issues.

4.7. The development–security link in threat perception

A further insight, particularly visible in statements by developing countries, is that threats were often understood not only as security risks but also as risks to development pathways, institutional trust and digital transformation. The African Group, for example, repeatedly linked malicious ICT activity to the ability of African States to pursue digitalization, protect public institutions and maintain societal trust.[129]

The Final Report did reflect such capacity gaps and digital divides, but the deliberations show a more specific point: for many States, the threat landscape is experienced through the lens of digital transformation and economic growth amid resource constraints, competing priorities and uneven resilience. This goes beyond generic capacity-building language. It shows why the EPT theme became closely linked to calls for practical support, CERT/CSIRT cooperation, public–private partnerships, and the Global Mechanism's capacity-building function.

---

127 For example, Russian Federation (session 11, meeting 1); Argentina (session 11, meeting 1); United States (session 11, meeting 7; session 11, meeting 8).

128 A/80/257, Section B, paragraph 29.

129 See Nigeria on behalf of the African Group (session 10, meeting 1; session 11, meeting 1; session 11, meeting 6).

In conclusion, taken together, these insights show that the OEWG's contribution on existing and potential threats cannot be assessed only by reading the agreed reports. The APRs and the Final Report provided the formal record of consensus, but the deliberations reveal a wider process of learning, testing, narrowing and reframing ideas. The discussions, even those that did not yield consensus language, supported delegations in building a more precise understanding of how threats are evolving, how they affect different States and what kinds of cooperative responses may be needed.

Several of the issues discussed above were only partially reflected in negotiated outcomes. Others were translated into more general language or moved into adjacent pillars such as capacity-building, confidence-building measures or regular institutional dialogue.

For the Global Mechanism on ICT security, the issues that featured in the Final Report provide a solid baseline for future work. But the issues that remained outside – or were only partially reflected – may be equally important for understanding where future discussions will need to go. The legacy of the OEWG 2021–2025 in the EPT space therefore lies both in the threat categories it institutionalized and in the unresolved questions it revealed for continued dialogue.

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

STATE	COUNT	STATE	COUNT
Russian Federation	44	Colombia	15
Iran (Islamic Republic of)	26	Syrian Arab Republic	14
European Union	23	New Zealand	13
China (the People's Republic of)	22	Fiji	13
Cuba	21	Viet Nam	13
Canada	21	Costa Rica	13
Netherlands (Kingdom of the)	20	Kazakhstan	12
United Kingdom of Great Britain and Northern Ireland	20	Ghana	12
Republic of Korea	20	Portugal	11
Germany	20	Uruguay	11
France	19	Ukraine	11
Australia	19	Ireland	11
Argentina	19	Chile	11
Singapore	18	Mauritius	10
South Africa	18	Nigeria	10
United States of America	17	Italy	10
Malaysia	17	Estonia	10
Israel	17	India	10
Japan	17	Bangladesh	10
Mexico	16	Nicaragua	9
Brazil	16	Kenya	9
Indonesia	16	Croatia	7
Egypt	16	Albania	7
Pakistan	15	Republic of Moldova	7
El Salvador	15	Slovakia	7
Switzerland	15	Thailand	7
Czechia	15	Venezuela, Bolivarian Republic of	7

STATE	COUNT	STATE	COUNT
Jordan	7	Mozambique	2
Ecuador	7	Cameroon	2
Belgium	7	Togo	2
Poland	6	Djibouti	2
Democratic People's Republic of Korea	6	Botswana	2
Vanuatu	6	Timor-Leste	2
Austria	6	Romania	2
Denmark	5	Peru	2
Philippines	5	Democratic Republic of the Congo	2
Dominican Republic	5	Uganda	2
Malawi	4	Sudan	2
Qatar	4	Georgia	2
Côte d'Ivoire	4	Yemen	2
Finland	4	Kuwait	1
Spain	4	Rwanda	1
Sri Lanka	4	Papua New Guinea	1
Latvia	4	Sierra Leone	1
Greece	4	Cambodia	1
Bosnia and Herzegovina	3	Ethiopia	1
Morocco	3	Senegal	1
Zimbabwe	3	Slovenia	1
Algeria	3	Brunei Darussalam	1
Türkiye	3	Kyrgyztan	1
Lao People's Democratic Republic	3	Tonga	1
Armenia	3	Montenegro	1
Iraq	3	State of Palestine	1
Belarus	3	Burkina Faso	1
Guatemala	3	Antigua and Barbuda	1
Paraguay	3	Kiribati	1
Sweden	2	Chad	1
Tunisia	2		

Rules, norms and principles of responsible State behaviour

Dr Andraz Kastelic

1. Introduction

This chapter provides an overview of the discussions on rules, norms and principles during this second OEWG, which convened between 2021 and 2025. As well as the areas of agreement, the overview also focuses on disagreements and on elements of the discussions that did not garner consensus support and were therefore not included in the written outcome records of the OEWG – the three annual progress reports (APRs)[1] and the final consensus report.[2]

1.1. The road to the OWEG 2021–2025

Following the recognition of the UN General Assembly in 1999 that information telecommunication technologies (ICTs) "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security",[3] States engaged in a multilateral dialogue on "existing and potential threats in the sphere of information security and possible cooperative measures to address them."[4]

Much like the technology itself, [5] the deliberations on ICT challenges to international security have evolved since then. Throughout the multilateral discussions in six Groups of Governmental Experts (GGEs) and two Open-Ended Working Groups (OEWGs), States have elaborated a number of cooperative measures to address these challenges; the norms, rules and principles of responsible State behaviour in the use of ICTs are chief among these measures.

The beginnings of the substantive multilateral discussions on normative frameworks setting international expectations of State behaviour in the use of ICTs can be traced back to the second GGE on Developments in the Field of Information and Telecommunications in the Context of International Security. This GGE noted in its consensus report of 2010 that there is a "lack of shared understanding regarding international norms pertaining to State use of

1 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; A/78/265, 2023; A/79/214, 2024.

2 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.

3 General Assembly, resolution 53/70, 1998, 2.

4 General Assembly, resolution 56/19, 2001. See also e.g. General Assembly, resolutions 59/61, 2004; 62/17, 2007; 65/41, 2010; 68/243, 2013; 73/27, 2018; 78/237, 2023.

5 Giacomo Persi Paoli and Samuele Dominioni, "Exploring the AI–ICT Security Nexus", UNIDIR, 2024, https://unidir.org/publication/exploring-the-ai-ict-security-nexus/, 1.

ICTs"[6] and recommended that States "engage in further dialogue on norms pertaining to State use of ICTs".[7]

Indeed, the following GGE recognized norms as one of the primary international cooperative measures to address the existing and potential ICT challenges to international security. Under its agenda point on "Norms, rules and principles of responsible behaviour by States", that GGE discussed norms that derived from existing international law. That GGE went on to conclude that international law "is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[8]

The most influential multilateral negotiations on rules, norms and principles of State use of ICTs occurred in the fourth GGE, between July 2014 and June 2015. The outcomes are encapsulated in the substantive final report of the fourth GGE, which was subsequently welcomed by General Assembly resolution 70/237 without a vote.[9] The resolution also called on Member States to be guided in their use of ICTs by the GGE's report and, therefore, the norms elaborate in that report. One of the most notable achievements of the fourth GGE was the establishment of 11 voluntary, non-binding norms of responsible State behaviour in their use of ICTs. These 11 norms can increase predictability[10] and "help to prevent conflict in the ICT environment and contribute to its peaceful use".[11] International law in the context of the use of ICTs was no longer discussed under the "Norms, rules and principles" agenda point, but now occurred under a separate, dedicated agenda point.[12] However, as indicated below, the confluence of voluntary expectations and mandatory rules persists in the context of multilateral discussions on the behaviour of States in their use of ICTs to this day.

In the period between 2018 and 2021, the multilateral discussions on rules, norms and principles occurred in two parallel United Nations processes – the sixth GGE and the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security. Both groups acknowledged the commitment of the international community to the 2015 norms and acknowledged that additional norms could be developed in the future.[13] At the same time, the OEWG and GGE processes of 2018–2021 also took steps towards supporting the operationalization of the existing norms. The OEWG 2018–2021 recommended that States survey their national implementation efforts, share good practices with the international community and support the implementation and development of norms.[14]

---

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/65/201**, 2010, Section III, paragraph 14.

7 **A/65/201**, 2010, Section IV, paragraph 18(i).

8 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, Section III, paragraph 19.

9 General Assembly, Official Record, **A/70/PV.82**, 2015, 11.

10 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 24.

11 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, Section III, paragraph 10.

12 **A/70/174**.

13 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, Section III, paragraph 16

14 **A/75/816**, paragraphs 30–33.

Meanwhile, the sixth GGE equipped the list of 11 norms with additional layer of understanding.[15] It also supported operationalization of the norms by providing guidance on their implementation.[16]

In late 2020, the General Assembly decided to convene the OEWG on security of and in the use of information and communications technologies 2021–2025. Among other things, the Assembly mandated this new OEWG to, "as a priority, further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour".[17]

In an effort to provide an overview of the discussions on rules, norms and principles during this second OEWG, section 2 of the chapter first outlines the chronological development of the normative discussions in the OEWG 2021–2025. Section 3 then focuses on substantive aspects of the discussions by providing an account of national inputs on a number of prominent themes related to the norms, rules and principles guiding State behaviour in cyberspace. The final section of this chapter, Section 4, focuses on the additional two aspects of discussions not reflected in the final report of the OEWG 2021–2025: the external factors influencing the exchanges between States; and a list of proposals for new norms that were introduced throughout sessions of the second OEWG but did not garner sufficient support among the States to be included in the final consensus report (also listed in Annex A).

The chapter intends to inform further relevant multilateral discussions on ICTs in the context of international security. As reflected in the relevant General Assembly resolutions[18] and in the outcome reports of the GGEs and OEWGs,[19] discussion on rules, norms and principles of responsible State use of ICTs is set to continue in the context of the permanent mechanism – the 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.[20] Much like in the past few GGEs and OEWGs, the discussions in the Global Mechanism will focus on the 11 agreed non-binding norms, the ways to implement them and potential additional norms.[21]

---

15 A/76/135, paragraphs 18–71.

16 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 36(b).

17 General Assembly, resolution 75/240, 2021, 3.

18 General Assembly, resolutions 78/237, 2023; 79/237, 2024; 78/16, 2023; 80/16, 2025.

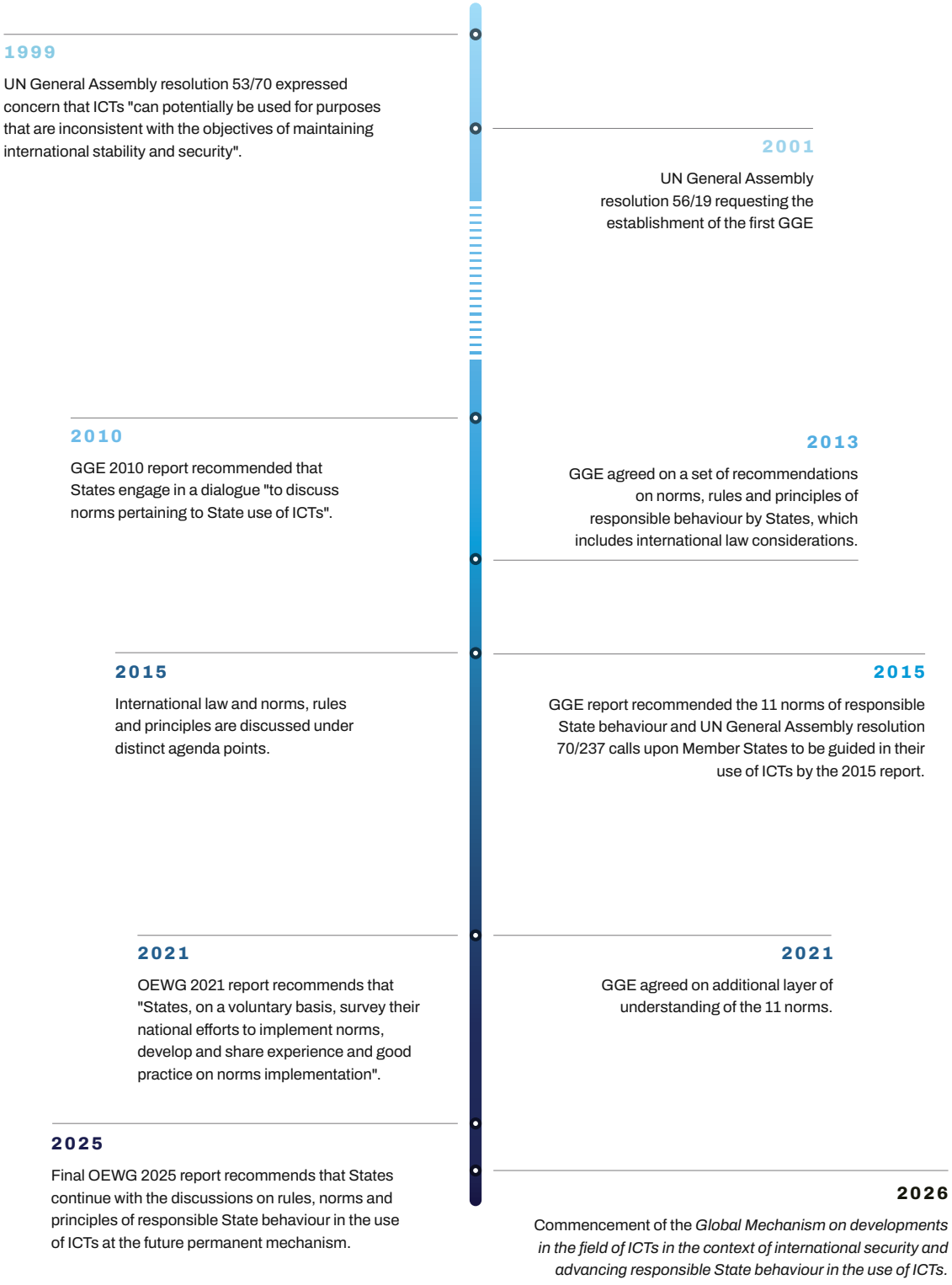
19 A/79/214; A/80/257.

20 A/80/257, Annex I.

21 A/79/214, Annex C, paragraph 9.

FIGURE 1.

Evolution of the multilateral discussions on rules, norms and principles of State behaviour in their use of ICTs



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

The substantive discussions of the OEWG 2021–2025 commenced with the reaffirmation of the 11 voluntary norms of responsible State use of ICTs. They eventually transitioned to the questions of their operationalization, which included discussion of proposed tools supporting their implementation. Throughout the mandate of the second OEWG, the contributions of the participating States revealed persistent divergence on whether the efforts of the international community should focus on the implementation of the existing norms or on development of new norms (or even rules). Over time, this became one of the most significant areas of divergence between States on this agenda item, and one that dominated the later substantive sessions of the OEWG.

The following subsections, divided into four cycles,[22] provide a chronological overview of the discussions in the OEWG 2021–2025.

2.1. Broad commitment to the normative framework

The substantive discussions of the OEWG commenced with a broad reaffirmation of the 11 voluntary, non-binding norms inherited from the consensus outcomes of the previous dedicated multilateral discussions, including the 2014–2015 Group of Governmental Experts.

During the OEWG's inaugural sessions, most of the States reiterated their support for these norms and emphasized their central role within the wider framework of responsible State behaviour.[23] While no State is on the record as explicitly opposing the norms, related concerns over legitimacy[24] or effectiveness[25] were raised by some delegations, while they invited Member States to engage in a discussion on new normative or legally binding instruments.

Early in the OEWG discussions, States also explored ways to enhance the implementation of the voluntary norms. Accordingly, several States emphasized different regional and cross-regional (efforts to develop) instruments supporting the implementation of the norms.[26] A few States also suggested negotiation on common definitions of relevant cybersecurity terminology[27] or sharing of national definitions[28] to support the implementation of norms as well as to increase confidence among States.[29]

---

22 A cycle includes substantive sessions and the negotiation session when a report was negotiated. For more information on this, see Introduction in this volume.

23 For example, Brazil (session 2, meeting 5); Singapore (session 1, meeting 6); United States (session 2, meeting 5); Nigeria (session 1, meeting 5); India (session 1, meeting 6).

24 For example, Cuba (session 1, meeting 6); Iran (Islamic Republic of) (session 2, meeting 5).

25 For example, Russian Federation (session 1, meeting 5); Cuba (session 1, meeting 6); Nicaragua (session 4, meeting 4).

26 Such as the National Survey of Implementation and the ASEAN Checklist of Implementation. See further discussion on these tools in Subsection 3.4 below.

27 For example, Iran (Islamic Republic of) (session 1, meeting 6); Cuba (session 1, meeting 5).

28 For example, El Salvador (session 4, meeting 4).

29 For further discussion on unified terminology in the context of confidence-building measures, see the Confidence-building measure chapter in this volume.

By the end of the first cycle of the OEWG mandate, States had agreed to continue discussing rules, norms and principles. The first APR also acknowledged that further development of norms and implementation of the existing ones are "not mutually exclusive but could take place in parallel".[30] Indeed, the APR encouraged future discussions on implementation of the norms by inviting interested States to submit working papers to contribute to the development of "guidance, checklists and to share national views on technical ICT terms".[31] The APR also encouraged States to survey and report on their implementation efforts.[32]

2.2. The continuing binary debate

The divergences between States that prioritized the implementation of existing norms and those that advocated for the development of new norms or of legally binding instruments persisted, if not intensified, in the following period. This rather polarizing debate often took the form of what the Chair of the OEWG labelled as a "binary framing".[33]

Most of the States contributing to the OEWG discussion on rules, norms and principles during 2023 continued to argue that the existing norms form a sufficient framework to reduce risks to international peace, security and stability. They suggested that international efforts should rather focus on their implementation.[34]

On the other side, a few States continued to promote the view that the voluntary norms are not fit for the challenge of growing ICT threats and incidents in the context of international security.[35] They tabled proposals to overcome this.[36]

In the 2023 APR, States agreed to continue discussing norms and their implementation, with a particular focus on protection of critical infrastructure and critical information infrastructure and on security of supply chains. This APR indicated a continuous appetite among Member States for additional tools and mechanisms to assist with the implementation of norms and provided the Chair of the OEWG with the mandate to draft a checklist on the implementation of the existing norms.[37]

---

30 A/77/275, paragraph 14(b).

31 Chairperson OEWG 2021–2025, Rev.2 of annual progress report, annexed to Letter from the Chair, 27 July 2022, https://documents.unoda.org/wp-content/uploads/2022/07/Letter-from-OEWG-Chair-27-July-2022.pdf.pdf.

32 A/77/275, paragraph 14(1, 2).

33 See Ambassador Gafoor (session 7, meeting 4).

34 For example, United Kingdom (session 4, meeting 4); Japan (session 4, meeting 4); Canada (session 4, meeting 3); Israel (session 4, meeting 4); United States (session 4, meeting 4); Australia (session 6, meeting 3); Republic of Korea (session 6, meeting 3); European Union (on behalf of 37 States) (session 6, meeting 3); Switzerland (session 6, meeting 3).

35 For example, Pakistan (session 3, meeting 2); Iran (Islamic Republic of) (session 4, meeting 3); Nicaragua (session 4, meeting 4); Syria (session 7, meeting 4).

36 For example, Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security" (Cosponsors: Belarus, Cuba, the Democratic People's Republic of Korea, Nicaragua, Syria, Venezuela), 3 December 2024 (Unofficial translation), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on__ensuring_international_information_security.pdf.

37 A/78/265, paragraph 26.

2.3. Implementation, additional layer of understanding and new norms

While the divergent positions among the contributing States on the questions of the sufficiency of the existing voluntary norms persisted, if not deepened, the discussion on norms, rules and principles simultaneously took further steps towards implementation.

Notably, during the third cycle of the OEWG, States discussed a Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs.[38] This had been prepared by the OEWG Chair following the mandate given in the second APR.[39]

Several States continued to emphasize the utility of the Survey of Implementation (undertaken in 2023)[40] and its complementarity[41] with the Voluntary Checklist of Practical Actions. A few States also continued reflecting on progress made by the Association of Southeast Asian States (ASEAN) in development of a checklist[42] and noted its utility.[43] Moreover, some States shared their implementation efforts through examples of the integration of norms in their domestic frameworks.[44]

A number of States dedicated (parts of) their interventions to the additional layer of understanding – featured in the 2021 consensus report of the GGE,[45] subsequently welcomed by General Assembly resolution 76/19 and now known as "guidance on implementation"[46] – which provides further guidance on the normative expectations and actions relevant for their implementation.

Prior to the commencement of the seventh substantive session in 2024, the Chair invited Member States and non-State actors to consider specific new voluntary norms.[47] Indeed, some States and non-State actors responded with proposals for potential new voluntary norms addressing different contemporary technological challenges, such as artificial intelligence (AI).[48]

---

38 A/79/214, Annex A.

39 A/78/265, paragraph 26.

40 For example, Ghana (session 4, meeting 4); Kenya (session 4, meeting 4); Germany (session 4, meeting 3); Mexico (session 7, meeting 4).

41 For example, Canada (session 6, meeting 3).

42 For example, Singapore (session 2, meeting 5); Malaysia (session 8, meeting 2).

43 For example, Slovakia (session 6, meeting 3); Poland (session 6, meeting 4).

44 For example, Costa Rica (session 6, meeting 3); Kenya (session 6, meeting 4); Brazil (session 7, meeting 4); Sri Lanka (session 6, meeting 4). See also Russian Federation, "Review of Compliance of National Legislation of the Russian Federation with the UN Voluntary Rules, Norms and Principles of Responsible Behavior of States in the Field of International Information security", https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Review_of_compliance_of__Russia's_national_legislation__with_the_rules_norms_and_principles__of_behavior.pdf.

45 A/76/135.

46 A/80/257, Section C, paragraph 36(b).

47 Chairperson OEWG 2021–2025, Letter, 20 February 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_20_February_2024.pdf.

48 For example, Algeria (session 4, meeting 4).

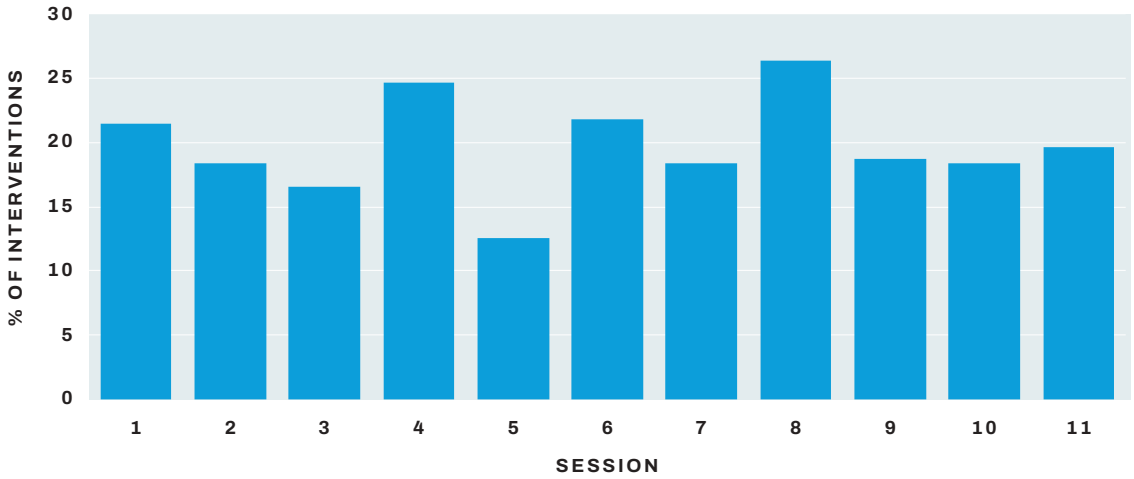
The third APR acknowledged that, while States had discussed new norms, they had not reached consensus on any of them; the report noted that "several proposals were put forward for possible new norms which are still being discussed by States".[49] In addition to the commitment to continue discussing existing rules, norms and principles and possible additional norms of responsible use of ICTs, in the third APR States made a commitment to continue efforts to implement the norms and to further develop the Voluntary Checklist of Practical Actions.[50]

2.4. Evaluation of the role of norms, rules, principles and relevant tools in the future Global Mechanism

Some States continued to propose specific new norms for the consideration of the OEWG,[51] and the divergence persisted between States on the necessity of a legally binding mechanism to regulate use of ICTs in the context of international security .[52] The final set of OEWG sessions, however, largely focused on evaluation of the Voluntary Checklist of Practical Actions and discussion on the structure of the Global Mechanism on ICT Security. Ultimately, the final consensus report took note of the Voluntary Checklist of Practical Actions, and States agreed that the Global Mechanism would feature rules, norms and principles as a cross-cutting topic; the relevant discussions on norm implementation and potential further development of additional norms are to occur in the plenary sessions and will be raised in the dedicated thematic groups of the Global Mechanism.[53]

FIGURE 2.

Proportion of state interventions on rules, norms and principles topics by session[54]



49 A/79/214, paragraph 31(k).

50 A/79/214, paras 32–34.

51 See, for example, China (session 9, meeting 4); Bangladesh (session 9, meeting 3); El Salvador (session 9, meeting 3).

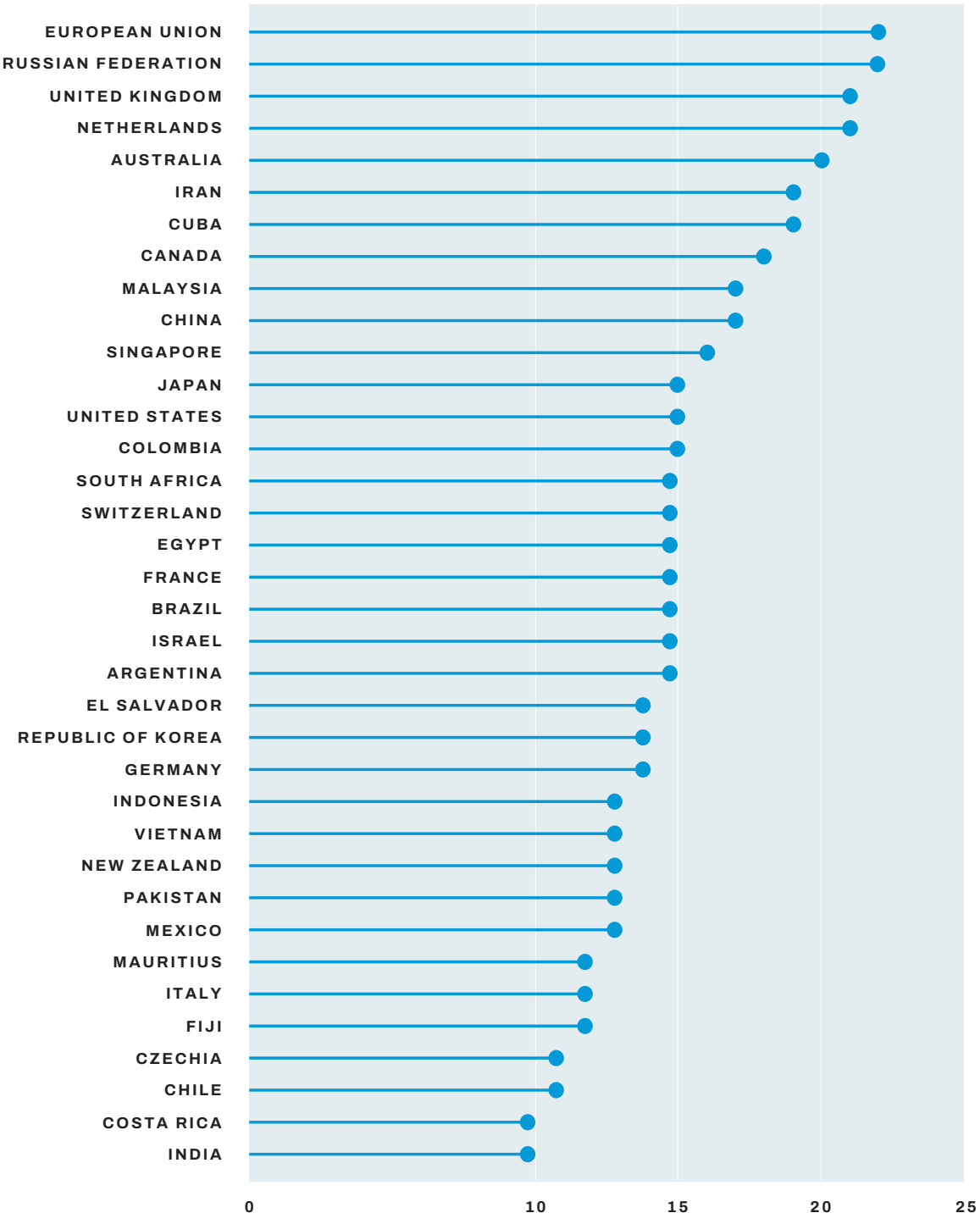
52 Contrast, for example, Pakistan (session 10, meeting 3) and Cuba (session 10, meeting 3) against the United States (session 9, meeting 4) and Israel (session 10, meeting 3).

53 A/80/257, Annex I, paragraph 7.

54 Proportions reflect state interventions matched against at least two key terms from a thematic dictionary search of topics relating to rules, norms and principles.

FIGURE 3.

Number of times delegations took the floor on rules, norms and principles in the OEWG 2021-2025[55]



55 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 B.

3. Trends and major themes addressed during the mandate

Delegations made over 800 interventions on rules, norms and principles in the 11 sessions of the OEWG 2021–2025 (see Figures 1 and 2). This section categorizes and analyses the prominent substantive issues that these interventions addressed. Themes are addressed in the order of their prominence during the discussions, measured by the number of interventions and proposals on the specific topic.

3.1. New rules or norms versus implementation of the existing ones

As indicated in Section 2, the overarching and persistent trend in the OEWG 2021–2025 discussions was the polarization between States advocating for the international community to focus on implementation of existing voluntary norms and those arguing for further development of the normative framework. This was not a new divergence; it had already permeated the discussions of the OEWG 2018–2021.[56]

This discussion also exhibited a blurring between, on the one hand, voluntary norms that outline expectations of responsible behaviour of States and, on the other, rules that prescribe obligations and prohibitions on State behaviour in the use of ICTs. This blurring also featured in the discussions under the agenda point on international law. The blurring originated in the transition from the third GGE (2012–2013) to the fourth (2014–2015) – the former discussed norms and international law under the same agenda point, on "Norms, rules and principles", while the latter discussed international law under a separate, dedicated agenda point. Yet, when this change was made, the scope of the previous agenda point remained unchanged: "rules" remained in the "Norms, rules and principles" agenda item.

To avoid further blurring of expectations and obligations of States, relevant multilateral discussions at the Global Mechanism could separate discussions on voluntary *norms* and *principles* on the one hand and mandatory rules of State behaviour in their use of ICTs on the other hand. Accordingly, States could consider discussing the latter under the agenda on international law.

Although a significant part of the OEWG 2021–2025 discussions focused on the implementation of the existing voluntary norms, some States questioned the legitimacy of voluntary norms or their ability to ensure peace and security in the ICT environment. Specifically, a few States suggested that the norm-elaboration process of the 2015 GGE[57] had not been sufficiently inclusive to be considered reflective of a universal agreement.[58] This is despite the

56 "Chair's Summary", A/AC.290/2021/CRP.3, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

57 General Assembly, resolution 70/237, 2015.

58 For example, Cuba (session 1, meeting 6); Iran (Islamic Republic of) (session 2, meeting 5).

fact that the General Assembly welcomed the outcomes of the 2015 GGE and the subsequent General Assembly resolutions called on States to be guided in their behaviour by the norms.[59] At the same time, a few States suggested that the voluntary nature of norms renders them ineffective in the maintenance of peace, security and stability in the ICT environment.[60] According to one of the proponents of this argument, the voluntary nature of the norms only benefits States with more developed ICT capabilities .[61] Some States also questioned the effectiveness of the existing voluntary norms in the context of rapidly developing technology, including ICTs.[62]

Several proposals to overcome the alleged deficiency of the voluntary norms were made during the OEWG 2021–2025. Specifically, to enhance legitimacy of the normative framework and ensure its implementation, a few States argued that the OEWG should seek to add to the existing list of 11 norms. This would provide States that had not previously participated in the norm-elaboration process of the 2015 GGE an opportunity to ensure that the normative framework is reflective of circumstances of all States.[63]

Furthermore, a few States concerned with the voluntary nature of the norms also expressed support for the negotiation and adoption of a universal legal instrument regulating State use of ICTs.[64] A specific revised proposal for this was tabled during the 2023 and 2024 discussions as a draft legally binding multilateral United Nations Convention on International Information Security.[65] An argument for a dedicated legal regime for the ICT domain was also advanced by a few States in the context of the discussion on international law.[66]

A few States also proposed modernization of the normative framework by adding specific norms with a view to ensuring the effectiveness of the framework in the context of the evolution of the ICTs,[67] including AI.[68] (See Annex A for a list of national proposals for new voluntary norms.)

Several States strongly opposed the negotiation of a new legally binding treaty for cyberspace, arguing that the true problem is a lack of compliance with existing norms, rules and principles.[69]

---

59 For example, General Assembly, resolution **76/19**, 2021.

60 For example, Russian Federation (session 1, meeting 5); Cuba (session 1, meeting 6); Nicaragua (session 4, meeting 4).

61 Russian Federation (session 1, meeting 5).

62 Russian Federation (session 1, meeting 5); Cuba (session 1, meeting 6); Nicaragua (session 2, meeting 5).

63 Iran (Islamic Republic of) (session 9, meeting 3); Cuba (session 4, meeting 3).

64 For example, Russian Federation (session 4, meeting 3); Pakistan (session 5, meeting 3); Iran (Islamic Republic of) (session 4, meeting 3); Democratic People's Republic of Korea (session 8, meeting 3).

65 Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security".

66 On such a legal regime, see the International Law chapter in this volume.

67 For example, Vietnam (session 10, meeting 3); China (session 1, meeting 6).

68 For example, South Africa (session 9, meeting 3); Bangladesh (session 9, meeting 3).

69 For example, Canada (session 2, meeting 5); Germany (session 4, meeting 3); Estonia (session 4, meeting 3); Poland (session 6, meeting 4); United States (session 4, meeting 4).

They argued further that efforts should instead focus on implementing current norms with a human rights-based approach.[70]

Some delegations cautioned against this so-called binary division between the implementation of existing voluntary norms and the elaboration of new norms or rules. They argued that the two are not mutually exclusive processes,[71] which indeed aligned with the duality of the OEWG 2021–2025 mandate.[72] The divergence was theoretically put to rest in the 2022 APR, in which "States proposed that additional norms could continue to be developed over time, noting that the further development of norms and the implementation of existing norms were not mutually exclusive but could take place in parallel." [73] This sentiment was also been included in the final consensus report, where "States recalled the mandate of the OEWG contained in General Assembly resolution 75/240, inter alia, 'to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour'."[74]

However, national statements on the adoption of the final OEWG report testify to the fact that States largely remained entrenched on the question of which direction should be pursued by the international community. This extends to the context of the Global Mechanism, where some States expect a discussion on a new legal regime dedicated to international ICT security and other States expect a discussion on the implementation of the existing normative framework.[75]

---

70 For example, Canada (session 2, meeting 5); Netherlands (session 2, meeting 5); United Kingdom (session 4, meeting 4).

71 For example, South Africa (session 1, meeting 5); Egypt (session 4, meeting 3); Brazil (session 6, meeting 4); Singapore (session 9, meeting 3); China (session 9, meeting 4).

72 Resolution **75/240**, 3.

73 **A/77/275**, paragraph 14(b).

74 **A/80/257**, paragraph 36(c).

75 For example, Russian Federation, "Statement by the Russian Interagency Delegation at the Eleventh Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025", **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_-_Adoption_of_the_final_report_-_ENG.pdf**; Joint Statement of the Group of Like-Minded States (Belarus, Venezuela, Iran, China, Cuba, Nicaragua, Russia, Sudan, Niger, Zimbabwe, Eritrea) on the Final Report of the Open-Ended Working Group on security of and in the use of ICTs 2021–2025, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/LMG_statement_on_the_final_OEWG_report.pdf**. Compare, for example, Malta, "Malta's Position for the Compendium of Statements", 11 July 2025, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Malta.pdf**; Israel, "Israel's Explanation of Vote (EOV) and Remarks on the Final Progress Report of the 2021–2025 OEWG", **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Israel.pdf**.

A representative of the European Union speaks during the eleventh substantive session of the the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 2025. Credit: UN Photo / Loey Felipe.

3.2. (Inter)national critical infrastructure protection

A notable concern of the States throughout the discussions on normative protections of critical infrastructure – which is covered by voluntary norms F[76] and G[77] – are the trans-boundary effects of ICT operations.[78] Most of the delegations taking the floor to address the subject of norms in the context of critical infrastructure acknowledged that malicious ICT activities against such infrastructure pose a significant threat to international peace and security as well as economic stability and public safety.

According to the discussions during the OEWG 2021–2025, a large number of States consider ransomware[79] and ICT operations in the context of an armed conflict[80] as the most significant contemporary threats to critical infrastructure. A few States shared specific examples of such ICT operations.[81] To respond to this threat landscape, some States called

76 "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." A/76/135.

77 States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199. A/76/135.

78 For example, Portugal (session 4, meeting 3); Switzerland (session 4, meeting 4); Netherlands (session 4, meeting 3).

79 For example, Israel (session 1, meeting 5); Netherlands (session 4, meeting 3); Singapore (session 7, meeting 2); Canada (session 10, meeting 2); Papua New Guinea (session 11, meeting 3).

80 For example, European Union on behalf of 35 States (session 2, meeting 5).

81 For example, Ukraine (session 6, meeting 3); Poland (session 4, meeting 3).

for compliance with the relevant voluntary norms; others advocated for the expansion of the existing additional layer of understanding of norms F, G and H;[82] and other States shared their domestic efforts to implement the norms in national legislative frameworks.[83]

The discussion in the OEGW 2021–2025 also focused on the concept and scope of critical infrastructure. In their interventions, a few delegations emphasized the critical nature of specific sectors – such as the health sector;[84] technical infrastructure essential to the general availability or integrity of the Internet (the so-called public core of the Internet);[85] electoral infrastructure;[86] and civil aviation.[87] Some interventions suggested that developing States would benefit from international assistance when seeking to develop critical infrastructure designation methodology.[88]

3.3. Supply chain integrity and the commercialization of malicious ICT tools or practices

A major concern for States during the OEWG 2021–2025 discussions proved to be supply chain integrity and the commercialization of malicious ICT tools or practices. Although these could be considered two distinct issues, the multilateral discussions frequently addressed them in conjunction.[89] Specifically, to tackle these two issues, some States proposed various additions to the layer of understanding of norm I[90]with the aim of ensuring the "integrity of the ICT supply chain and the security of ICT products".[91]

First, noting specific recent incidents involving compromised supply chains, several delegations proposed various transparency measures that States could take in support of the implementation of the norm I. These included software bills of materials:[92] national certification schemes aligned with established international standards;[93] and cybersecurity labelling schemes for Internet of Things (IoT) devices.[94] In this context, one State also submitted a

---

82 For example, Australia (session 1, meeting 6); United States (session 6, meeting 3).

83 For example, China (session 2, meeting 5); Japan (session 4, meeting 4).

84 For example, Switzerland (session 1, meeting 5); Israel (session 8, meeting 2); Bangladesh (session 8, meeting 3); Ireland (session 11, meeting 2); Sierra Leone (session 11, meeting 3).

85 For example, India (session 1, meeting 6); Netherlands (session 2, meeting 5); Canada (session 8, meeting 2).

86 See e.g. Netherlands (session 1, meeting 5); Singapore (session 2, meeting 5); European Union (session 5, meeting 3); Iraq (session 8, meeting 6)

87 For example, Israel (session 1, meeting 5); Singapore (session 4, meeting 3); Bangladesh (session 8, meeting 3); Democratic Republic of the Congo (session 10, meeting 3).

88 For example, Fiji (session 10, meeting 3); Mauritius (session 6, meeting 4).

89 For example, Denmark (session 1, meeting 5); European Union (session 3, meeting 3); Australia (session 6, meeting 3).

90 "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions." A/76/135, Norm 13(i). See also, for example, Czechia (session 4, meeting 4); France (session 6, meeting 3); United Kingdom (session 9, meeting 3).

91 A/76/135, paragraph 56.

92 For example, Japan (session 7, meeting 4); Italy (session 10, meeting 3).

93 For example, Italy (session 10, meeting 3).

94 For example, Singapore (session 6, meeting 3).

working paper seeking multi-stakeholder support for the Global Initiative on Data Security, which includes a number of proposals intended to promote security of supply chain of ICT products and services, among other things.[95]

Additional proposals related to supply chain security focused on the rise of commercially available malicious ICT exploits and tools, beyond ransomware. Drawing inspiration from relevant initiatives such as the Pall Mall Process,[96] and in response to the "growing market for commercially-available ICT intrusion capabilities as well as hardware and software vulnerabilities",[97] some States proposed an additional layer of understanding to accompany norm I that encouraged national measures inhibiting the proliferation of commercially available malicious ICT tools.[98] A few States also expressed concern over the potential for these tools to be used contrary to the human rights protections stipulated in norm E.[99]

The final report of OEWG 2021–2025 not only outlines some of these discussions on supply chain security but also emphasizes the role of the private sector "in promoting openness and ensuring the integrity, stability and security of the supply chain, and in preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions".[100]

3.4. Operationalization of the framework via surveys and checklists

A prominent aspect of the OEWG 2021–2025 discussion was the operationalization of the existing voluntary norms. In addition to the wealth of exchanges on additional layer of understanding supporting the implementation of the norms and a few suggestions to harmonize relevant cybersecurity terminology,[101] States explored various tools supporting the norms' implementation.

The first such tool to emerge during the second OEWG was the "National Survey of Implementation of United Nations recommendations on responsible use of ICTs by States in the context of international security".[102] Initially endorsed by the OEWG 2018–2021, the National Survey was introduced to the second OEWG 2021–2025 as a voluntary, user friendly self-assessment tool that could be used by States to identify barriers to norm implementation,

---

95 "Global Initiative on Data Security", https://documents.unoda.org/wp-content/uploads/2022/03/Position-paper-Global-Initiative-on-Data-Security-submitted-by-China.pdf.

96 "The Pall Mall Process Declaration: Tackling Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities", 6 February 2024, https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

97 A/80/257, paragraph 25

98 For example, United Kingdom (session 6, meeting 3); Canada (session 9, meeting 3); France (session 9, meeting 4); Switzerland (session 7, meeting 4).

99 For example, United Kingdom (session 7, meeting 4). See also Subsection 3.6 below.

100 A/80/257, paragraph 34(h).

101 See Subsection 2.1 above.

102 See also Republic of Korea (session 1, meeting 5); South Africa (session 1, meeting 5); Mexico (session 1, meeting 6); Australia (session 2, meeting 5). The National Survey of Implementation is available at https://nationalcybersurvey.cyberpolicyportal.org/.

such as political prioritization[103] or capacity gaps.[104] The voluntary National Survey received wide, cross-regional support throughout the OEWG 2021–2025 discussions.[105] A few States further reported proven utility of the tool in supporting domestic policymaking efforts[106] or efforts promoting transparency among States.[107] However, a few States opposed tools supporting the implementation of the existing voluntary norms.[108] The National Survey of Implementation was not explicitly included in the final report.

In addition to the National Survey and the steady promotion by a few States of regional efforts and tools in support of the implementation of norms[109] (e.g., the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace),[110] the discussion centred on the Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs.

The preparation of the so-called Chair's Checklist (authored by the Chair, who submitted it to States for consideration) was requested in the second APR of 2023. In that report, States agreed "to elaborate additional guidance, including a checklist, on the implementation of norms, taking into account previous agreements" [111] and formally requested the OEWG Chair "to produce an initial draft of such a checklist for consideration by States".[112] The draft Chair's Checklist was ready by 2024 and was annexed to the third APR.[113]

While some States took the floor to support the Chair's Checklist,[114] not all States have been favourable towards it, with some delegations expressing reservations[115] or opposition.[116] Despite this, States "took note"[117] of the Chair's Checklist and, in the final report of OEWG 2021–2025, committed to "continue discussing and updating [the Chair's Checklist] at the future permanent mechanism . . . with a view to its finalization".[118]

---

103 Australia (session 2, meeting 5).

104 For example, Malaysia (session 1, meeting 6); France (session 1, meeting 6); Netherlands (session 1, meeting 5)

105 For example, United States (session 4, meeting 4); Argentina (session 2, meeting 5); Chile (session 2, meeting 5); South Africa (session 2, meeting 5); Kenya (session 4, meeting 4); Malaysia (session 1, meeting 6); Japan (session 2, meeting 5)

106 Republic of Korea (session 2, meeting 5); Ghana (session 4, meeting 4).

107 For example, Estonia (session 1, meeting 6); Switzerland (session 1, meeting 6); Canada (session 1, meeting 5)

108 For example, Russian Federation (session 9, meeting 3); Iran (Islamic Republic of) (session 9, meeting 3).

109 Singapore (session 7, meeting 4); Malaysia (session 10, meeting 3); Thailand (session 10, meeting 3).

110 Singapore (session 2, meeting 5); ASEAN, "ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace", **https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf**.

111 **A/78/265**, paragraph 26.

112 Ibid.

113 **A/79/214**.

114 For example, Singapore (session 9, meeting 3); Malaysia (session 9, meeting 4); Australia (session 9, meeting 4); Ireland (session 9, meeting 4).

115 For example, Egypt (session 7, meeting 4); United States (session 7, meeting 4); Russian Federation (session 9, meeting 3).

116 For example, Cuba (session 10, meeting 3); Iran (Islamic Republic of) (session 9, meeting 3).

117 **A/79/214**, paragraph 31(i).

118 **A/80/257**, paragraph 38

During the OEWG 2021–2025, stakeholders also developed and proposed tools supporting the implementation of norms.[119]

3.5. Due diligence

The significance and utility of norm C, which sets the expectation of due diligence[120] in cyberspace, has been widely recognized by the States contributing to the discussions.[121] Some States have recognized the utility of due diligence as a mechanism to address the rising prominence of malicious non-State actors[122] and the growing threat of ransomware.[123] However, long-standing divergences have persisted[124] on whether diligent behaviour of States in cyberspace is an expectation of a voluntary norm[125] or is a prescribe legal obligation of conduct,[126] violation of which can result in international responsibility of a State.

An important part of the negotiations on norm C focused on ways to operationalize it, including through the expansion of the additional layer of understanding adopted by the 2021 GGE or tools supporting its implementation. For instance, a few States suggested the development of communication templates and standard operating procedures[127] or a practical guide for the implementation of the norm.[128] Indeed, a number of States followed up and submitted a working paper to this effect.[129] At the same time, some States outlined how the Global Intergovernmental Points of Contact Directory (established on the recommendation of the OEWG 2021–2025)[130] can practically support the operationalization of the norm C;[131] this suggestion was reflected in the Chair's Checklist among the suggested measures for the implementation of norm C.[132]

---

119 See, for example, Geneva Dialogue, "Geneva Manual on Responsible Behaviour in Cyberspace", https://genevadialogue.ch/geneva-manual/; Global Partners Digital, "Inclusive Cyber Norms Toolkit", 19 July 2023, https://www.gp-digital.org/publication/inclusive-cyber-policymaking-toolkit/.

120 "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." A/76/135, Norm 13(c).

121 For example, Republic of Korea (session 1, meeting 5); Egypt (session 10, meeting 3); Costa Rica (session 1, meeting 5); Portugal (session 9, meeting 3).

122 For example, India (session 1, meeting 6); Portugal (session 9, meeting 3); Denmark (session 1, meeting 5).

123 For example, France (session 9, meeting 4); Switzerland (session 10, meeting 3).

124 Andraz Kastelic, *Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights* (Geneva: UNIDIR, 2021), https://unidir.org/publication/due-diligence-in-cyberspace-normative-expectations-of-reciprocal-protection-of-international-legal-rights/.

125 For example, Israel (session 6, meeting 4); Portugal (session 9, meeting 3).

126 For example, Netherlands (session 7, meeting 4); European Union (on behalf of 35 States) (session 2, meeting 5); Iran, "Submission to the First Substantive Session by Iran (Islamic Republic of) (Islamic Republic of)", 1 December 2021, 6, https://documents.unoda.org/wp-content/uploads/2021/12/Irans-submission-to-first-substantive-session_13-17-Dec-21.pdf.

127 For example, Kenya (session 2, meeting 5).

128 For example, France (session 4, meeting 3); United States (session 7, meeting 4).

129 "Multiple States' views on best practices relating to the implementation of norm 13(c)", 23 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_paper_-_Best_practices_relating_to_the_implementation_of_norm_13(c).pdf.

130 On the directory, see the Confidence-building measures chapter in this volume.

131 For example, Kazakhstan (session 10, meeting 3); Portugal (session 9, meeting 3); Netherlands (session 4, meeting 3); Australia (session 4, meeting 4); France (session 7, meeting 4).

132 A/79/214, Annex A, 21.

3.6. Human rights

In the OEWG 2021–2025 discussion of norm E,[133] national contributions coalesced around three main human rights considerations in relation to State conduct using ICTs. However, none of the arguments outlined below garnered consensus and all were therefore absent from the final report of OEWG 2021–2025.

First, especially during the earlier sessions, some States took the floor to reiterate that human rights were applicable online,[134] consistent with the agreements reached in other United Nations bodies (e.g., the General Assembly).[135] The notion that States should respect and protect human rights and fundamental freedoms, both online and offline, has been reflected in the Chair's Checklist as the central recommendation for the implementation of norm E.[136] Additionally, the Chair's Checklist recognizes that implementation efforts of norm E should go beyond the consideration of the General Assembly resolutions referred to in the norm and should take into account new challenges and dilemmas reflected in the General Assembly resolutions adopted since the norm was formulated in 2015.[137]

Second, the right to privacy has been a central component of the debate surrounding norm E. A few States expressed concern over State practices – such as arbitrary or unlawful mass surveillance, spyware, Internet shutdowns and the blocking of political content – viewing these practices as contrary to the expectations of norm E.[138] Some States proposed strengthening the privacy protections of the norm through the expansion of the additional layer of understanding to include measures to protect personal data.[139]

Finally, a few delegations emphasized the role of norm E in the mitigation of the gendered impacts of cyberthreats. One State, for instance, suggested that gendered impacts and proposals for implementation should be explicitly included in the additional layer of understanding for norm E.[140] Another State proposed an amendment to the Chair's Checklist to link freedom of expression to non-discrimination.[141]

---

133 "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression." A/76/135, 11.

134 For example, United Kingdom (session 1, meeting 5); Ireland (session 4, meeting 4); Czechia (session 4, meeting 4); European Union (on behalf of 38 States) (session 4, meeting 3)

135 General Assembly, resolution 78/213, 2023.

136 A/79/214, Annex A, 23.

137 A/79/214, Annex A, 26. See also A/76/135, paragraph 38.

138 For example, Costa Rica (session 4, meeting 3); Czechia (session 1, meeting 5); Netherlands (session 7, meeting 4).

139 For example, Kazakhstan (session 9, meeting 3); El Salvador (session 10, meeting 3); Malaysia (session 9, meeting 4); Brazil (session 9, meeting 4).

140 See Australia (session 4, meeting 4).

141 Netherlands (session 7, meeting 4).

3.7. Non-escalatory attribution

Several aspects of non-escalatory attribution, encapsulated in norm B although not described as such,[142] attracted rather polarized discussion among States participating in the OEWG 2021–2025. Just as for the human rights considerations, the final report of OEWG 2021–2025 does not record the discussions on attribution.

Early in the discussions in the OEWG 2021–2025, some States emphasized the fact that attribution is a sovereign national prerogative or shared their interpretations of aspects of an independent and unilateral attribution.[143]

In their interventions and proposals, delegations frequently cited technical difficulties – notably the ability of State and non-State actors to obfuscate their identities – that complicate attribution.[144] These concerns appear to have been raised with a view to strengthening the argument for a prudent, non-escalatory approach to attribution, as prescribed by norm B. Such an approach would involve a complex process, with consideration of different aspects of the ICT incident before pointing a finger.

States proposed various other solutions to support the operationalization of norm B. Some delegations recognized capacity-building as being the key enabler of an independent, objective attribution by States.[145] Other States suggested expanding the additional layer of understanding of the norm to support its implementation.[146]

However, some States rejected the credibility of any unilateral attribution, arguing that they are often politicized and subjective. Solutions suggested by some of the States objecting to unilateral attribution included the establishment of an impartial international attribution mechanism;[147] internationally agreed technical standards for attribution;[148] and a dedicated specific legal regime of primary rules, establishing legal foundation for attribution.[149]

---

142 "In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences." A/76/135.

143 For example, United States (session 2, meeting 5); Germany (session 2, meeting 5); France (session 4, meeting 3); Switzerland (session 4, meeting 4).

144 For example, Pakistan (session 1, meeting 5); Bangladesh (session 7, meeting 4); Argentina (session 1, meeting 5); Russian Federation (session 4, meeting 4); China (session 2, meeting 5); Portugal (session 9, meeting 3).

145 United States (session 2, meeting 5); India (session 4, meeting 4); Kenya (session 4, meeting 4).

146 For example, Switzerland (session 1, meeting 6); United States (session 2, meeting 5); Germany (session 2, meeting 5); Kenya (session 2, meeting 5).

147 Cuba (session 1, meeting 5); China (session 10, meeting 3); Pakistan (session 9, meeting 3).

148 Viet Nam (session 7, meeting 4).

149 For example, Iran (Islamic Republic of) (session 6, meeting 3).

Izumi Nakamitsu, UN High Representative for Disarmament Affairs, addresses the tenth substantive session of the the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 2025. Credit: UN Photo / Manuel Elías.

The second subject of contention remained proof in the context of attribution claims. One delegation argued that attribution claims "must be proven and substantiated by undisputable technical facts".[150] This alluded to the existence of legal obligation[151] and arguably signalled a departure from the expectations of voluntary behaviour of norm B and from the consensus conclusions of the 2021 GGE, namely that "accusations of organizing and implementing wrongful acts brought against States should be substantiated", [152] denoting expectations and not obligations of behaviour in extrajudicial setting.

150 Russian Federation (session 2, meeting 5) [emphasis added].

151 Previously outlined in Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security". For further discussion on international law of attribution, see the International Law chapter in this volume.

152 A/76/135, paragraph 71(g).

4. Insight beyond the official outcomes

As indicated in Sections 2–3, not all discussions and proposals garnered consensus in the OEWG 2021–2025; consequently, the final report remains silent on a number of aspects of the discussions on rules, norms and principles. Additionally, the final outcome document also lacks any indication of external factors influencing the relevant discussions and of proposals for new norms on responsible State use of ICTs; these two aspects are outlined in this section.

Throughout the negotiations of the OEWG 2021–2025, various external factors provided context for the delegations' arguments. In particular, the use of ICTs in the context of armed conflicts and the evolving ICT threat landscape proved to be the most influential factors.

Some States[153] argued that incidents involving the use of ICTs in the context of armed conflicts provided examples of non-adherence to the norms.

ICT incidents outside armed conflicts also influenced the discussions. A surge in ransomware attacks prompted a few States to suggest clearer guidance on norms related to due diligence in cyberspace and to cross-border cooperation.[154] A few States also highlighted specific ICT incidents as evidence of the urgent need for further multilateral discussion on the normative framework related to supply chain security.[155]

During the discussion of the OEWG 2021–2025, the broader threat landscape was also certainly not static,[156] which prompted a few States to either propose additional layer of understanding of existing norms[157] or to introduce new norms,[158] including in response to the specific guiding questions proposed by the Chair.[159] By the end of the process, States had not reached consensus on any of the proposed specific new norms of responsible State behaviour in their use of ICTs.

---

153 For example, Ukraine (session 6, meeting 3); Poland (session 6, meeting 4); European Union (on behalf of 35 States) (session 2, meeting 5); Netherlands (session 2, meeting 5); Germany (session 4, meeting 3); Slovakia (session 6, meeting 3); China (session 9, meeting 2); Russian Federation (session 9, meeting 3); Croatia (session 5, meeting 9); Switzerland (session 4, meeting 4); United States (session 2, meeting 5); Canada (session 2, meeting 5); Estonia (session 2, meeting 5).

154 For example, Germany (session 1, meeting 6); United States (session 7, meeting 4); Switzerland (session 2, meeting 5); France (session 9, meeting 4).

155 For example, Denmark (session 1, meeting 5); Czechia (session 4, meeting 4; United Kingdom (session 1, meeting 5).

156 For further discussion of threats, see the *Existing and Potential Threats* chapter in this volume.

157 For example, United States (session 7, meeting 4); Singapore (session 9, meeting 3); Kazakhstan (session 9, meeting 3).

158 For example, Algeria (session 4, meeting 4); South Africa (session 7, meeting 4); Bangladesh (session 9, meeting 3).

159 For example, Chairperson, Letter, 22 November 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_22_November_2023.pdf.

A non-exhaustive list of national proposals for the adaptation of the existing norms or adoption of new rules or norms, made either in writing in one of the working papers submitted by Member States during the process or communicated through statements made during the substantive sessions of the OEWG 2021–2025, can be found in Annex A of this chapter. Inclusion of this list does not imply that any of these norms should be adopted; it is instead for the benefit of potential further consideration, for instance in the context of the Global Mechanism.

Annex A. Proposals for new norms made by States during the OEWG 2021–2025

The table below includes a non-exhaustive list of proposals made by States during the OEWG 2021–2025 agenda point on "Norms, rules and principles" as well as proposals found in working papers submitted by States.[160] As reflected by the silence of the final report, none of the proposals below garnered consensus in the OEWG 2021–2025.

The table does not include proposals for norms that were restatements of existing voluntary norms. Nor does it include those either labelled by the proposing State or coalition of States as proposals for international legal obligations[161] or that feature language typical of legal obligations (e.g., the phrase "States must").

PROPOSAL TEXT	SOURCE	PROPOSING STATE(S)
"Countries should require their companies to strictly abide by the laws of the countries in which they are located, and must not require domestic companies to store data generated or obtained overseas within your borders."	OEWG statement, Session 1, meeting 6	China
"ICT products and services providers should . . . refrain from installing backdoors in your products and services to illegally obtain user data or to control or manipulate user systems and devices."		
"States should not use ICT information and communication networks, mass media and transnational media companies in order to carry out hostile information campaigns to interfere in the internal affairs of other States."	OEWG statement, Session 2, meeting 5	Russian Federation
"States that dominate the sphere of Information Technology, should not use their position to deprive other States of control over ICT products and services or to create threats to their political, economic and social security."		
"States should not use ICT advances as a tool for economic, political or any other type of coercive measures, including limiting or blocking measures against targeted States."	OEWG statement, Session 2, meeting 5	Iran (Islamic Republic of)
"States should refrain from and prevent the abuse of ICT supply chains developed under their jurisdiction and control to create or assist in the development of vulnerabilities in products [and] services."		

160 These papers are available from UNODA Meetings Place, https://meetings.unoda.org/meeting/57871.

161 Such as the proposal for the United Nations Convention on Ensuring International Information Security, introduced to the OEWG during the discussion on norms, rules and principles. See Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security".

PROPOSAL TEXT	SOURCE	PROPOSING STATE(S)
"States should ensure that appropriate measures are taken to ensure that the private sector with extra territorial impacts, including platforms, are held accountable for their behaviour in the ICT environment."	OEWG statement, Session 2, meeting 5	Iran (Islamic Republic of)
"All States should play an equal role in international internet governance and bear equal responsibility for internet governance."	OEWG statement, Session 2, meeting 5	Russian Federation
"States must exercise due control over their companies and platforms under their jurisdiction and control, otherwise they are responsible for knowingly intervening in the national sovereignty, security and public order of other States."	OEWG statement, Session 2, meeting 5; 'Submission to the First Substantive Session by Iran', 1 December 2021	Iran (Islamic Republic of)
"All countries should explicitly commit to non-proliferation of offensive cyber technology and develop relevant rules and norms on this matter."	OEWG statement, Session 4, meeting 3	China
"[A] new norm to protect against AI-powered cyber operations and attacks on AI systems."	OEWG statement, Session 7, meeting 4	South Africa
"[T]he prevention of the use of ICTs to undermine or infringe upon the sovereignty, territorial integrity, or independence of States, or to interfere in the internal affairs of States."	OEWG statement, Session 7, meeting 4	Russian Federation
"Inadmissibility of unsubstantiated accusations against States accused of organizing and committing wrongful acts with the use of ICTs . . . followed by the imposition of various restrictions such as sanctions."		
"States should ensure that AI technologies built and integrated into ICT systems within their territories are transparent and accountable, not biased."	OEWG statement, Session 9, meeting 3	Bangladesh
"States should take measures to prevent and hold accountable non-State actors, including private entities and individuals operating from their territory."		
"[S]tates should promote technological diversity and avoid actions that create monocultures in ICT products and services, which increase systemic vulnerabilities."		
"States should respect the digital sovereignty of other States by refraining from unauthorized access to data stored within another State's jurisdiction."		
"[W]e suggest that States provide better protection, including the allocation of criminal responsibility for those who, in good faith, penetrate into information systems to address vulnerabilities that could be exploited for unlawful purposes."	OEWG statement, Session 9, meeting 3	El Salvador

PROPOSAL TEXT	SOURCE	PROPOSING STATE(S)
"Kazakhstan advocates for a norm on zero trust approach, ensuring continuous verification and strict access controls."	OEWG statement, Session 10, meeting 3	Kazakhstan
"States should not use ICTs and information and communications networks . . . to carry out information campaigns, interfere in the internal affairs of other States and to undermine their political, economic and social stability."	"Contribution of the Russian Federation on rules, norms and principles of responsible behaviour of States in information space", 1 December 2021	Russian Federation
"States should endeavour to ensure supply chain security of ICT goods and services at all stages, to prevent other States from exploiting their dominant position in information technologies, including, inter alia, dominance in resources, critical infrastructures, core technologies, ICT products and services and information and communications networks to undermine States' right for independent control of ICT products and services, or to threaten their political, economic and social security."		
"States should promote a prominent role for the United Nations in areas such as encouraging the development of international legal norms for information security, peaceful settlement of international disputes, qualitative improvement in international cooperation in the field of information security; and other areas. States should enhance coordination among relevant international organizations."		
"The roles of States, with the primary responsibility for maintaining a secure, safe and trustable ICT environment, should be enhanced in ICT environment governance, including policy and decision making, at the global level."	"Submission to the First Substantive Session by Iran", 1 December 2021	Iran (Islamic Republic of)
"The principle of [s]tate sovereignty and international norms and principles that flow from sovereignty should be respected in ICT environment."		
"States should ensure appropriate measures to make the private sector with extraterritorial impacts, including platforms accountable for their behavior in the ICT environment."		
"States should refrain from and prevent abusing ICT supply chains developed under their jurisdiction and control, to create or assist the development of vulnerabilities in products, services and maintain compromising sovereignty and data protection of the target States."		
"Ensuring the balance between rights and responsibilities of States in the ICT environment."		

PROPOSAL TEXT	SOURCE	PROPOSING STATE(S)
"States should foster a cyberspace featuring peace, security, openness, cooperation and order, and should not use ICTs to carry out activities inconsistent with the objectives of maintaining international peace and security."	"China's Positions on International Rules-making in Cyberspace", 1 December 2021	China
"The principle of sovereignty applies in cyberspace. States should exercise jurisdiction over the ICT infrastructure, resources, data as well as ICT-related activities within their territories, and have the rights to protect their information systems and important data against damage resulting from threats, interference, attack and sabotage. ... States should participate in the management and distribution of international Internet resources on equal footings, and build a global Internet governance system of multilateralism, democracy and transparency."		
"States should enhance critical ICT infrastructure protection. States should stand against ICT activities that impair other States' critical infrastructure, impair or steal important data of other States' critical infrastructure. States should increase exchanges on legislation, best practices and technologies with regard to critical ICT infrastructure protection, and promote international cooperation on personnel training, technological innovation, early warning and prevention, emergency response, standards and regulations, and information sharing.		
"States should handle data security in a comprehensive, objective and evidence-based manner. States should foster an open, fair and non-discriminatory business environment, and maintain an open, secure and stable supply chain of global ICT products and services. States should take actions to prevent and put an end to activities that jeopardize personal information through the use of ICTs, and oppose mass surveillance against other States and unauthorized collection of personal information of other States with ICTs as a tool. States should encourage companies to abide by laws and regulations of the State where they operate, should not request domestic companies to store data generated and obtained overseas in their own territory, or obtain data located in other States through companies or individuals without other States' permission. ICT products and services providers should abide by laws and regulations of the State where they operate, not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices. ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products, nor force users to upgrade their systems and devices. Products providers should make a commitment to notifying their cooperation partners and users of serious vulnerabilities in their products in a timely fashion and offering remedies."		

PROPOSAL TEXT	SOURCE	PROPOSING STATE(S)
"States should step up cooperation against cyber terrorism. States should prohibit terrorist organizations from using the Internet to set up websites, online forums and blogs to conduct terrorist activities, including manufacturing, publication, storage and broadcasting of terrorist audio and video documents, disseminating violent terrorist rhetoric and ideology, fund-raising, recruiting, inciting terrorist activities, etc. States should conduct intelligence exchanges and law-enforcement cooperation, and develop cooperative partnership with international organizations, enterprises and citizens in countering cyber terrorism. States should request Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and accounts and deleting terrorist and violent extremist content."	"China's Positions on International Rules-making in Cyberspace", 1 December 2021	China
"States should reaffirm their commitment to the principle of abandonment of militarization of existing ICTs and the creation of new ICTs specifically designed to harm information resources, infrastructure and critical facilities of other countries."	"Russian amendments to draft OEWG report of 22 June 2022", 7 February 2022	Russian Federation
"States have the rights and responsibilities regarding legal protection of their CII against damage resulting from materialized threats in the use of ICTs, interference, attacks and sabotage."		
"States should not exploit political and technical advantages to undermine the security and integrity of CI of other States."		
"States should increase exchanges on standards and best practices with regard to CI protection and encourage enterprises to embark on such exchanges."		

Annex B. Number of times delegations took the floor on rules, norms and principles in the OEWG 2021-2025

STATE	COUNT	STATE	COUNT
European Union	22	New Zealand	13
Russian Federation	22	Pakistan	13
United Kingdom of Great Britain and Northern Ireland	21	Mexico	13
Netherlands (the Kingdom of the)	21	Mauritius	12
Australia	20	Italy	12
Iran (Islamic Republic of)	19	Fiji	12
Cuba	19	Czechia	11
Canada	18	Chile	11
Malaysia	17	Costa Rica	10
China (the People's Republic of)	17	India	10
Singapore	16	Albania	9
Japan	15	Portugal	9
United States of America	15	Kenya	9
Colombia	15	Ukraine	9
South Africa	15	Uruguay	9
Switzerland	15	Syrian Arab Republic	9
Egypt	15	Bangladesh	9
France	15	Thailand	8
Brazil	15	Ireland	8
Israel	15	Ghana	8
Argentina	15	Nigeria	8
El Salvador	14	Kazakhstan	7
Republic of Korea	14	Nicaragua	7
Germany	14	Poland	7
Indonesia	13	Austria	7
Viet Nam	13	Estonia	6

STATE	COUNT	STATE	COUNT
Dominican Republic	6	Malawi	2
Ecuador	6	Morocco	2
Slovakia	6	Senegal	2
Finland	5	Peru	2
Belarus	5	Uganda	2
Vanuatu	4	Timor-Leste	2
Côte d'Ivoire	4	Hungary	2
Botswana	4	Democratic People's Republic of Korea	2
Paraguay	4	Burkina Faso	2
Denmark	4	Saudi Arabia	1
Sweden	4	Kuwait	1
Zimbabwe	4	Papua New Guinea	1
Latvia	4	Sierra Leone	1
Jordan	4	Kiribati	1
Sri Lanka	4	Tunisia	1
Democratic Republic of the Congo	3	United Republic of Tanzania	1
Mozambique	3	Haiti	1
Djibouti	3	Greece	1
Cameroon	3	Sudan	1
Venezuela, Bolivarian Republic of	3	Qatar	1
Lao People's Democratic Republic	3	Honduras	1
Romania	3	Georgia	1
Guatemala	3	Armenia	1
Iraq	3	Republic of Moldova	1
Philippines	3	Antigua and Barbuda	1
Croatia	3	Bosnia and Herzegovina	1
Belgium	3	Mali	1
Spain	3	Ethiopia	1
Tonga	2	Lebanon	1
Algeria	2		

International law

Andrea Gronke and Dominique Steinbrecher

1. Introduction

International law is a set of binding rules and principles that guide relations between sovereign States, providing a framework for peaceful coexistence.[1] The international legal order, and in particular the United Nations Charter adopted in 1945, remains a core element of the maintenance of international peace and security and forms the foundation of international cooperation, which is essential to making cyberspace stable and secure.[2]

This chapter analyses the discussions on international law during the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025. The OEWG 2021–2025 was established pursuant to United Nations General Assembly resolution 75/240 to continue to discuss, among other issues, how international law applies to State use of information and communications technologies (ICTs).[3] The chapter first gives a historical outline of key milestones in the evolution of multilateral discussions on the application of international law to State use of ICTs.[4] It then, in Section 2, provides an overview of how these discussions evolved over the four cycles of the OEWG 2021–2025 process. Section 3 explores the main thematic issues raised during the negotiations, before the chapter concludes in Section 4 with insights into areas of convergence and divergence that extend beyond the OEWG's official outcomes.

1.1. The road to OEWG 2021–2025

International law considerations have been an important element of maintaining international stability and security in the use of ICTs since 1999, when discussions on international ICT security formally landed on the agenda of the United Nations General Assembly.[5]

In 2013, the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security 2012–2013

---

1 UNIDIR Security and Technology Programme, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (Geneva: UNIDIR, 2024), https://unidir.org/publication/a-compendium-of-good-practices-developing-a-national-position-on-the-interpretation-of-international-law-and-state-use-of-ict/.

2 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, forward by the Secretary-General.

3 General Assembly, resolution 75/240, 2021, paragraph 1.

4 This chapter uses the terms "international ICT security" and "cybersecurity", as well as "state use of ICTs" and "cyberspace", where relevant, to remain faithful to the language used in the United Nations process and by Member States in their statements.

5 General Assembly, resolution 53/70, 1998.

acknowledged the central role of international law in governing the use of ICTs. For the first time, the GGE explicitly recognized that international law, and in particular the United Nations Charter, is applicable to State use of ICTs and "essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[6] Moreover, it explicitly recognized the application of specific areas of international law to State use of ICTs. These included the concrete recognition of State sovereignty and the "international norms and principles that flow from sovereignty"; respect for human rights and fundamental freedoms as set forth in the 1948 Universal Declaration of Human Rights and other relevant instruments; obligations regarding the law of State responsibility; and certain expectations regarding due diligence.[7] This final report of the GGE 2012–2013 was welcomed by the General Assembly.[8]

In the subsequent GGEs, international law became a distinct substantive issue in intergovernmental negotiations on international ICT security, and thus an evolving independent pillar of the so-called United Nations Framework for Responsible State Behaviour in Cyberspace.[9] This separated international law from the agenda topic on "Norms, rules and principles for the responsible behaviour of States",[10] which focused on voluntary non-binding norms.[11] Having reaffirmed the application of international law to State use of ICTs on many occasions through the successive outcome reports of the GGEs and the OEWG 2019–2021,[12] Member States turned the focus of their discussions to *how* international law rules and principles apply to State behaviour, with the aim of building common understandings in this regard.[13]

In 2015, the final report of the GGE 2014–2015 identified a list of principles of the United Nations Charter and other international law as being of central importance to State use of ICTs.[14]

This list encompassed:

- Sovereign equality
- The settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered
- Refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations

---

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/68/98**, 2013, paragraph 19.

7 **A/68/98**, paragraphs 21, 23.

8 General Assembly, resolution **68/243**, 2013.

9 **A/70/174**, defining the so-called "pillars" of the Framework.

10 **A/70/174**. The agenda topic was then relabelled as 'Rules, norms and principles for responsible State behaviour' in the OEWG 2019–2021.

11 See the chapter on rules, norms and principles in this volume.

12 **A/70/174** (GGE 2014–2015); 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 (GGE 2019–2021); 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 (OEWG 2019–2021).

13 **A/68/98**, paragraph 16; **A/70/174**, paragraph 29.

14 This report was welcomed by General Assembly resolution **70/237**, 2015.

- Respect for human rights and fundamental freedoms, and
- Non-intervention in the internal affairs of other States[15]

Moreover, the members of the GGE articulated non-exhaustive views on how certain rules and principles of international law apply to the use of ICTs by States. These views included, for example, additional language regarding State jurisdiction, the right of States to take measures consistent with international law, and attribution. Additionally, the GGE noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.[16]

Discussion on the application of international law continued during the GGE 2016–2017 but failed to reach consensus.[17] Between 2019 and 2021, States embarked on further negotiations regarding the application of international law in cyberspace in two parallel processes on ICT security: a sixth GGE and a new OEWG, open to all United Nations Member States.

Building on previous understandings, the final report of the GGE 2019–2021 elaborated an additional layer of understanding on how international law applies to State use of ICTs.[18] The GGE expanded on certain aspects of the application of the obligations set forth in Articles 2(3) and 33 of the United Nations Charter on the peaceful settlement of disputes, as well as on the application of State sovereignty and non-intervention, the prohibition of the threat or use of force, the inherent right to take measures consistent with international law and as recognized in the Charter, and States' obligations regarding internationally wrongful acts attributable to them under international law.[19] Moreover, for the first time, the GGE noted that international humanitarian law (IHL) applies only in situations of armed conflict, recalled the established principles noted in the 2015 GGE report, and the need to further study how and when these principles apply to the use of ICTs by States.[20]

Through the final report of the OEWG 2019–2021, States recognized the General Assembly resolutions welcoming the 2013 and 2015 GGE reports and reaffirmed the application of international law to the use of ICTs.[21] Although less detailed than the report of the GGE 2019–2021 that followed shortly after, the OEWG report carried particular weight as a consensus outcome of all United Nations Member States. In addition to areas of consensus reflected in the final report, the Chair of the OEWG 2019–2021 issued a "Chair's Summary" reflecting his understanding of the main points discussed during the meetings, including the in-depth exchanges on international law.[22]

---

15 A/70/174, paragraph 26.

16 A/70/174, paragraph 28.

17 General Assembly, First Committee, Official Record, A/C.1/72/PV.19, 2017, 1, explaining that one of the reasons was the lack of consensus on some aspects of how international law applies to the use of ICTs by States.

18 This report was welcomed by the General Assembly. See A/76/135.

19 A/76/135, paragraph 71. See also General Assembly, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Draft Final Substantial Report, A/AC.290/2021/CRP.2, 2021, paragraph 36.

20 A/76/135, paragraph 71(f).

21 A/AC.290/2021/CRP.2. The report was welcomed by the General Assembly.

22 See General Assembly, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021

A representative of Liberia (centre) gives statement on behalf of African States during the eleventh substantive session of the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025, New York. Credit: UN Photo / Loey Felipe.

Both processes recommended that States continue to study this topic to further clarify and develop common understandings on how international law applies to State use of ICTs as an essential step towards avoiding misunderstandings and increasing predictability and stability.[23] In particular, States were encouraged to exchange views, including through the voluntary sharing of national views and practices.[24] The GGE 2019–2021 also made available an official compendium of voluntary national contributions of participating governmental experts on the application of international law to the use of ICTs by States.[25]

(noting in its paragraph 3 that the summary "may not reflect the full contributions of all delegations and should not be seen as reflecting the consensus view of States on any specific points covered in it"). See, in particular, paragraph 18, highlighting that certain questions on how international law applies to the use of ICTs have yet to be fully clarified.

23 A/76/135, paragraph 72.

24 A/AC.290/2021/CRP.2, paragraphs 36, 38, 40. See also A/76/135.

25 General Assembly, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly resolution 73/266", A/76/136, 2021. See also A/76/135, paragraph 73.

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

Across the different cycles of the OEWG 2021–2025, different approaches underpinned the discussions on the application of international law in cyberspace. On one side were States that emphasized the sufficiency of existing international law and prioritized its application in cyberspace.[26] On the other were those proposing the development of new legally binding rules, including through the negotiation of a specific international legal instrument, to address gaps arising from the unique characteristics of ICTs.[27] Some States were less categorical about one approach or the other; these States highlighted that the two approaches were not contradictory or mutually exclusive since discussions on the application of existing international law could lead to the eventual negotiation of new rules.[28]

2.1. Consolidating foundational elements and designing future discussions on the application of international law to the State use of ICTs

Substantive discussions on international law within the OEWG 2021–2025 commenced with a reaffirmation of the application of international law in cyberspace and its role in contributing to peace and stability in international relations.[29] Many States stressed that discussions should build upon the existing *acquis* – a term used by some States to refer to existing consensus based on the reports of the previous multilateral processes – and take forward the foundational elements of the consensus language of the previous processes.[30] This included, predominantly, the non-exhaustive list of international law principles developed in the previous GGEs and OEWG.[31]

---

26 For example, Israel (session 1, meeting 6); Colombia (session 1, meeting 6); European Union on behalf of 35 States (session 2, meeting 6); Republic of Korea (session 2, meeting 6); Switzerland (session 2, meeting 6); Australia (session 2, meeting 6); New Zealand (session 2, meeting 6); Netherlands (session 4, meeting 5); Japan (session 4, meeting 5).

27 For example, Russian Federation (session 1, meeting 6; session 4, meeting 4); Iran (Islamic Republic of) (session 2, meeting 6); Cuba (session 2, meeting 6; session 4, meeting 5); Pakistan (session 1, meeting 7); China (session 1, meeting 7); Belarus (session 2, meeting 6); Syria (session 2, meeting 6).

28 For example, Brazil (session 7, meeting 5); Philippines (session 9, meeting 5). See similarly Egypt (session 11, meeting 3).

29 For example, European Union on behalf of 34 States (session 1, meeting 6); United Kingdom (session 1, meeting 6); Switzerland (session 1, meeting 6); Philippines (session 1, meeting 6); Argentina (session 1, meeting 6); South Africa (session 1, meeting 7); Republic of Korea (session 1, meeting 7); India (session 1, meeting 7); Singapore (session 1, meeting 7; session 2, meeting 6); Iraq (session 1, meeting 7); Egypt (session 1, meeting 7; session 2, meeting 6); Indonesia (session 1, meeting 7); Australia (session 1, meeting 7); Malaysia (session 1, meeting 7); Mexico (session 1, meeting 7); Brazil (session 1, meeting 7); Pakistan (session 1, meeting 7); France (session 1, meeting 7); China (session 1, meeting 7); Costa Rica (session 1, meeting 7); India (session 2, meeting 6); Chile (session 2, meeting 6); Botswana (session 2, meeting 6); Fiji (session 2, meeting 6).

30 For example, Ireland (session 1, meeting 6); Austria (session 1, meeting 6); United Kingdom (session 1, meeting 6); Switzerland (session 1, meeting 6); Estonia (session 1, meeting 7); France (session 1, meeting 7; session 2, meeting 6); European Union on behalf of 35 States (session 2, meeting 6); Sweden (session 2, meeting 6); Fiji (session 2, meeting 6); Canada (session 2, meeting 6); India (session 2, meeting 6).

31 For example, Switzerland (session 1, meeting 6); Netherlands (session 1, meeting 6); India (session 1,

Recalling the existing *acquis*, some States considered the question of whether international law applies to have been answered in the affirmative. On that basis, they encouraged States to advance discussions on how international law applies to State use of ICTs.[32] Other States considered that specific questions on the application of international law in cyberspace remained unresolved and lacked consensus.[33] Moreover, many States emphasized the OEWG as an opportunity to enhance transparency of views and build common understandings on the topic.[34]

During the negotiations of the OEWG's first annual progress report (APR) in July 2022, Member States shared their views primarily on both the role of the OEWG in facilitating discussion on international law as well as on priority topics to focus on during the negotiations.

On the role of the OEWG, many States expressed the view that this multilateral process should provide a platform for focused and in-depth discussions on particularly important topics of international law.[35] Priority topics identified by some States included, among others, State sovereignty,[36] State responsibility,[37] human rights and fundamental freedoms,[38] international humanitarian law,[39] and the principle of cooperation.[40] While some States stressed that discussions should focus on identifying areas of convergence and divergence with a view to developing common understandings on the application of international law in cyberspace,[41]

---

meeting 7); Singapore (session 1, meeting 7); Egypt (session 1, meeting 7; session 2, meeting 6); Iran (Islamic Republic of) (session 2, meeting 6); Brazil (session 1, meeting 7); Pakistan (session 1, meeting 7); Ghana (session 2, meeting 6;); India (session 2, meeting 6); Ukraine (session 1, meeting 6).

32 For example, Brazil (session 2, meeting 6); European Union on behalf of 35 States (session 1, meeting 6).

33 For example, China (session 1, meeting 7). See similarly Cuba (session 1, meeting 7).

34 For example, Israel (session 1, meeting 6); Austria (session 1, meeting 6); Japan (session 1, meeting 6); India (session 1, meeting 7); Indonesia (session 1, meeting 7); Estonia (session 1, meeting 7); Kenya (session 1, meeting 7); Malaysia (session 1, meeting 7); Czechia (session 1, meeting 7); France (session 1, meeting 7); Costa Rica (session 1, meeting 7); European Union on behalf of 35 States (session 2, meeting 6); Kenya (session 2, meeting 6); India (session 2, meeting 6); South Africa (session 2, meeting 6); Colombia (session 2, meeting 6); New Zealand (session 2, meeting 6); Ireland (session 2, meeting 6).

35 For example, Austria (session 1, meeting 6); India (session 1, meeting 7); Colombia (session 2, meeting 6); Czechia (session 1, meeting 7); Sweden (session 2, meeting 6); Switzerland (session 2, meeting 2); Costa Rica (session 2, meeting 6); Canada (session 2, meeting 6); Brazil (session 2, meeting 6); France (session 2, meeting 6); Indonesia (session 2, meeting 6); Chile (session 2, meeting 6).

36 For example, China (session 1, meeting 7) on the publication of "China's Views on the Application of the Principle of Sovereignty in Cyberspace", **https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf**. See also Japan (session 2, meeting 6).

37 For example, Ukraine (session 1, meeting 6); Netherlands (session 2, meeting 6); Switzerland (session 2, meeting 6); Republic of Korea (session 1, meeting 7); Australia (session 1, meeting 7); Estonia (session 1, meeting 7); Canada (session 2, meeting 6).

38 For example, Ireland (session 1, meeting 6); United Kingdom (session 1, meeting 6); Switzerland (session 1, meeting 6); Netherlands (session 1, meeting 6); Germany (session 1, meeting 7); Estonia (session 1, meeting 7); Italy (session 1, meeting 7); Mexico (session 1, meeting 7); European Union on behalf of 35 States (session 2, meeting 6); Canada (session 2, meeting 6); Uruguay (session 2, meeting 6).

39 For example, European Union on behalf of 34 States (session 1, meeting 6); United Kingdom (session 1, meeting 6); Colombia (session 1, meeting 6); Switzerland (session 1, meeting 6); Indonesia (session 1, meeting 7); Australia (session 1, meeting 7); Mexico (session 1, meeting 7); Costa Rica (session 1, session 7, meeting 7); Canada (session 2, meeting 6); Chile (session 2, meeting 6); Republic of Korea (session 2, meeting 6); Joint statement of Argentina, Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Indonesia, Japan, Jordan, Mexico, Netherlands, Republic of Korea, Senegal, Sweden and Switzerland, **https://documents.unoda.org/wp-content/uploads/2022/07/Joint- statement-IHL-OEWG.pdf**. However, some States presented cautious approaches to the application of IHL in cyberspace. For example, Cuba (session 1, meeting 7; session 2, meeting 6); Russian Federation (session 3, meeting 4); Nicaragua (session 3, meeting 3).

40 For example, Russian Federation (session 1, meeting 6; session 2, meeting 6).

41 For example, Austria (session 1, meeting 6); France (session 1, meeting 7); United Kingdom (session 1, meeting 6);United States (session 2, meeting 6); Australia (session 1, meeting 7); Kenya (session 2, meeting 6).

others also highlighted the need to identify gaps in, and matters left unregulated by, existing international law.[42]

Capacity-building specific to international law was considered essential to fostering understanding of international law and increasing participation of all States in related discussions. Its promotion was thus widely endorsed from the beginning of discussions.[43]

The first APR reflected many of the discussions, including a non-exhaustive list of proposals for further consideration in the subsequent OEWG sessions.[44] It provided guidance for the next steps, including the continued exchange of views and encouragement to share them voluntarily through existing mechanisms (e.g., the UNIDIR Cyber Policy Portal) as requested by several States during the negotiations.[45] Moreover, the consensus language provided the basis for focused discussions on topics from the "non-exhaustive list" proposed by States.[46] These included how relevant rules and principles of international law apply, and whether gaps in common understandings exist.[47]

2.2. Designing a road map for focused discussions

Following the recommended steps from the APR, States agreed to continue exchanging views on how international law applies to their use of ICTs. They aimed to engage in focused substantive discussions, predominantly on the topics included in the non-exhaustive list – in particular, on how the Charter of the United Nations applies in the use of ICTs and related questions on sovereignty, sovereign equality, non-intervention in the internal affairs of other States and the peaceful settlement of disputes.[48]

---

42 For example, Pakistan (session 1, meeting 7); Russian Federation (session 1, meeting 6; session 2, meeting 6); see, relatedly, Egypt (session 2, meeting 5).

43 For example, Ireland (session 1, meeting 6; session 2, meeting 6); Austria (session 1, meeting 6); Colombia (session 1, meeting 6; session 2, meeting 6); Switzerland (session 1, meeting 6); Republic of Korea (session 1, meeting 7); Singapore (session 1, meeting 7); Australia (session 1, meeting 7; session 2, meeting 6); Estonia (session 1, meeting 7); Italy (session 1, meeting 7); Kenya (session 1, meeting 7); Malaysia (session 1, meeting 7); Czechia (session 1, meeting 7); France (session 1, meeting 7); European Union on behalf of 35 States (session 2, meeting 6); Paraguay (session 2, meeting 6); Canada (session 2, meeting 6); Chile (session 2, meeting 6); Botswana (session 2, meeting 6); Guatemala (session 2, meeting 6); Malawi (session 2, meeting 6); India (session 2, meeting 6); Brazil (session 2, meeting 6).

44 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 15.

45 For example, Austria (session 1, meeting 6); Japan (session 1, meeting 6; session 2, meeting 6); Germany (session 1, meeting 7; session 2, meeting 6); United Kingdom (session 1, meeting 6; session 2, meeting 6); Colombia (session 1, meeting 6; session 2, meeting 6); Estonia (session 1, meeting 7; session 2, meeting 6); Italy (session 1, meeting 7); Kenya (session 1, meeting 7); France (session 1, meeting 7; session 2, meeting 6); Uruguay (session 2, meeting 6); Republic of Korea (session 2, meeting 6); Fiji (session 2, meeting 6); Malawi (session 2, meeting 6); United States (session 2, meeting 6).

46 **A/77/275**, paragraph 15(a).

47 **A/77/275**, recommendation 2.

48 See the Chair's guiding questions for session 4 of the OEWG, annexed to Chairperson OEWG 2021–2025, Letter from the Chair, 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**.

Some States restated the need to move beyond the reaffirmation of the applicability of the non-exhaustive list of rules and principles, and turn to focused,[49] detailed[50] and practical[51] discussions on a defined set of international law topics, allowing for substantive legal exchanges and development of common understandings. In this regard, substantive contributions from States significantly grew during the discussions in the second cycle of the OEWG, with a predominant focus on the application of the United Nations Charter.[52] To that end, a group of States proposed identifying areas of emerging convergence.[53] The second APR explicitly reaffirmed focused discussions on topics such as the principles of sovereignty and sovereign equality, the peaceful settlement of disputes, the prohibition of the threat or use of force, and the prohibition of intervention.[54]

There was widespread support for continuing to develop a clear road map with concrete next steps and topics for discussions.[55] A paper submitted on "A Practical Approach to International Law in the 2021–2025 OEWG"[56] included proposals on modalities and thematic areas (e.g., the United Nations Charter, State responsibility, peaceful settlement of disputes and IHL) as a starting point for the OEWG discussions. It received support from several delegations.[57]

Some States deemed it important to also focus on gaps in existing international law and the development of additional legal rules.[58] The proposal to develop a legally binding instrument was discussed, including in the context of the submission of an "Updated Concept of the

---

49 For example, Netherlands (session 4, meeting 5); Czechia (session 4, meeting 5); Estonia (session 4, meeting 5); Australia (session 4, meeting 5); Germany (session 4, meeting 5); Japan (session 4, meeting 5); Croatia (session 4, meeting 5); United States (session 4, meeting 5); India (session 4, meeting 5); Pakistan (session 4, meeting 6).

50 For example, Austria (session 4, meeting 4).

51 For example, Sweden on behalf of the Nordic States (session 4, meeting 4); United Kingdom (session 4, meeting 4).

52 For example, Singapore (session 4, meeting 4); Estonia (session 4, meeting 5); Australia (session 4, meeting 5); Chile (session 4, meeting 5); New Zealand (session 4, meeting 5); Germany (session 4, meeting 5); United States (session 4, meeting 5); China (session 4, meeting 5); France (session 4, meeting 5); Fiji (session 4, meeting 6).

53 "Applicability of International Law, in Particular the United Nations Charter, in the Use of ICTs: Areas of Convergence", Working paper submitted by Australia, Colombia, El Salvador, Estonia and Uruguay, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cyber_OEWG_-_International_Law_APR_paper_-_updated_-_24_July_2023.pdf. This was welcomed by many delegations, including, for example, European Union (session 5, meeting 3); United Kingdom (session 5, meeting 4); Vanuatu (session 5, meeting 5); New Zealand (session 5, meeting 3); Croatia (session 5, meeting 4).

54 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, paragraph 30.

55 For example, Canada (session 4, meeting 4); United Kingdom (session 4, meeting 4); Switzerland (session 4, meeting 5); Australia (session 4, meeting 5).

56 "A Practical Approach to International Law in the 2021–2025 OEWG", Working paper submitted by Canada and Switzerland, 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated_-_A_Practical_Approach_to_International_Law_in_the_OEWG_-_Canada-Switzerland_Concept_Paper_Nov_18_2022.pdf.

57 For example, Netherlands (session 4, meeting 5); Sweden on behalf of the Nordic States (session 4, meeting 4); United Kingdom (session 4, meeting 4); European Union on behalf of 36 States (session 4, meeting 4); Austria (session 4, meeting 4); Czechia (session 4, meeting 5); Estonia (session 4, meeting 5); New Zealand (session 4, meeting 5); Germany (session 4, meeting 5); Croatia (session 4, meeting 5); Belgium (session 4, meeting 5); Ireland (session 4, meeting 5); France (session 4, meeting 5); Colombia (session 4, meeting 6).

58 For example, Russian Federation (session 4, meeting 4); Iran (Islamic Republic of) (session 4, meeting 5); Iraq (session 4, meeting 5).

Convention of the United Nations on Ensuring International Information Security",[59] support for which extended beyond its cosponsors.[60] The second APR included language on this issue, noting the possibility of future elaboration of additional binding obligations, if appropriate.[61]

In terms of modalities, there was wide support for the establishment of dedicated sessions at the OEWG and intersessional meetings on international law.[62] However, other States requested a cautious approach and the need for balance in the selection of topics for intersessional discussions.[63] Engagement with legal experts during focused discussions was encouraged.[64] Others suggested seeking views from relevant bodies, such as the International Law Commission (ILC), on the applicability of international law to the use of ICTs by States.[65]

The topic of capacity-building on international law gained prominence during the second cycle. In addition to seminars, workshops and training courses, emphasis was also put on sharing good practices at different levels.[66]

2.3. Growing involvement, deepening substantive deliberation and methodological maturation

While divergent views on the sufficiency of existing international law to safeguard the peace and security of ICTs persisted, the third cycle of the OEWG was marked by a significant increase in participation and substantive contributions from Member States on the matter.

The increased number of States delivering detailed statements on international law was highlighted by the Chair of the OEWG and several delegations.[67] Member States shared

---

59 Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security" (Cosponsors: Belarus, Democratic People's Republic of Korea, Nicaragua, Syria, Venezuela), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf.

60 For example, Iran (Islamic Republic of) (session 4, meeting 5); Cuba (session 4, meeting 5); China (session 4, meeting 5); Nicaragua on behalf of Burundi, Belarus, China, Cuba, Democratic People's Republic of Korea, Nicaragua, Russia, Syria and Venezuela (session 5, meeting 1); Iran (Islamic Republic of) on behalf of the same group (session 5, meeting 4).

61 A/78/265, paragraph 32.

62 For example, European Union on behalf of 36 States (session 4, meeting 4); Sweden on behalf of the Nordic States (session 4, meeting 4); United Kingdom (session 4, meeting 4); Austria (session 4, meeting 4); Canada (session 4, meeting 4); South Africa (session 4, meeting 4); Netherlands (session 4, meeting 5); Belgium (session 4, meeting 5); Switzerland (session 4, meeting 5); Czechia (session 4, meeting 5); Australia (session 4, meeting 5); New Zealand (session 4, meeting 5); Croatia (session 4, meeting 5); Ireland (session 4, meeting 5); Malawi (session 4, meeting 5); Republic of Korea (session 4, meeting 5); Romania (session 4, meeting 6); Pakistan (session 4, meeting 6); Colombia (session 4, meeting 6); Fiji (session 4, meeting 6); Dominican Republic (session 4, meeting 6); El Salvador (session 4, meeting 6); Jordan (session 4, meeting 6); Costa Rica (session 4, meeting 5); Philippines (session 5, meeting 3).

63 For example, China (session 4, meeting 5); Nicaragua (session 4, meeting 6).

64 For example, Switzerland (session 4, meeting 5); United Kingdom (session 4, meeting 4); Netherlands (session 4, meeting 5); Canada (session 4, meeting 4); Australia (session 4, meeting 5); Iraq (session 4, meeting 5); Mexico (session 5, meeting 3).

65 For example, South Africa (session 4, meeting 4); Jordan (session 4, meeting 6); Viet Nam (session 4, meeting 5); Argentina (session 5, meeting 3).

66 For example, India (session 4, meeting 5); Fiji (session 4, meeting 6).

67 For example, Joint Statement by Colombia on behalf of Australia, El Salvador, Estonia and Uruguay (session 7,

substantive views, including concrete examples, on the application of different rules and principles, particularly those included in the non-exhaustive list, which significantly deepened the discussions.[68]

The need for focused discussion on the application of IHL to the use of ICTs in situations of armed conflict was highlighted by numerous delegations.[69] A group of States submitted a dedicated working paper on the subject.[70] These States considered that the discussion would help to develop common understandings on how to best protect civilians and civilian objects and on what actions are prohibited or required during armed conflict.[71] Nevertheless, this topic remained controversial. Some States emphasized the lack of consensus on the application of IHL in cyberspace[72] (see Subsection 3.2.2) and called for a cautious approach to transposing the application of IHL in a generalized manner.

A topic that gained prominence in the discussions was the concern for growing threats against critical civilian infrastructure and calls to address these threats through international law.[73] In addition, several delegations highlighted the need to address the complexities of attribution in the use of ICTs.[74]

Moreover, some States sought to identify three additional areas of emerging convergence, namely, IHL, State responsibility, and human rights and fundamental freedoms.[75] A cross-regional working paper was presented by a group of States proposing specific language for the third APR.[76] While the third APR maintained the references to core rules and principles,

---

meeting 5); Canada (session 7, meeting 6).

68 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, paragraph 38(a).

69 For example, United States (session 6, meeting 5; session 7, meeting 6); Mexico (session 6, meeting 5); Germany (session 6, meeting 5; session 7, meeting 6); United Kingdom (session 6, meeting 5); Bangladesh (session 6, meeting 5); South Africa (session 6, meeting 5); Australia (session 6, meeting 5); Chile (session 6, meeting 6; session 7, meeting 5); Ukraine (session 6, meeting 6); Austria (session 7, meeting 5); Italy (session 7, meeting 5); France (session 7, meeting 6); Kiribati (session 6, meeting 5). See also ICRC (session 6, meeting 6).

70 "Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts", Working paper submitted Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Senegal, Sweden and Switzerland, 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations.pdf. The paper was supported by other delegations, for example, Belgium (session 7, meeting 5); Italy (session 7, meeting 5); Ireland (session 7, meeting 5); Spain (session 7, meeting 6).

71 See Senegal on behalf of Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Sweden, Switzerland and Senegal (session 7, meeting 5).

72 For example, China (session 7, meeting 5); Russian Federation (session 8, meeting 3).

73 For example, Ukraine (session 6, meeting 6); United Kingdom (session 6, meeting 5); Mexico (session 7, meeting 5); Japan (session 6, meeting 5); Slovakia (session 7, meeting 5).

74 For example, Pakistan (session 7, meeting 5). See similarly China (session 8, meeting 3).

75 For example, South Africa (session 6, meeting 5); Australia (session 7, meeting 5); Austria (session 6, meeting 5); New Zealand (session 6, meeting 5); Canada (session 6, meeting 4); European Union on behalf of 37 States (session 6, meeting 4); Ireland (session 6, meeting 5).

76 "Application of International Law in the Use of ICTs: Areas of Convergence", Working paper submitted by Australia, Colombia, El Salvador, Estonia, Fiji, Kiribati, Thailand, Uruguay, 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cyber_OEWG9_-_Cross-Regional_Working_Paper_on_International_Law.pdf. The paper was welcomed by other delegations: for example, Switzerland (session 7, meeting 5); Netherlands (session 7, meeting 5); Italy (session 7, meeting 5); Ireland (session 7, meeting 5); Canada (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6); Spain (session 7, meeting 6).

it included some updated language and added further nuance to the legal interpretations, particularly on sovereignty and the prohibition of the threat or use of force.[77]

Several States highlighted the importance of in-depth discussions on international law during intersessional meetings, with participation of legal advisors and legal experts.[78] The third APR proposed that future discussions should benefit from experts and, following their mention by a few delegations, included explicit reference to the ILC[79] and academia.[80]

Different views were also shared on the unique features of ICTs in the context of the sufficiency of existing international law.[81] On the one hand, some States considered that the unique technical characteristics of ICTs result in legal gaps that merit new legally binding rules.[82] On the other hand, some States considered that cyberspace is not so unique that it requires a different approach[83] that cannot be accommodated through the application of existing rules.[84] Many States emphasized that discussions on potential gaps or additional rules are premature.[85] Some considered that discussions on the application of existing rules of international law to ICTs and the potential pursuit of specific legally binding measures were not mutually exclusive.[86] The third APR only broadly reflected the spectrum of views in this regard.

Negotiations during this cycle included discussions on methodologies to address the topic of international law. Many States emphasized the impact of holding scenario-based exercises on international law and suggested using scenarios as an element to facilitate focused discussions and the exchange of views at the OEWG.[87]

---

77 A/79/214, paragraph 37.

78 For example, Netherlands (session 7, meeting 5); Austria (session 7, meeting 5); Mexico (session 7, meeting 5); Malaysia (session 7, meeting 5); Canada (session 7, meeting 6).

79 For example, Mexico (session 6, meeting 5; session 7, meeting 5); Italy (session 6, meeting 5); Bangladesh (session 6, meeting 5; session 7, meeting 5); South Africa (session 7, meeting 5).

80 For example, United Kingdom (session 7, meeting 5); Malaysia (session 7, meeting 5); Netherlands (session 8, meeting 3).

81 Compare with Guiding question shared by Chair for seventh substantive session, annexed to Chairperson OEWG 2021–2025, Letter from the Chair, 20 February 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_20_February_2024.pdf.

82 For example, Russian Federation (session 6, meeting 5); Bangladesh (session 6, meeting 5). See, in this regard, Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security" (Cosponsors: Belarus, Cuba, Democratic People's Republic of Korea, Nicaragua, Syria, Venezuela), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on__ensuring_international_information_security.pdf. See also Iran (Islamic Republic of) (session 7, meeting 5); Sri Lanka (session 7, meeting 6); Pakistan (session 6, meeting 5); China (session 6, meeting 5); and support from Viet Nam (session 6, meeting 5) and Burkina Faso (session 7, meeting 6).

83 For example, Canada (session 6, meeting 4); Switzerland (session 6, meeting 5); New Zealand (session 6, meeting 5). See also Spain (session 6, meeting 5).

84 For example, Ireland (session 6, meeting 5); Switzerland (session 6, meeting 5); Netherlands (session 6, meeting 5); United Kingdom (session 6, meeting 5); Czechia (session 6, meeting 5); Italy (session 6, meeting 5).

85 For example, United States (session 6, meeting 5); France (session 6, meeting 5).

86 For example, Brazil (session 6, meeting 5; session 7, meeting 5); Philippines (session 9, meeting 5); Egypt (session 11, meeting 3).

87 For example, Germany (session 6, meeting 5; session 7, meeting 6); Singapore (session 7, meeting 5); United States (session 7, meeting 6); Republic of Korea (session 7, meeting 5); Colombia on behalf of Australia,

Several national positions and a regional position[88] on how international law applies in cyberspace were launched or their development announced during the third cycle of the OEWG (see Subsection 3.4). The development and publication of positions received widespread support from delegations.[89] This reinforced the encouragement to develop national positions,[90] as well as the role of capacity-building and cooperation in sharing experiences[91] and good practices,[92] enhancing the expertise to develop national and regional positions,[93] and strengthening national expertise[94] to support participation in international law discussions in an equal footing.[95] Several States emphasized the work of regional and subregional organizations in capacity-building[96] and developing common understandings.[97]

El Salvador, Estonia, Uruguay (session 7, meeting 5); Philippines (session 7, meeting 5); Switzerland (session 7, meeting 5); Belgium (session 7, meeting 5); Austria (session 7, meeting 5); Japan (session 7, meeting 5); United Kingdom (session 7, meeting 5); Malaysia (session 7, meeting 5); Canada (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6); Israel (session 7, meeting 6); Malawi (session 7, meeting 6).

88 The Common African Position, which represents the 55 member States of the African Union. African Union Common Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, annexed to African Union, Peace and Security Council, Communiqué, 29 January 2024, https://cms.cyberpolicyportal.org/uploads/CAP_Communiques_FULL_0e34eb5799.pdf.

89 For example, Canada (session 6, meeting 4); European Union on behalf of 36 States (session 6, meeting 4); Brazil (session 6, meeting 5); Ireland (session 6, meeting 5); Austria (session 6, meeting 5); Spain (session 6, meeting 5); Colombia on behalf of Australia, El Salvador, Estonia and Uruguay (session 7, meeting 5); European Union on behalf of 38 States (session 7, meeting 5); Netherlands (session 7, meeting 5); Switzerland (session 7, meeting 5); Belgium (session 7, meeting 5); Austria (session 7, meeting 5); Italy (session 7, meeting 5); Brazil (session 7, meeting 5); Japan (session 7, meeting 5); Mexico (session 7, meeting 5); United Kingdom (session 7, meeting 5); Ireland (session 7, meeting 5); Canada (session 7, meeting 6); Germany (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6).

90 For example, Thailand (session 6, meeting 5); Finland on behalf of the Nordic States (session 6, meeting 5); Nigeria (session 6, meeting 5); Kenya (session 6, meeting 5); Austria (session 6, meeting 5); Italy (session 6, meeting 5); Israel (session 6, meeting 5); United Kingdom (session 6, meeting 5); Australia (session 7, meeting 5); Colombia (session 7, meeting 6). See also A/79/214, paragraph 38(c).

91 For example, Ireland (session 6, meeting 5); Japan (session 6, meeting 5); Colombia (session 7, meeting 6).

92 For example, Switzerland (session 7, meeting 5); Italy (session 7, meeting 5); Brazil (session 7, meeting 5); Australia (session 7, meeting 5); France (session 7, meeting 6).

93 For example, Canada (session 6, meeting 4); European Union on behalf of 38 States (session 6, meeting 4); Switzerland (session 6, meeting 5); Kenya (session 6, meeting 5); Spain (session 6, meeting 5); Netherlands (session 6, meeting 5); France (session 7, meeting 6); United States (session 7, meeting 6).

94 For example, Uganda (session 6, meeting 6; session 7, meeting 5). Similarly, Chile (session 7, meeting 5).

95 For example, Finland on behalf of the Nordic States (session 6, meeting 5); Estonia (session 6, meeting 5); Netherlands (session 6, meeting 5); Pakistan (session 6, meeting 5); Malaysia (session 6, meeting 5); Uganda (session 6, meeting 6); Nigeria (session 7, meeting 5).

96 For example, Malaysia (session 7, meeting 5); Chile (session 7, meeting 5); Canada (session 7, meeting 6); Kenya (session 7, meeting 5); Mexico (session 6, meeting 5).

97 For example, Kenya (session 6, meeting 5); Germany (session 7, meeting 6).

2.4. Focusing on negotiation outcomes and looking towards the future Global Mechanism

The last cycle of negotiations reaffirmed once again the application of international law to State use of ICTs.

Many States stressed that international law – particularly the United Nations Charter, IHL, international human rights law (IHRL)[98] and, for some, also State responsibility[99] – is fully applicable to cyberspace. These States proposed that efforts should focus on interpreting and applying those existing rules and principles in cyberspace.[100]

Other States emphasized that there was a lack of consensus on topics such as attribution,[101] self-defence[102] and IHL,[103] and these should therefore be approached with caution. Many of these States restated their view that gaps exist in the current legal framework and called for focused discussions on the development of new legally binding obligations.[104] Some delegations indicated openness to discussing legally binding instruments as a future step.[105]

IHL was again one of the most discussed substantive topics on international law.[106] Several delegations proposed capturing in the outcome reports the progress that had been made in the discussions on IHL beyond the language agreed in previous processes.[107] Concrete proposals were put forward referencing the progress made at the 34th International Conference of the Red Cross and Red Crescent in 2024,[108] with some States suggesting incorporation of specific language from that conference's consensus resolution 341C/24/R2.[109] Conversely, as in previous cycles, a few delegations cautioned against including

98 For example, Brazil (session 10, meeting 4); Albania (session 10, meeting 4); North Macedonia (session 10, meeting 4); Netherlands (session 10, meeting 4); Germany (session 10, meeting 5); Malawi (session 10, meeting 4).

99 For example, Sweden (session 10, meeting 4); Australia (session 10, meeting 4); Canada (session 10, meeting 4); Japan (session 10, meeting 4); France (session 10, meeting 4); European Union (session 10, meeting 3; session 9, meeting 4).

100 For example, Sweden (session 10, meeting 4); Canada (session 10, meeting 3).

101 For example, Iran (Islamic Republic of) (session 10, meeting 4); Pakistan (session 10, meeting 4).

102 For example, Pakistan (session 10, meeting 4); Cuba on behalf of Venezuela, Nicaragua and Cuba (session 9, meeting 5).

103 For example, China (session 10, meeting 4); Cuba (session 10, meeting 4).

104 For example, Cuba (session 10, meeting 4); Iran (Islamic Republic of) (session 10, meeting 4); China (session 10, meeting 4); Russian Federation (session 10, meeting 3); Pakistan (session 10, meeting 4).

105 For example, Egypt (session 11, meeting 8); Indonesia (session 11, meeting 2).

106 See also in this regard, "Working Paper on the Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts", Update submitted by Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Senegal, Sweden and Switzerland, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations_Update_2025.pdf.

107 For example, Sweden (session 10, meeting 4); Colombia (session 10, meeting 4); Switzerland (session 10, meeting 4); Australia (session 10, meeting 4); Brazil (session 10, meeting 4); Senegal (session 10, meeting 4); United States (session 10, meeting 4).

108 For example, Sweden (session 10, meeting 4); El Salvador (session 10, meeting 4); France (session 10, meeting 4); Colombia (session 10, meeting 4); Switzerland (session 10, meeting 4); Australia (session 10, meeting 4); Egypt (session 10, meeting 5).

109 For example, Brazil (session 10, meeting 4); Canada (session 10, meeting 4); Netherlands (session 10, meeting 4); Ireland (session 10, meeting 5).

language on IHL in the final report. These States argued against the automatic application of IHL[110] and cited concerns that its application would promote the militarization of cyberspace and risk ICTs becoming a new battlefield.[111]

The prohibition of the use of force was also a topic that generated discussion. Some States advocated for specific language on the threshold for an ICT operation to constitute a use of force;[112] some other delegations were resistant to such language due to the existence of divergent views on the issue.[113] Another topic that gained prominence was IHRL, with several delegations sharing substantive views and arguing for stronger language to be reflected in the final report.[114]

The last cycle was also marked by deepening cross-regional articulation of developments in common understandings. This was reflected in the growing number of States supporting or co-sponsoring working papers on, for example, the application of IHL[115] or proposing text on areas of convergence.[116] Moreover, several statements were delivered on behalf of regional or subregional groups,[117] and a second regional position on the application of international law was published.[118]

A number of States drew attention to the multiple ongoing capacity-building efforts on international law. This included efforts to support the development of national positions,[119] which they considered had significantly contributed to increased participation in and substantive discussions at the OEWG.[120] Indeed, the main addition to the final report was a detailed list of capacity-building efforts and proposals[121] and calls for continued support to neutral and objective efforts, including within the United Nations, to build capacity on international law.[122]

---

110 For example, Venezuela (session 11, meeting 3).

111 For example, Cuba (session 10, meeting 4); China (session 10, meeting 4).

112 For example, Brazil (session 11, meeting 2); Netherlands (session 11, meeting 2); United Kingdom (session 11, meeting 2); Finland (session 11, meeting 2).

113 For example, Israel (session 11, meeting 3); Russian Federation (session 11, meeting 2).

114 For example, Thailand (session 10, meeting 4); Senegal (session 10, meeting 3); Mozambique (session 10, meeting 4); North Macedonia (session 10, meeting 4); Malawi (session 10, meeting 3); Switzerland (session 10, meeting 4); Australia (session 10, meeting 4); Ireland (session 10, meeting 5); Portugal (session 10, meeting 4).

115 "Working Paper on the Application of International Humanitarian Law", Update submitted by Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Senegal, Sweden and Switzerland.

116 "Working Paper on the Application of International Law in the Use of ICTs: Proposed Text Outlining Areas of Convergence for Inclusion in the 2025 Final Report International Law Section", submitted by Australia, Chile, Colombia, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Fiji, Germany, Ireland, Kiribati, Moldova, Netherlands, Papua New Guinea, Poland, Romania, Thailand, Uruguay, Vanuatu and Viet Nam, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_-_Cross-regional_Working_Paper_on_International_Law_-_11_July_2025.pdf.

117 For example, Nigeria on behalf of the African Group (session 9, meeting 4); Tonga on behalf of the Pacific Islands Forum (session 9, meeting 5; session 10, meeting 4); Tunisia on behalf of the Arab Group (session 11, meeting 6).

118 European Union, "Declaration on a Common Understanding of International Law in Cyberspace", 2024, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.

119 For example, Vanuatu (session 10, meeting 4); Mauritius (session 10, meeting 4); Australia (session 10, meeting 4); Estonia (session 11, meeting 3); Japan (session 11, meeting 3); Fiji (session 10, meeting 5).

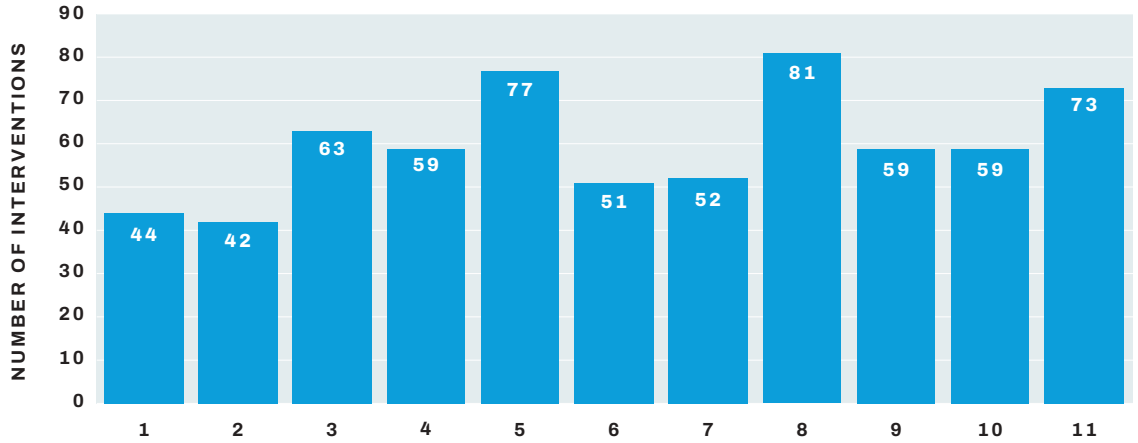
120 For example, Canada (session 10, meeting 4); Czechia (session 10, meeting 4).

121 A/80/257, paragraph 43(d).

122 A/80/257, paragraph 46.

FIGURE 1.

Number of States which participated in international law discussions



Although many delegations highlighted the success of the OEWG in advancing in-depth discussions and promoting additional layers of common understanding,[123] some States expressed views that this progress should have been more comprehensively and accurately documented in the final report.[124] The final report notes that States expressed diverse views on some of the issues, such as sovereignty, State responsibility, due diligence and IHL.[125]

Among the methodologies for addressing the practical application of international law that were discussed, scenario-based exercises again featured prominently. Many States suggested that they be incorporated into the modalities of the future permanent mechanism.[126] Involvement of legal experts continued to be a point of discussion. Many States supported expert input from relevant organizations and stakeholders,[127] while a few delegations considered that this should be approached cautiously. Those advocating a cautious approach cited, for example, concern about the burden that this may put on developing countries and stressed that these discussions are not only technical or legal in nature but also bear on States' political, economic and social considerations.[128]

123 For example, Canada (session 10, meeting 4); Thailand on behalf of Australia, Chile, Colombia, Dominican Republic, El Salvador, Estonia, Fiji, Kiribati, Moldova, Netherlands, Papua New Guinea, Thailand, Uruguay and Viet Nam (session 10, meeting 4).

124 For example, Canada (session 10, meeting 4); Brazil (session 10, meeting 4); Czechia (session 10, meeting 4); El Salvador (session 11, meeting 5); Switzerland (session 11, meeting 5); Viet Nam (session 11, meeting 5).

125 A/80/257, paragraph 42.

126 For example, Portugal (session 10, meeting 4); Thailand on behalf of Australia, Chile, Colombia, Dominican Republic, El Salvador, Estonia, Fiji, Kiribati, Moldova, Netherlands, Papua New Guinea, Thailand, Uruguay and Viet Nam (session 10, meeting 4); Canada (session 10, meeting 4); France (session 10, meeting 4); Philippines (session 9, meeting 5); Singapore (session 10, meeting 4).

127 For example, Netherlands (session 10, meeting 4); Brazil (session 10, meeting 4); Senegal (session 10, meeting 4); Sweden (session 10, meeting 4).

128 For example, China (session 10, meeting 4).

Participants attend 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.

As in previous cycles, some States brought up how the future permanent mechanism could incorporate international law through focused and structured discussions[129] and capacity-building.[130] The fourth cycle was thus very forward looking regarding the integration of international law into the future mechanism. In this regard, some States argued that international law was a cross-cutting issue that should be integrated across discussions.[131] Other delegations considered that international law merited its own dedicated thematic group[132] or platform for discussion.[133]

129 For example, Colombia on behalf of Australia, El Salvador, Estonia, Uruguay and Colombia (session 7, meeting 5).

130 For example, Uruguay (session 7, meeting 6). Some States directly related this to the so-called "Programme of Action". For example, Austria (session 4, meeting 4); Australia (session 4, meeting 5); Estonia (session 6, meeting 5); Italy (session 6, meeting 5); United Kingdom (session 3, meeting 8); European Union on behalf of 38 States (session 7, meeting 5); Japan (session 7, meeting 5); United Kingdom (session 7, meeting 5); Ireland (session 7, meeting 5); Canada (session 7, meeting 6); United States (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6); Kenya (session 10, meeting 5); Ghana (session 10, meeting 5); Malawi (session 9, meeting 4).

131 For example, Canada (session 10, meeting 4); France (session 10, meeting 4); United States (session 10, meeting 4).

132 For example, Russian Federation (session 10, meeting 4); Iran (Islamic Republic of) (session 10, meeting 4).

133 For example, Egypt (session 10, meeting 5; session 11, meeting 8); Tunisia on behalf of the Arab Group (session 11, meeting 6); Colombia (session 11, meeting 6); El Salvador (session 11, meeting 7). For more on the deliberation on the future mechanism see the chapter on regular institutional dialogue in this volume.

3. Trends and major themes addressed during the mandate

States' discussions under the international law agenda item ranged from conceptual debates on the sufficiency of existing international law to regulate State use of ICTs, via substantive topics regarding how international law applies to State use of ICTs, to practical considerations concerning how to progress discussions on international law in the OEWG 2021–2025. The following subsections cover, non-exhaustively, some of the key themes discussed during the OEWG under the international law agenda item.

3.1. The sufficiency of existing international law

Despite the standing consensus that existing international law, including the United Nations Charter, is applicable and essential for maintaining peace and stability in the ICT environment, divisions remained on whether existing rules of international law are entirely sufficient to govern State use of ICTs.

Over the course of the OEWG discussions, a large group of States maintained that the current corpus of international law – treaties, customary international law and general principles of international law – provides a comprehensive and robust framework for regulating State conduct in cyberspace.[134] Many of these States emphasized that international law is technology-neutral and thus automatically applies to the use of ICTs, although the nuances of precisely how it applies warranted further discussion.[135]

In contrast, a separate group of States contended that, due to the unique characteristics of the ICT environment, there is not necessarily an automatic application of existing international law and, to ensure global security, a new legally binding instrument is required.[136] The argument for a dedicated legal instrument was also put forward by a few States in the discussions under the agenda topic on rules, norms and principles.[137]

An overlapping feature of both views was the consideration and treatment of potential gaps. One group of States contended there were no gaps in the law itself, only gaps in understanding of how international law applies.[138] Another group of States argued that a legally binding instrument was the only way to fill the clear gaps left by existing international law.[139]

---

134 For example, Australia (session 4, meeting 5); Finland on behalf of the Nordic States (session 6, meeting 5); Japan (session 10, meeting 4).

135 For example, Finland on behalf of the Nordic States (session 6, meeting 5); Estonia (session 1, meeting 7).

136 For example, Russian Federation (session 7, meeting 5); Iran (Islamic Republic of) (session 10, meeting 4); Cuba also on behalf of Venezuela and Nicaragua (session 9, meeting 5); Pakistan (session 1, meeting 7); China (session 7, meeting 5).

137 See the chapter on rules, norms and principles in this volume.

138 For example, Canada (session 6, meeting 4); European Union (session 6, meeting 4); El Salvador (session 6, meeting 5); Mexico (session 7, meeting 5); Ireland (session 7, meeting 5).

139 For example, Russian Federation (session 7, meeting 5); Iran (Islamic Republic of) (session 10, meeting 4); Cuba also on behalf of Venezuela and Nicaragua (session 9, meeting 5); Pakistan (session 1, meeting 7); China (session 7, meeting 5).

Many of the latter States relatedly proposed the elaboration of a glossary with agreed terminology to facilitate understanding of discussions and provide consistency to terms used in consensus United Nations documents.[140] Several States, while affirming that existing international law applies to State use of ICTs, also remained open to studying potential gaps and did not rule out the future development of a legally binding instrument as common understandings evolved.[141]

3.2. Substantive topics of international law

Early convergences were established on a non-exhaustive list of topics that were proposed for further discussion, as reflected in the first APR.[142] This list guided the subsequent substantive discussions on how international law applies to State use of ICTs.

3.2.1. Rules and principles under the Charter of the United Nations

The application of specific rules and principles under the United Nations Charter emerged early on as an area of potential consensus.[143] States reaffirmed that "international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment".[144] Although only some specific sections of the Charter were explicitly referred to in the OEWG reports, some States emphasized their belief that the Charter is applicable in its entirety and a contrary intention should not be implied.[145] However, other delegations expressed reservations about the automatic applicability of the Charter as a whole.[146]

Over the course of the OEWG, a number of States emphasized the centrality of sovereignty within international law and the need to deepen discussions on the topic.[147] Discussions on sovereignty and sovereign equality evolved from initial mentions as part of a non-exhaustive list of topics,[148] to acknowledgement of them as general principles that apply to State use

---

140 For example, Russian Federation (session 1, meeting 6); Syria (session 2, meeting 6): Iran (session 4, meeting 5). On the glossary of terms, see also the chapter on confidence-building measures in this volume.

141 For example, Brazil (session 9, meeting 4); Indonesia (session 1, meeting 3); Thailand (session 10, meeting 4).

142 A/77/275, paragraph 15.

143 "Applicability of International Law, in Particular the United Nations Charter, in the Use of ICTs", Working paper submitted by Australia, Colombia, El Salvador, Estonia, and Uruguay, 24 July 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cyber_OEWG_-_International_Law_APR_paper_-_updated_-_24_July_2023.pdf.

144 A/77/275, paragraph 2; A/75/816, Annex I, paragraph 7.

145 For example, United Kingdom (session 4, meeting 4); Austria (session 4, meeting 4); Canada (session 4, meeting 4); South Africa (session 4, meeting 4); Switzerland (session 4, meeting 5); Australia (session 4, meeting 5); Germany (session 4, meeting 5); Japan (session 4, meeting 5); Croatia (session 4, meeting 5); Costa Rica (session 4, meeting 5); Belgium (session 4, meeting 5); Ireland (session 4, meeting 5); Viet Nam (session 4, meeting 5); Republic of Korea (session 4, meeting 5); Romania (session 4, meeting 6); Fiji (session 4, meeting 6); Brazil (session 5, meeting 3). In this regard, some States recalled the language included in the previous GGE outcome reports from 2015 (A/70/174, paragraph 28(c)) and 2021 (A/76/135, paragraph 71(e)) that "the Charter applies in its entirety".

146 For example, Iran (session 5, meeting 5); Cuba (session 5, meeting 4).

147 For example, China (session 1, meeting 7); India (session 1, meeting 7); Ukraine (session 6, meeting 6); Estonia (session 6, meeting 5); Thailand (session 6, meeting 5); Nigeria on behalf of the African Group (session 9, meeting 4); Switzerland (session 6, meeting 5).

148 A/77/275, paragraph 15(a).

of ICTs in the second APR,[149] and finally to a more comprehensive consensus that "State sovereignty and the international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory".[150]

Significant, detailed discussion evolved within the OEWG on the legal nature of sovereignty, revealing varying views. Some States put forward the view that sovereignty constitutes a stand-alone legally binding rule of international law applicable to State use of ICTs, the violation of which constitutes an internationally wrongful act.[151] However, this view did not garner consensus, with other States urging caution about using the OEWG to resolve the debate in its APRs.[152] Nevertheless, States were able to broadly agree that conduct using ICTs below the threshold of a threat or use of force may still be contrary to other principles of international law, such as State sovereignty or the principle of non-intervention.[153]

The application of peaceful settlement of disputes, and specifically the obligations under Articles 2(3) and 33(1) of the United Nations Charter, to the State use of ICTs garnered early agreement and the relevant agreed language remained essentially unchanged in subsequent consensus reports.[154] The obligation on States to settle their international disputes by peaceful means was considered to be essential to the maintenance of international security.[155] Some States advocated for the inclusion of additional detail in the report regarding the obligation to settle disputes peacefully, including a broader reference to Chapter 6 of the United Nations Charter.[156] In their discussions, some States noted that confidence-building measures (CBMs), such as the Global Intergovernmental Points of Contact (POC) Directory, can help reduce the risk of misunderstanding and escalation and thus serve as practical tools that support and complement the peaceful settlement of disputes.[157]

Following reaffirmation in the first APR of the principle of non-intervention and the prohibition on the threat or use of force, consensus language on these topics did not evolve significantly in subsequent reports. In discussions, States emphasized interference with electoral processes[158] and "election manipulation or destabilization of governmental institutions through cyber methods"[159] as examples of conduct that may violate the principle of non-intervention.

---

149 A/78/265, paragraph 30(a).

150 A/79/214, paragraph 37(a); A/80/257, paragraph 41(a). See also A/76/135, paragraph 71(b); General Assembly, resolution 76/19, 2021.

151 For example, Austria (session 4, meeting 4); Netherlands (session 4, meeting 5); Switzerland (session 4, meeting 5); Singapore (session 4, meeting 4); Estonia (session 4, meeting 5); Japan (session 4, meeting 5); France (session 4, meeting 5); Brazil (session 5, meeting 3); Thailand (session 6, meeting 5); South Africa (session 7, meeting 5); Italy (session 6, meeting 5); Viet Nam (session 5, meeting 3). See also Nigeria on behalf of the African Group (session 9, meeting 4).

152 For example, Israel (session 8, meeting 3).

153 A/80/257, paragraph 41(e).

154 A/78/265, paragraph 30(b); A/79/214, paragraph 37(b); A/80/257, paragraph 41(b).

155 For example, Singapore (session 4, meeting 4).

156 For example, Uruguay (session 5, meeting 3); European Union (session 5, meeting 3); United States (session 5, meeting 3); New Zealand (session 5, meeting 3); Switzerland (session 5, meeting 4).

157 For example, United Kingdom (session 4, meeting 4); Netherlands (session 4, meeting 5); Switzerland (session 4, meeting 5). On the POC Directory, see the chapter on confidence-building measures in this volume.

158 For example, Singapore (session 4, meeting 4); Estonia (session 4, meeting 5).

159 For example, Mexico (session 7, meeting 5). See similarly, Thailand (session 6, meeting 5).

One topic that did not achieve consensus was the right to self-defence under Article 51 of the United Nations Charter. In discussions, some States expressly emphasized a State's inherent right to self-defence in response to a cyber operation that amounts to an armed attack,[160] or an imminent threat thereof.[161] Another group of States urged that the "automatic" application of the right to self-defence to State use of ICTs be treated with extreme caution. They argued that there was a lack of consensus around whether a malicious use of ICTs could qualify as an armed attack, and that such considerations risked cyberspace becoming a theatre of military operations and escalation.[162]

3.2.2. International humanitarian law

One of the most contentious topics addressed by States throughout the sessions was the applicability of IHL to ICTs. While most States affirmed that IHL applies to the use of ICTs in situations of armed conflict,[163] some States continued to express significant reservations.[164] The latter group argued that recognizing the application of IHL in cyberspace could legitimize the use of ICTs for military purposes and contribute to the militarization of cyberspace.[165] Several States rebutted this argument, stating that it would not be aligned with the protective nature of IHL, which is aimed at limiting civilian harm in armed conflict,[166] rather than legitimizing conflict in any domain.[167]

Despite its divisive nature, IHL was one of the areas with the most in-depth legal discussion and debate during the OEWG. Several States called for focused discussions on IHL in order to protect civilians and civilian objects from ICT operations during armed conflict and emphasized the importance of the protection of critical infrastructure.[168]

---

160 For example, Austria (session 4, meeting 4); South Africa (session 4, meeting 4).

161 Singapore (session 4, meeting 4), available at **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/2023-03-07_OEWG_4SS_IL_Intervention_(SG).pdf**; New Zealand (session 4, meeting 5); Thailand (session 7, meeting 5).

162 For example, Cuba (session 1, meeting 7; session 4, meeting 5); Russian Federation (session 1, meeting 6); Syria (session 6, meeting 5).

163 For example, "Working Paper on the Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts", Update submitted by submitted by Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Senegal, Sweden and Switzerland, 9 July 2025, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations_Update_2025.pdf**. See also "Working Paper on the Application of International Law in the Use of ICTs", submitted by Australia, Chile, Colombia, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Fiji, Germany, Kiribati, Moldova, the Netherlands, Papua New Guinea, Poland, Romania, Thailand, Uruguay, Vanuatu and Viet Nam, 11 July 2025, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_-_Cross-regional_Working_Paper_on_International_Law_-_11_July_2025.pdf**. See also, for example, Fiji on behalf of the Pacific Islands Forum (session 11, meeting 2).

164 For example, Cuba (session 2, meeting 6); Nicaragua (session 3, meeting 3); Russian Federation (session 4, meeting 4): China (session 4, meeting 5).

165 Ibid.

166 For example, Estonia (session 1, meeting 7); Italy (session 1, meeting 7); France (session 1, meeting 7); European Union (session 2, meeting 6; session 7, meeting 5); Switzerland (session 4, meeting 5; session 10, meeting 4); Australia (session 6, meeting 5); Senegal on behalf of Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Sweden, Switzerland and Senegal (session 7, meeting 5); El Salvador (session 10, meeting 4); Brazil (session 10, meeting 4). This argument was also raised by the ICRC (e.g., session 10, meeting 4).

167 For example, Viet Nam (session 4, meeting 5); Fiji (session 4, meeting 6).

168 For example, Switzerland on behalf of Argentina, Brazil, Canada, Chile, Colombia, Czechia, Estonia, Germany,

In this context, some States also expressed concerns about the growing involvement of civilians in armed conflicts through means of ICTs.[169]

Groups of States developed and presented various language formulations on IHL through working papers and joint papers.[170] After the early discussions within the OEWG, States were unable to reach consensus on including IHL within the non-exhaustive list of topics for further discussion. Accordingly, IHL was mentioned only by quotation of the relevant recommendation in the 2021 GGE report.[171] Despite many language proposals on IHL, none made it into the second or third annual progress reports. However, in the final report, IHL was acknowledged as a topic on which States expressed views during the OEWG, without prejudice to their positions.[172]

3.2.3. State responsibility

State responsibility gained significant attention and discussion as a key topic. A number of States referred to existing customary international law (which is largely reflected in the ILC's Articles on Responsibility of States for Internationally Wrongful Acts)[173] as the basis for attributing acts to States and determining the responsibility of States and the consequences that flow from internationally wrongful acts.[174] In contrast, another group of States contended that accountability of States for violating international law in the use of ICTs can only be achieved through developing a universal legally binding treaty.[175]

As with the parallel discussions under the agenda topic on rules, norms and principles,[176] the issue of attribution remained divisive and generated a range of views from States. Some States argued that all accusations of unlawful activity must be substantiated,[177] and that, to prevent politicization, no attribution of responsibility to a State should be done without

---

Indonesia, Japan, Jordan, Mexico, Netherlands, Senegal, Sweden, Republic of Korea and Switzerland (session 3, meeting 3).

169 For example, Germany (session 6, meeting 5); Kiribati (session 6, meeting 5). This concern was also raised by the ICRC (e.g., session 6, meeting 6).

170 For example, "Working Paper on the Application of International Humanitarian Law", Update submitted by submitted by Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Senegal, Sweden and Switzerland, 9 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations_Update_2025.pdf; "Working Paper on the Application of International Law in the Use of ICTs", submitted by Australia, Chile, Colombia, the Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Fiji, Germany, Ireland, Kiribati, Moldova, the Netherlands, Papua New Guinea, Poland, Romania, Thailand, Uruguay, Vanuatu, and Viet Nam, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_-_Cross-regional_Working_Paper_on_International_Law_-_11_July_2025.pdf.

171 A/77/275, paragraph 15(b)(ii).

172 A/80/257, paragraph 42.

173 International Law Commission, "Responsibility of States for Internationally Wrongful Acts", Draft Articles, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

174 For example, Australia (session 1, meeting 7; session 6, meeting 5); European Union (session 9, meeting 4); Thailand (session 6, meeting 5); Singapore (session 6, meeting 5).

175 For example, Russian Federation (session 6, meeting 5); Iran (session 9, meeting 5).

176 On discussions on the voluntary normative framework pertaining to non-escalatory attribution, see the chapter on rules, norms and principles in this volume.

177 For example, Russian Federation (session 2, meeting 6). See also related statement delivered during the agenda item of rules, norms and principles: Russian Federation (session 2, meeting 5).

technical evidence.[178] Other States noted that there is no international legal obligation for a State to publicly share the evidence or technical data upon which an attribution decision is based.[179] Nevertheless, it was acknowledged that it was in a State's best interest to be careful when making attributions.[180] Indeed, some noted that a sufficient level of confidence is needed to attribute a wrongful act to a State and that such attributions should be substantiated.[181] Some States expressed views on how to address perceived challenges associated with attribution, including the possibility of additional legally binding obligations;[182] the proposal of a dedicated multilateral attribution mechanism;[183] and capacity-building for States that lack the technical capability to objectively identify perpetrators.[184]

Further, some States were keen to discuss lawful responses under international law, including some delegations that highlighted countermeasures as an area that requires further analysis.[185] A more cautious view was also expressed, suggesting that discussions on countermeasures might be premature given the unresolved issues surrounding attribution and State responsibility, which underpin the use of countermeasures.[186]

3.2.4. Due diligence

Although minimal language on due diligence was included in the reports,[187] many States emphasized the importance of States not knowingly allowing their territory to be used for acts that are harmful to third States. While there were substantive discussions, States were unable to achieve consensus on key aspects of due diligence, including its precise parameters or whether it constitutes a legally binding obligation.

In advocating for further discussion on due diligence under the international law pillar,[188] some States presented the view that due diligence is an obligation[189] tied to the capabilities of the State.[190] An alternative view was that due diligence should be considered within the discussions on the voluntary non-binding norms.[191] In this context, norm C provides that

---

178 For example, Iran (session 9, meeting 4); Russian Federation (session 4, meeting 4).

179 For example, Australia (session 2, meeting 6); Denmark (session 6, meeting 5); France (session 4, meeting 5).

180 For example, Australia (session 2, meeting 6).

181 For example, Germany (session 1, meeting 7).

182 For example, Iran (session 9, meeting 4); Russian Federation (session 4, meeting 4).

183 For example, Cuba (session 4, meeting 5); Nicaragua (session 4, meeting 6). In this regard see also the chapter on existing and potential threats in this volume.

184 For example, Thailand (session 4, meeting 5); Kenya (session 7, meeting 5).

185 For example, Israel (session 1, meeting 6); Philippines (session 1, meeting 6); Switzerland (session 2, meeting 4); Malawi (session 4, meeting 5); Senegal (session 7, meeting 5).

186 For example, China (session 1, meeting 7).

187 Due diligence appeared in the APRs and the final report only within the non-exhaustive list of topics, and in the final report in a broad sentence noting, without prejudice to States' positions, that deepening discussions were held on the topic (among others). See A/80/257, paragraph 42.

188 For example, European Union on behalf of 38 States (session 7, meeting 5); Thailand (session 5, meeting 3); Egypt (session 9, meeting 4).

189 For example, France (session 4, meeting 5); Thailand (session 6, meeting 5); Denmark (session 6, meeting 5); Japan (session 2, meeting 6); Czechia (session 7, meeting 6).

190 For example, Thailand (session 7, meeting 5); Egypt (session 9, meeting 4).

191 For example, United Kingdom (session 3, meeting 5).

States should not knowingly allow their territory to be used for internationally wrongful acts against other States.[192]

3.2.5. International human rights law

Human rights was another topic featured in discussions.[193] A broad cross-regional group of States consistently reaffirmed that IHRL applies in its entirety to State use of ICTs and sought to promote emerging convergence.[194] States frequently highlighted the rights to privacy, freedom of expression, freedom of association and non-discrimination as being of particular relevance in the digital realm.

Despite agreement among most States, some delegations opposed the inclusion of concrete language on human rights on the basis that it should be discussed in other United Nations forums.[195]

3.3. Methodologies for progressing international law discussions in the OEWG

Over the course of the OEWG, discussions moved from general affirmations of the application of international law in cyberspace to a focus on practical, action-oriented and detailed methodologies for progressing discussions on international law within the OEWG.

To advance common understandings on substantive areas of international law, many States favoured focused discussions on a cluster of priority topics, rather than general exchanges.[196] Recognizing the complexity of the topic, a number of States advocated for more time to be available for international law discussions,[197] including through additional intersessional meetings on specific topics.[198]

---

192 A/70/174, paragraph 13(c); A/76/135, paragraphs 29–30; A/80/257, paragraph 34(a). See also the chapter on rules, norms and principles in this volume.

193 For example, New Zealand (session 4, meeting 5); Ireland (session 4, meeting 5); Fiji (session 4, meeting 6); Germany (session 5, meeting 3); Mexico (session 5, meeting 3); Costa Rica (session 5, meeting 3); United States (session 5, meeting 3); Latvia (session 5, meeting 3); Colombia (session 5, meeting 3); Greece (session 5, meeting 4); Czechia (session 5, meeting 3).

194 "Working Paper on the Application of International Law in the Use of ICTs", submitted by Australia, Chile, Colombia, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Fiji, Germany, Kiribati, Moldova, the Netherlands, Papua New Guinea, Poland, Romania, Thailand, Uruguay, Vanuatu and Viet Nam, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_-_Cross-regional_Working_Paper_on_International_Law_-_11_July_2025.pdf. See also Finland on behalf of the Nordic States (session 6, meeting 5); Statements on behalf of the Pacific Islands Forum delivered by, for example, Tonga (session 10, meeting 4) and Fiji (session 11, meeting 2).

195 For example, Sudan (session 5, meeting 4); Iran on behalf of Burundi, Belarus, China, Cuba, Democratic People's Republic of Korea, Nicaragua, Russia, Syria, Venezuela and Iran (session 5, meeting 4).

196 For example, Chair's initiation of a first cluster of topics (session 4, meeting 4); Canada (session 4, meeting 4).

197 For example, Austria (session 4, meeting 4); European Union (session 4, meeting 4); Viet Nam (session 4, meeting 5); Malawi (session 4, meeting 5); Fiji (session 4, meeting 6).

198 A/78/265, paragraph 35.

Calls for the involvement of international legal experts to provide briefings or share relevant studies and opinions also gained widening support. While a few States considered that references should be kept broad,[199] specific suggestions included the ILC,[200] the International Committee of the Red Cross (ICRC),[201] academia,[202] think tanks[203] and civil society.[204] However, it was also argued that legal experts should not be invited to brief the OEWG as it would invoke more technical discussions and thus increase the burden on delegates, especially those from developing countries.[205] An initial broad reference in the second APR[206] to the possibility of expert briefings was later expanded in the third APR to include suggestions that such briefings could be provided by "the ILC or academia as appropriate, with due consideration given to equitable geographical representation and national contexts".[207]

Many States advocated for workshops[208] and scenario-based exercises[209] as a key methodological approach with multiple purposes, including facilitating exchange of views;[210] promoting transparency and confidence-building;[211] and building common understandings on the application of international law to State use of ICTs.[212] Other States also saw value in scenario-based exercises for identifying potential gaps[213] and supporting the need to develop a legally binding instrument.[214] The scenario-based workshop held by UNIDIR in November 2023 was cited as a successful example.[215]

---

199 For example, Czechia (session 3, meeting 4); Israel (session 3, meeting 4).

200 For example, South Africa (session 2, meeting 6; session 7, meeting 5); Jordan (session 4, meeting 6); Viet Nam (session 4, meeting 5); Brazil (session 3, meeting 4); Argentina (session 5, meeting 3).

201 For example, Switzerland (session 3, meeting 3); Republic of Korea (session 3, meeting 3); Austria (session 3, meeting 5); Costa Rica (session 3, meeting 4).

202 For example, Belgium (session 8, meeting 2); United States (session 8, meeting 2); Estonia (session 6, meeting 5).

203 For example, United States (session 8, meeting 2).

204 For example, Estonia (session 6, meeting 5).

205 For example, China (session 8, meeting 3).

206 A/78/265, paragraph 35.

207 A/79/214, paragraph 38(a); A/80/257, paragraph 43(a).

208 For example, Estonia (session 1, meeting 7); Chile (session 2, meeting 6).

209 For example, Singapore (session 10, meeting 4); United Kingdom (session 6, meeting 5); Switzerland (session 7, meeting 5); Australia (session 7, meeting 5); United States (session 7, meeting 6); Malawi (session 7, meeting 6); Colombia on behalf of Australia, El Salvador, Estonia, Uruguay and Colombia (session 7, meeting 5).

210 For example, Republic of Korea (session 7, meeting 5); Colombia on behalf of Australia, El Salvador, Estonia, Uruguay and Colombia (session 7, meeting 5); El Salvador (session 7, meeting 5); Switzerland (session 7, meeting 5); Belgium (session 7, meeting 5); Austria (session 7, meeting 5); Japan (session 7, meeting 5); United Kingdom (session 7, meeting 5); Malaysia (session 7, meeting 5); Singapore (session 7, meeting 5); Canada (session 7, meeting 6); Germany (session 7, meeting 6); United States (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6); Israel (session 7, meeting 6); Malawi (session 7, meeting 6).

211 For example, Colombia (session 7, meeting 6).

212 For example, Germany (session 6, meeting 5); France (session 6, meeting 5); Australia (session 6, meeting 5); Switzerland (session 6, meeting 5); United States (session 6, meeting 5).

213 For example, Bangladesh (session 7, meeting 5).

214 For example, Iran (session 7, meeting 5); Russian Federation (session 7, meeting 5).

215 Examples of States welcoming the initiative include Canada (session 6, meeting 4); European Union on behalf of 37 States (session 6, meeting 4); Mexico (session 6, meeting 5); Brazil (session 6, meeting 5); Switzerland (session 6, meeting 5); Italy (session 6, meeting 5); Republic of Korea (session 6, meeting 5); Netherlands (session 6, meeting 5); United States (session 6, meeting 5); Germany (session 6, meeting 5); United Kingdom (session 6, meeting 5); France (session 6, meeting 5); Japan (session 6, meeting 5); Czechia (session 6, meeting 5); China (session 6, meeting 5); Australia (session 6, meeting 5); Colombia on behalf of

3.4. Voluntary sharing of national and regional positions

Throughout the OEWG process, States welcomed and encouraged the development and publication of national positions on how international law applies in State use of ICTs. These positions were recognized as key contributions to the development of the debate and reaching common understandings;[216] to ensuring transparency, predictability and stability in cyberspace;[217] and to both confidence-building[218] and capacity-building.[219] This was consistently reflected in the APRs and the final report of the OEWG.[220]

At the commencement of the OEWG in December 2021, 23 States had published national positions, many of which appeared in the official compendium of voluntary national contributions issued as part of the outcome of the 2021 GGE process.[221] Over the course of the OEWG 2021–2025, an additional 12 States published national positions,[222] with some further States issuing updated or complementary national positions.[223] Several other States publicly announced that they were working on developing a national position.[224] Furthermore, two

---

Australia, El Salvador, Estonia, Uruguay and Colombia (session 7, meeting 5); Uruguay (session 7, meeting 6). The UNIDIR event was supported by the governments of China, Czechia, France, Germany, the Netherlands, the Russian Federation, Switzerland and the United Kingdom. For a summary of the workshop, see UNIDIR Security and Technology Programme, "International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities", Workshop Summary Report, n.d., https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNIDIR_International_Law_and_the_Behaviour_of_States_in_the_Use_of_ICT.pdf.

216 For example, Canada (session 6, meeting 4; session 7, meeting 6); European Union on behalf of 37 States (session 6, meeting 4); Brazil (session 6, meeting 5; session 7, meeting 5); Ireland (session 6, meeting 5); Austria (session 6, meeting 5; session 7, meeting 5); Spain (session 6, meeting 5); Colombia on behalf of Australia, El Salvador, Estonia, Uruguay and Colombia (session 7, meeting 5); European Union on behalf of 38 States (session 7, meeting 5); Netherlands (session 7, meeting 5); Switzerland (session 7, meeting 5); Belgium (session 7, meeting 5) ; Italy (session 7, meeting 5); Japan (session 7, meeting 5); Mexico (session 7, meeting 5); United Kingdom (session 7, meeting 5); Ireland (session 7, meeting 5); Germany (session 7, meeting 6); Czechia (session 7, meeting 6); France (session 7, meeting 6).

217 For example, European Union (session 1, meeting 6; session 2, meeting 6; session 4, meeting 4); Ireland (session 1, meeting 6; session 2, meeting 6); Israel (session 1, meeting 6); United Kingdom (session 1, meeting 6; session 2, meeting 6); Japan (session 1, meeting 6; session 2, meeting 6); Switzerland (session 1, meeting 6; session 2, meeting 6); Netherlands (session 1, meeting 6); Republic of Korea (session 1, meeting 7); India (session 1, meeting 7); Australia (session 1, meeting 7; session 2, meeting 6; session 4, meeting 5); Estonia (session 1, meeting 7; session 2, meeting 6); Italy (session 1, meeting 7); Brazil (session 1, meeting 7); France (session 1, meeting 7; session 2, meeting 6); Costa Rica (session 1, meeting 7; session 2, meeting 6); Sweden (session 2, meeting 6); Canada (session 2, meeting 6); United States (session 2, meeting 6); Singapore (session 2, meeting 6); New Zealand (session 2, meeting 6); Germany (session 2, meeting 6); Botswana (session 2, meeting 6); Czechia (session 4, meeting 5).

218 For example, Costa Rica (session 1, meeting 7); United States (session 4, meeting 5); Kenya (session 6, meeting 5).

219 For example, United States (session 2, meeting 6); Sweden on behalf of the Nordic States (session 4, meeting 4); Japan (session 4, meeting 5).

220 A/77/275, paragraph 15(c); A/78/265, paragraph 34; A/79/214, paragraph 40; A/80/257, paragraph 45.

221 The compendium A/76/136 contains the national positions of 15 States: Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, Netherlands, Norway, Romania, the Russian Federation, Singapore, Switzerland, the United Kingdom and the United States, with some of them being the second or third iteration. An additional 8 States – China, Czechia, Finland, France, the Islamic Republic of Iran, Israel, Italy and New Zealand – had also published their national positions at the time of commencement of the work of the OEWG 2021–2025. See the UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/.

222 These 12 States are Austria, Canada, Colombia, Costa Rica, Cuba, Denmark, Ireland, the Republic of Korea, Pakistan, Poland, Sweden and Thailand. In addition, Belgium and Slovenia published their national positions after the conclusion of the OEWG 2021–2025.

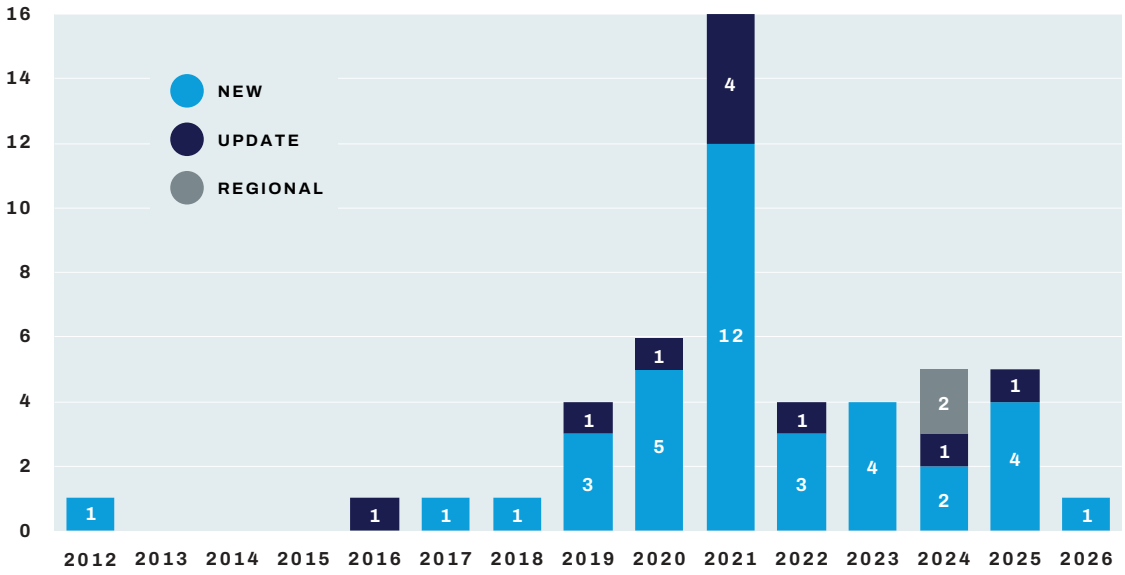
223 Czechia, New Zealand and the United Kingdom all issued updated national positions. China issued additional views on the application of sovereignty in cyberspace.

224 For example, Botswana (session 2, meeting 6); Spain (session 6, meeting 5); Mauritius (session 10,

regional organizations developed common regional views on the application of international law in cyberspace: the African Union[225] and the European Union.[226]

FIGURE 2.

National and regional positions on international law in cyberspace by year



During the discussions, several delegations reiterated the need to keep repositories of national views,[227] including using existing tools (e.g., the UNIDIR Cyber Policy Portal and the OEWG website),[228] to enhance transparency[229] and to provide a foundation for identifying convergencies and divergencies.[230]

Other efforts at the regional level were shared during the discussion, such as the work of the Inter-American Juridical Committee of the Organization of American States (OAS) on enhancing transparency that culminated in 2022.[231]

---

meeting 4); Vanuatu (session 10, meeting 4); Fiji (session 10, meeting 5); Senegal (session 10, meeting 4); Malawi (session 11, meeting 3).

225 African Union Common Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace.

226 European Union, "Declaration on a Common Understanding of International Law in Cyberspace".

227 For example, Bangladesh (session 6, meeting 5); Kenya (session 4, meeting 4); Costa Rica (session 2, meeting 6).

228 For example, Costa Rica (session 2, meeting 6); Colombia (session 2, meeting 6).

229 For example, United Kingdom (session 1, meeting 6); Germany (session 1, meeting 7); Estonia (session 1, meeting 7); Thailand (session 3, meeting 5); Brazil (session 2, meeting 6); Republic of Korea (session 1, meeting 7); Fiji (session 2, meeting 6); Malawi (session 2, meeting 6); Uruguay (session 2, meeting 6); Costa Rica (session 2, meeting 6).

230 For example, Austria (session 1, meeting 6); Japan (session 1, meeting 6); Kenya (session 4, meeting 4).

231 For example, Peru (session 9, meeting 5). See also intervention by the Organization of American States (session 6, meeting 6). See further Organization of American States, Inter-American Juridical Committee, "International Law and State Cyber Operations", n.d., https://www.oas.org/en/sla/iajc/themes_recently_concluded_International_law_State_cyber_operations.asp.

3.5. Capacity-building

Building capacity on how international law applies to State use of ICTs gained increasing prominence over the course of the OEWG. It was one of the areas that found more convergence and, as a result, was better reflected in the outcome documents of the OEWG 2021–2025.[232] A number of States emphasized that international law capacity building is essential for meaningful participation in the multilateral discussions,[233] particularly for developing States, and to allow all States to participate in these discussions on an equal footing.[234] The final report reflected the role of capacity-building in ensuring equal and meaningful participation of States in discussions on international law and the development of common understandings.[235]

The exchange of good practices and experiences[236] and targeted initiatives to develop national and regional[237] positions were both highlighted as essential aspects of capacity-building.[238] Many States also emphasized that capacity-building should be neutral, objective and tailored to help States acquire the expertise needed to develop their own independent views on the application of international law to the use of ICTs.[239]

Many States highlighted the work of different stakeholders in supporting capacity-building and the development of relevant tools. They also highlighted the initiatives conducted by relevant organizations, including the United Nations[240] and at the regional and subregional levels.[241]

Throughout the OEWG, most States consistently linked the need for capacity-building in international law with specific methodological approaches designed to move discussions from abstract political statements to practical legal application.[242] The final report reflected some of the specific modalities that were advanced by States, including workshops, conferences, exchanges of best practice and online resources.[243] However, a few States noted the lack of reference to scenario-based exercises, despite it being one of the most frequently promoted methodologies.[244]

---

232 **A/80/257**, paragraph 43(d).

233 For example, Malaysia (session 6, meeting 5); Mexico (session 10, meeting 4); Singapore (session 11, meeting 3); Moldova (session 10, meeting 5); Canada (session 6, meeting 4).

234 For example, Singapore (session 11, meeting 3); Finland on behalf of the Nordic States (session 6, meeting 5); Netherlands (session 6, meeting 5); Pakistan (session 6, meeting 5); Malaysia (session 6, meeting 5); Uganda (session 6, meeting 6); Nigeria (session 7, meeting 5).

235 For example, Fiji on behalf of the Pacific Islands Forum (session 11, meeting 2).

236 For example, Canada (session 4, meeting 4); Germany (session 4, meeting 5); Japan (session 4, meeting 5).

237 For example, Kenya (session 6, meeting 5); Senegal (session 7, meeting 5).

238 For example, European Union (session 6, meeting 4); Switzerland (session 6, meeting 5); Kenya (session 6, meeting 5); Brazil (session 7, meeting 5).

239 For example, Kenya (session 6, meeting 5); European Union (session 6, meeting 4).

240 For example, Canada (session 4, meeting 4); Netherlands (session 4, meeting 5); Switzerland (session 4, meeting 5); Colombia (session 4, meeting 6); Brazil (session 7, meeting 5); Australia (session 7, meeting 5).

241 For example, Colombia (session 4, meeting 6); India (session 4, meeting 5); Chile (session 4, meeting 5); Malaysia (session 4, meeting 6); Mexico (session 6, meeting 5); Canada (session 6, meeting 4); Kenya (session 7, meeting 5).

242 On scenario-based exercises and the involvement of international legal experts, see Subsection 3.3 above.

243 For example, Ghana (session 11, meeting 2); Tonga on behalf of the Pacific Islands Forum (session 10, meeting 4); Indonesia (session 9, meeting 5).

244 For example, Ghana (session 11, meeting 6); Netherlands (session 11, meeting 2).

4. Insights beyond the official outcomes

Discussions on the scope and application of international law in cyberspace were one of the most difficult and contentious issues throughout the OEWG 2021–2025. While the APRs and final report show very little consensus on how international law applies, a key aspect that stands out through analysis is that international law discussions moved beyond an exploratory stage and matured significantly over the four years of the OEWG. There are three clear indicators of this.

First, there was a significant increase in the number of States taking the floor during the international law agenda topic of the OEWG sessions. Second, the substantive contributions of States on the application of international law to State use of ICTs deepened over the four cycles.[245] Over the course of the OEWG, States' substantive interventions evolved beyond the reaffirmation of agreed language to offering detailed and practical contributions to the study of this topic. Third, there was a significant increase in the publication of national and regional positions, which is likely to have bolstered the two previous points.[246] Moreover, areas of convergence became increasingly visible, reflected in the rise of regional, subregional and cross-regional papers and joint statements.

Although the final report noted that different views were expressed on a number of topics,[247] many of the substantive discussions were not reflected or elaborated on in the report's text. This limited reflection of certain discussions was highlighted by several delegations during the 11th session of the OEWG when negotiating the text of the final report.[248] Some of these included deeply discussed substantive topics such as IHL,[249] IHRL[250] and State responsibility.[251] The lack of agreed language on these topics in the outcome reports reflects the ongoing divergences in States' positions. Some delegations also pointed out that the final report should have reflected the discussion on the potential development of a legally binding instrument and concrete proposals submitted in this regard.[252]

---

245 For example, Thailand (session 11, meeting 3); Morocco (session 11, meeting 7); Estonia (session 11, meeting 7).

246 For example, European Union (session 11, meeting 2) stressing that "over a hundred member States have now individually or collectively published their position and views on the application of international law".

247 A/80/257, paragraph 42.

248 For example, European Union (session 11, meeting 7); Brazil (session 11, meeting 7); Australia (session 11, meetings 7–8); New Zealand (session 11, meeting 7).

249 For example, Costa Rica (session 11, meeting 7); Chile (session 11, meeting 7); Republic of Korea (session 11, meeting 2); Australia (session 11, meeting 7; meeting 8); Fiji on behalf of the Pacific Islands Forum (session 11, meeting 2).

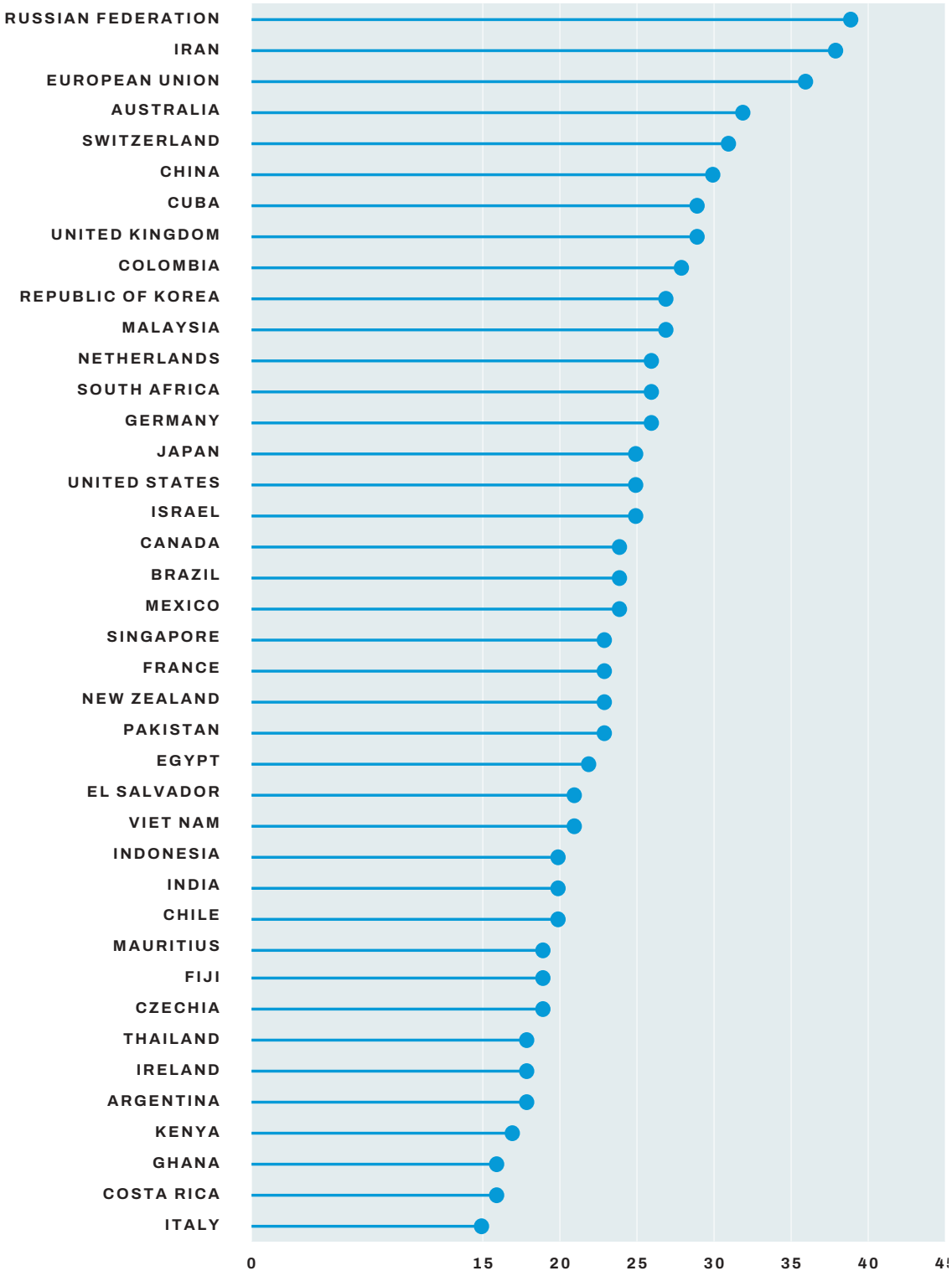
250 For example, Costa Rica (session 11, meeting 7); Ireland (session 11, meeting 8); Fiji on behalf of the Pacific Islands Forum (session 11, meeting 2); Australia (session 11, meetings 7–8).

251 For example, Viet Nam (session 11, meeting 2); Australia (session 11, meetings 7–8); Fiji on behalf of the Pacific Islands Forum (session 11, meeting 2).

252 For example, Iran (session 11, meeting 2); Russian Federation (session 11, meeting 2).

FIGURE 3.

Number of times delegations took the floor on international law in the OEWG 2021–2025[253]



253 This chart shows the delegations that took the floor at least 15 times during the sessions. The full list of interventions is provided in Annex A.

The final report reflects the complexity of reconciling the divergent approaches to international law, specifically whether discussions should focus on the application of existing international law or on identifying and addressing gaps in existing international law through the development of new legally binding rules. A few delegations pointed out that these two perspectives were not necessarily contradictory or mutually exclusive.[254] The final report also illustrates the challenge of accommodating a plurality of legal interpretations on a variety of topics and of capturing the nuance of those discussions and representing all views fairly. As a result, the outcome remained relatively modest, relying largely on previously agreed language from earlier processes or on formulations drawn directly from the United Nations Charter, without elaborating on specific interpretations.

One thing is clear: the long-standing affirmation by States that international law, including the United Nations Charter, applies to State use of ICTs remains unchallenged, and the OEWG generated a large base of substantive contributions on how international law applies to State use of ICTs. At the same time, the analysis here highlights the challenges that States faced in reaching agreement on outcomes that fully captured the depth and complexity of the discussions across the sessions. Nevertheless, matters that were less contentious – such as the strong encouragement to continue sharing national positions and the importance of capacity-building in international law – were better captured in the outcome reports. These efforts have been framed as key enablers for building common understandings and can serve as the foundation for continued discussions in the Global Mechanism.

To continue the discussions on how international law applies to State use of ICTs, bearing in mind the plurality of views evidenced in the OEWG, the Global Mechanism can rely on the different methodologies already discussed by States. These methodologies include continuing focused discussions anchored in practical approaches (such as scenario-based exercises); continuing to voluntarily share national and regional views on how international law applies; supporting neutral and objective capacity-building efforts; and leveraging inputs from experts and relevant organizations to equip all States to contribute to build common understanding.[255]

254 For example, Egypt (session 11, meeting 3); Malawi (session 11, meeting 7).

255 Compare with **A/80/257**, paragraph 46.

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

STATE	COUNT	STATE	COUNT
Russian Federation	39	India	20
Iran (Islamic Republic of)	38	Chile	20
European Union	36	Mauritius	19
Australia	32	Fiji	19
Switzerland	31	Czechia	19
China	30	Thailand	18
Cuba	29	Ireland	18
United Kingdom	29	Argentina	18
Colombia	28	Kenya	17
Republic of Korea	27	Ghana	16
Malaysia	27	Costa Rica	16
Netherlands (Kingdom of the)	26	Italy	15
South Africa	26	Nicaragua	13
Germany	26	Austria	13
Japan	25	Estonia	13
United States	25	Uruguay	13
Israel	25	Philippines	13
Canada	24	Syria	13
Brazil	24	Bangladesh	13
Mexico	24	Nigeria	12
Singapore	23	Portugal	11
France	23	Vanuatu	11
New Zealand	23	Albania	10
Pakistan	23	Malawi	10
Egypt	22	Poland	9
El Salvador	21	Dominican Republic	9
Viet Nam	21	Iraq	9
Indonesia	20	Kazakhstan	8

STATE	COUNT	STATE	COUNT
Croatia	8	Sierra Leone	3
Belgium	8	Tunisia	3
Finland	7	Guatemala	3
Ukraine	7	Lebanon	3
Venezuela	7	Djibouti	2
Ecuador	7	Kuwait	2
Mozambique	6	Bosnia and Herzegovina	2
Saudi Arabia	6	Republic of Moldova	2
Tonga	6	Ethiopia	2
Sweden	6	Cameroon	2
Belarus	6	Zimbabwe	2
Greece	6	Morocco	2
Jordan	6	Denmark	2
Lao PDR	5	Kiribati	2
Paraguay	5	Sudan	2
Latvia	5	Antigua and Barbuda	2
Botswana	5	Türkiye	1
Slovakia	5	Serbia	1
Senegal	4	Cambodia	1
Algeria	4	Brunei Darussalam	1
North Macedonia	4	Timor-Leste	1
Papua New Guinea	4	Jamaica	1
Burkina Faso	4	Libya	1
Romania	4	Honduras	1
Peru	4	North Korea	1
Uganda	4	Georgia	1
Spain	4	Armenia	1
Hungary	4	Qatar	1
Sri Lanka	4	Mali	1
Democratic Republic of the Congo	3	Benin	1
Côte d'Ivoire	3		

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).

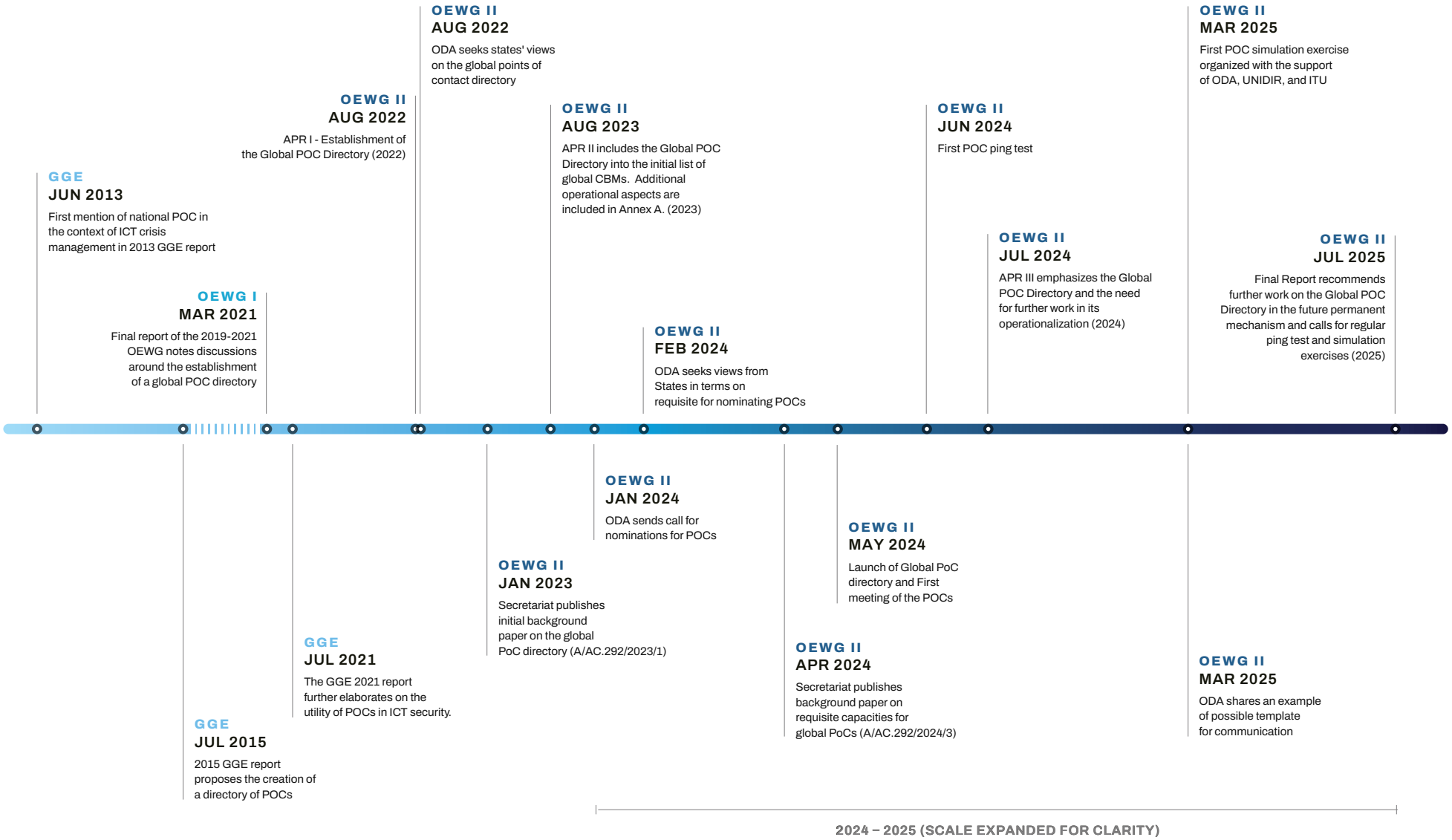
33 For example, Russian Federation (session 6, meeting 6); Thailand (session 8, meeting 3); European Union (session 8, meeting 4); United Kingdom (session 8, meeting 3); New Zealand (session 8, meeting 3).

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).

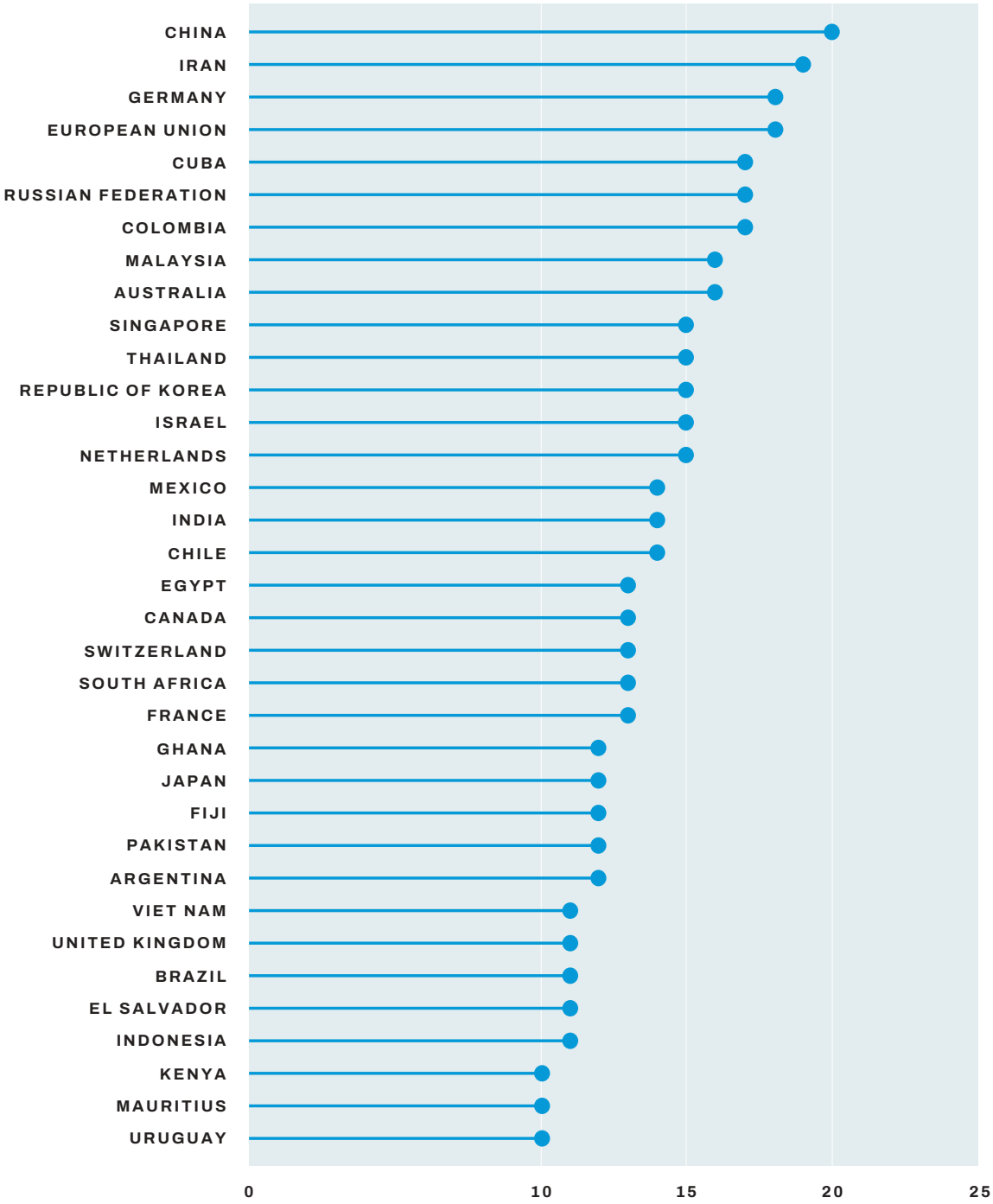
43 For example, United States (session 11, meeting 3); United Kingdom (session 11, meeting 5); Netherlands (session 11, meeting 5).

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.

Ambassador 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.

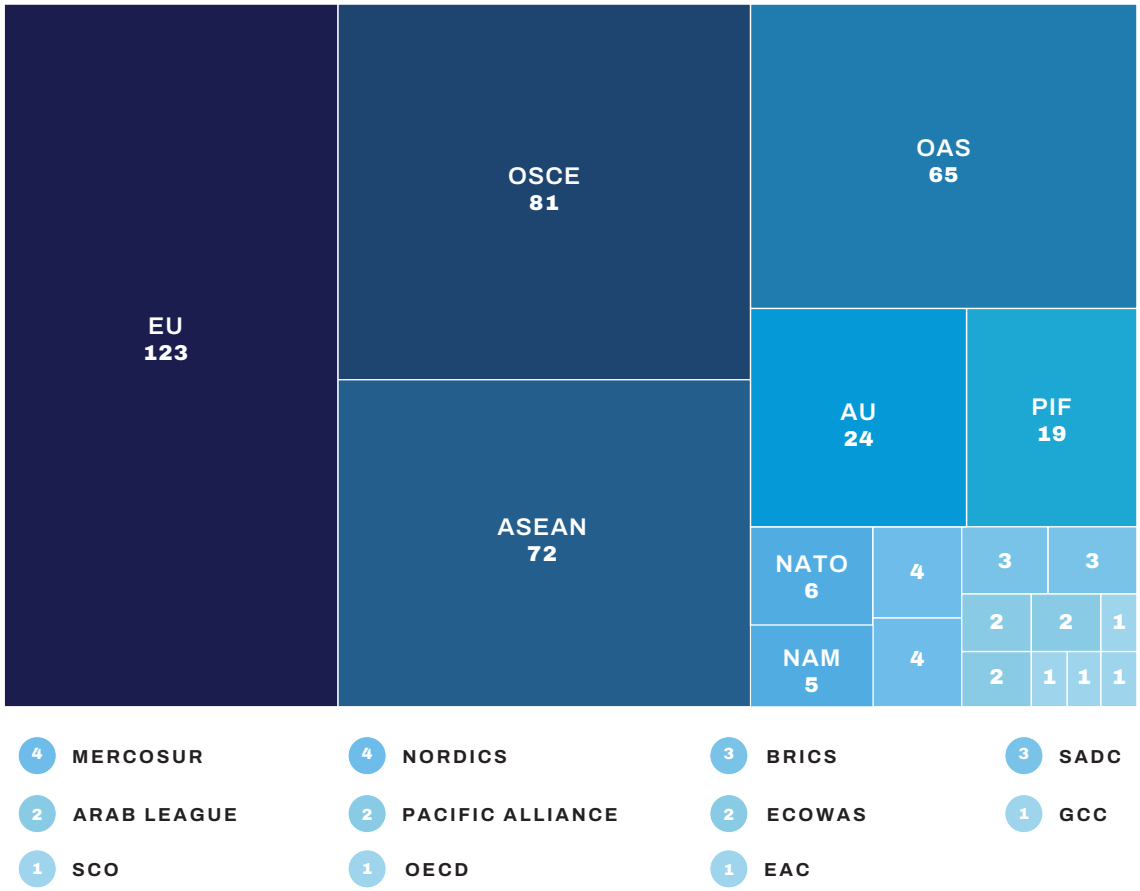
45 For example, United States (session 2, meeting 7; session 3, meeting 4); China (session 3, meeting 3).

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

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.[1] 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.[2] 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.[3] 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.[4] 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".[5]

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.[6] It underscored the voluntary, politically neutral, mutually beneficial and reciprocal nature of CB,[7] and it encouraged States to adopt a multidisciplinary, multi-stakeholder, modular and measurable approach to cooperation with the United Nations and regional bodies.[8]

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.[9] 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.[10]

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,[11] 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".[12]

Second, some States identified priority areas for capacity-building: development of national cybersecurity strategies; establishment of computer security incident response teams (CSIRTs);[13] protection of critical infrastructure;[14] and enhancement of incident response capabilities.[15] 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",[16] while detailing bilateral partnerships and ongoing negotiations between states' cybersecurity agencies.[17] 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.[18]

---

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.[19]

Finally, several delegations highlighted gender perspectives as a cross-cutting concern.[20]

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.[21] 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).[22] 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.[23]

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.[24] 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.[25] 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,[26] and States broadly supported development of tools for incorporating gender dimensions into CB strategies.[27]

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.[28] In contrast, the proposal for a centralized "global cybersecurity cooperation portal" as a coordination hub[29] drew differing views on its scope.[30] 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[31] – 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.[32] 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.[33] 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.[34]

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.[35] 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,[36] and broader United Nations coordination functions to take stock of needs, identify gaps through tools and surveys, and facilitate access.[37] 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.[38]

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.[39] 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).[40]

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".[41] The final text preserved the underlying concern (about digital divide) while omitting the more prescriptive formulations.[42] 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".[43]

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.[44] 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).[45]

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.[46] 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.[47] 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.[48] Another State proposed establishing a needs-based catalogue as a possible component of the future portal.[49] 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,[50] one delegation characterizing these as "controversial" and calling for a "radical revision" of the structure of the exercise.[51]

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.[52] 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.[53] Several delegations sought to anchor portal and fund decisions explicitly in the future permanent mechanism to ensure continuity;[54] others cautioned against deciding timing and modalities before that mechanism was settled.[55]

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.[56] The needs-based CB catalogue was retained as a complementary tool, framed to reduce overlap and duplication, with potential integration into the portal.[57] The regular Global Roundtable format was linked to the permanent mechanism, with parameters for equitable geographic representation and support for attendance by developing states.[58] 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.[59] 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.[60]

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.[61] 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.[62]

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.[63] 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.[64]

Moreover, in the final report negotiations, it appeared that States filtered proposals through practical criteria: available financial resources and budgetary constraints,[65] 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.[66] Duplication safeguards were explicitly embedded: the fund should maximize leveraging of existing initiatives and avoid duplication.[67] 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.[68]

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.[69]

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.

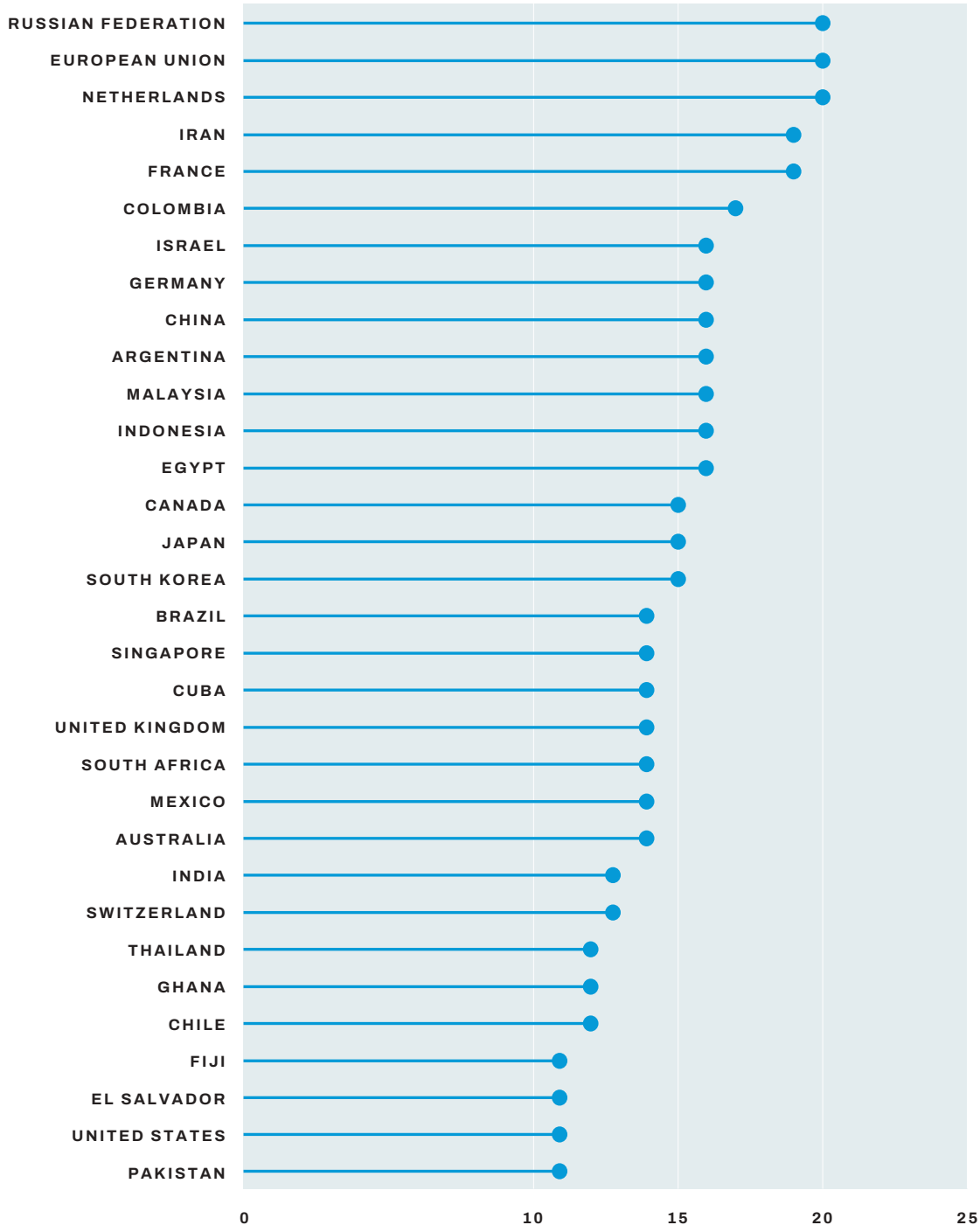
---

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[70]



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.[71] 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.[72] Similarly, Montenegro hosts the Western Balkans Cyber Capacity Centre while benefiting from projects offered by the European Commission.[73] 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.[74]

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.[75] 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.[76]

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.[77] Another proposal called for a dedicated digital tool to assist States in tracking their implementation of the norms and identifying specific capacity gaps.[78]

On international law, Member States consistently framed CB as a fundamental prerequisite for equal participation in global ICT security discussions.[79] 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.[80] 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.[81]

On confidence-building measures, several States underscored that CB is a "CBM in itself" because it fosters trust and international cooperation.[82] 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.[83]

---

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).

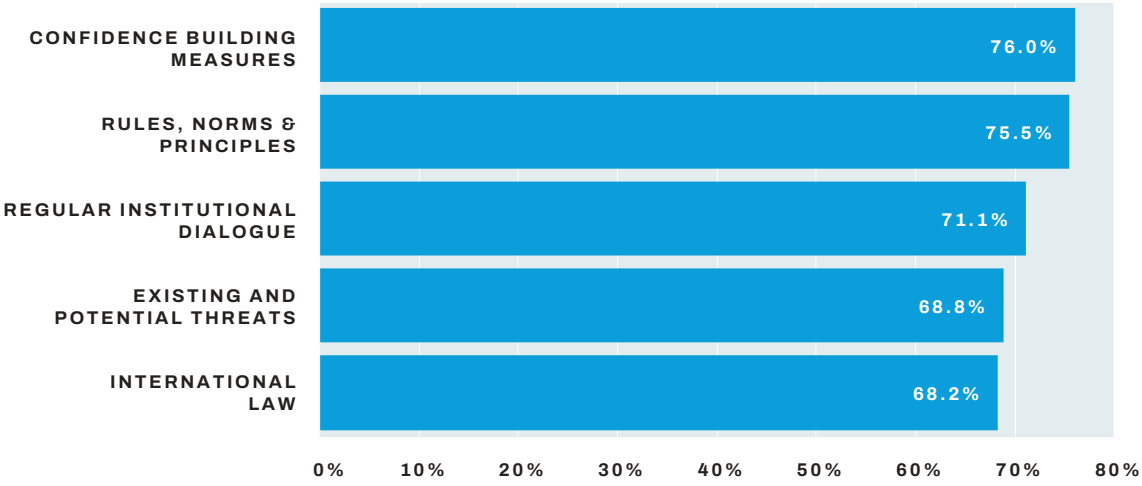
81 For example, Estonia (session 8, meeting 3); Colombia (session 10, meeting 3); Malawi (session 11, meeting 3); Singapore (session 11, meeting 3).

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.[84] The proposal emphasized that CB should not merely be a "standing item" on other agendas but required its own dedicated space and coordinator.[85] 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.[86] 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.[87]

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. 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.[88] These delegations positioned a United Nations-anchored platform as providing a neutral space where developing States could access assistance without political pressure.[89] 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.[90]

States in favour of coordination over centralization warned against "reinventing the wheel".[91] 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.[92]

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.[93] 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.[94] 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.[95] 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.[96] These delegations characterized such approaches as pragmatic responses to resource constraints that could mobilize significantly greater resources than State contributions alone.[97] 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.[98]

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".[99] 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.[100]

A middle ground proposal suggested that the United Nations function as a "clearing house" to link existing initiatives, rather than acting as direct provider.[101] The final report's consensus that the fund should "maximally leverage on existing initiatives" while remaining under United Nations management represented a compromise.[102] 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.[103] 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.[104] Other States viewed private sector partnerships as pragmatic necessities in a domain where non-State actors often possess superior technical capabilities.[105] 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.[106] The commitment to establish mechanisms "via a step-by-step modular approach" and to leverage existing initiatives represented formulations that enabled consensus.[107]

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.[108] 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.[109]

---

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.[110] 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.[111] 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.[112] 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".[113] 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.[114] 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.[115] 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**, 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.[116] States repeatedly debated whether ransomware and law enforcement cooperation belonged in OEWG capacity-building or the cybercrime process.[117] 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.[118] 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[119] – it was transparency.[120] 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.[121] 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**.

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

Regular Institutional Dialogue

Pavel Mráz and Lenka Filipová

1. Introduction

"Regular institutional dialogue" (RID) refers to continued and structured intergovernmental discussions under United Nations auspices on developments in the field of information and communications technologies (ICTs) in the context of international security. While the earlier reports of the Groups of Governmental Experts (GGEs) and Open-Ended Working Groups (OEWG) on ICT security did not formally define the term, RID progressively became shorthand for the efforts of United Nations Member States to institutionalize regular, inclusive and sustained United Nations dialogue on the subject.

The permanent institutionalization of discussions on ICT security at the United Nations represents a central outcome of the OEWG 2021–2025. While much of the OEWG's work focused on deepening the cumulative and evolving Framework of Responsible State Behaviour in the Use of ICTs (referred to simply as "the Framework"), the concurrent effort to a permanent process became arguably as significant. The adoption, by consensus, of the OEWG's final report in July 2025 included the modalities for the establishment of a Global Mechanism on International ICT Security,[1] marking the transition from time-bound working groups to a standing intergovernmental platform.

This chapter examines how discussions on RID evolved during the mandate of the OEWG on Security of and in the Use of Information and Communications Technologies 2021–2025 and culminated in the establishment of a permanent United Nations mechanism on ICT security. It situates these negotiations within the broader trajectory of United Nations discussions on international ICT security and traces how support for competing institutional models eventually coalesced around a consensus-based, single-track Global Mechanism on ICT Security. In doing so, the chapter shows how institutional design became both a reflection of and a response to the evolution of United Nations multilateral discussions in the field of international ICT security.

The following sections trace this evolution, examine the main themes and subthemes that structured the RID negotiations, and highlight key insights from the negotiation process. Specifically, Section 2 provides a chronological account of how States converged around key institutional design features of the Global Mechanism. Section 3 then analyses five design elements that structured the negotiations – the purpose and objective, guiding principles, scope and functions, structure, and modalities of RID – as well as related subthemes that surfaced under each of those themes. The chapter closes in Section 4 by highlighting key insights and lessons learned from the negotiations that are not covered by the official outcome documents, as well as their implications for the work of the Global Mechanism.

---

1 General Assembly, resolution 80/16, 2025.

This chapter focuses on negotiations conducted in the OEWG 2021–2025 and the consensus outcomes reflected in its annual progress reports (APRs) and final report. The discussions and outcomes of the March 2026 organizational session of the Global Mechanism are not reflected here. As a result, certain procedural and operational issues discussed here may have evolved further in practice beyond the scope of this analysis. Throughout the chapter, visual representations are included to facilitate understanding the evolution of discussion on RID as well as the agreed negotiation cycles and operational structure of the Global Mechanism.

1.1. The road to the OEWG 2021–2025

Discussions on this topic predated the OEWG; the first reference to RID with broad participation of States dates back to the final report of the GGE 2014–2015.[2] Between 2018 and 2021, two concurrent processes on international ICT security were established pursuant to separate General Assembly resolutions: a sixth GGE, composed of a limited number of States,[3] and the first OEWG, open to all States.[4] Both processes had a two-year mandate and adopted consensus reports in 2021.[5] However, this dual-track configuration raised questions of coherence, efficiency and allocation of scarce resources, particularly for smaller States. These factors would later contribute to calls from many States for an inclusive, single-track process.

During this dual GGE–OEWG period, calls for a permanent and action-oriented mechanism emerged. Most notable was the proposal for a Programme of Action (PoA), which was envisioned as a standing United Nations platform to facilitate the implementation of the Framework.[6] At the same time, other delegations favoured continuation of discussions within another time-limited OEWG-type body, albeit potentially with a longer mandate.[7] As discussions on a PoA and other proposals were introduced and debated within the OEWG 2019–2021, the General Assembly adopted a resolution establishing a second OEWG with a five-year duration.[8] The establishment, by vote, of a second time-bound OEWG (which was

2 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 18.

3 General Assembly, resolution 73/266, 2018, paragraph 3.

4 General Assembly, resolution 73/27, 2018, paragraph 5.

5 General Assembly, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Draft Final Substantial Report, A/AC.290/2021/CRP.2, 2021; 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.

6 "The Future of Discussions on ICTs and Cyberspace at the UN", Submitted by France et al., 2020, https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf.

7 General Assembly, First Committee, "Developments in the Field of Information and Telecommunications in the Context of International Security", Revised draft resolution submitted by Belarus, Burundi, Cambodia, China, Cuba, Democratic People's Republic of Korea, Kazakhstan, Kyrgyzstan, Lao People's Democratic Republic, Malawi, Nicaragua, Russian Federation, Syrian Arab Republic, Tajikistan, Turkmenistan, Uzbekistan, Venezuela (Bolivarian Republic of); Zimbabwe, A/C.1/75/L.8/Rev.1, 2020.

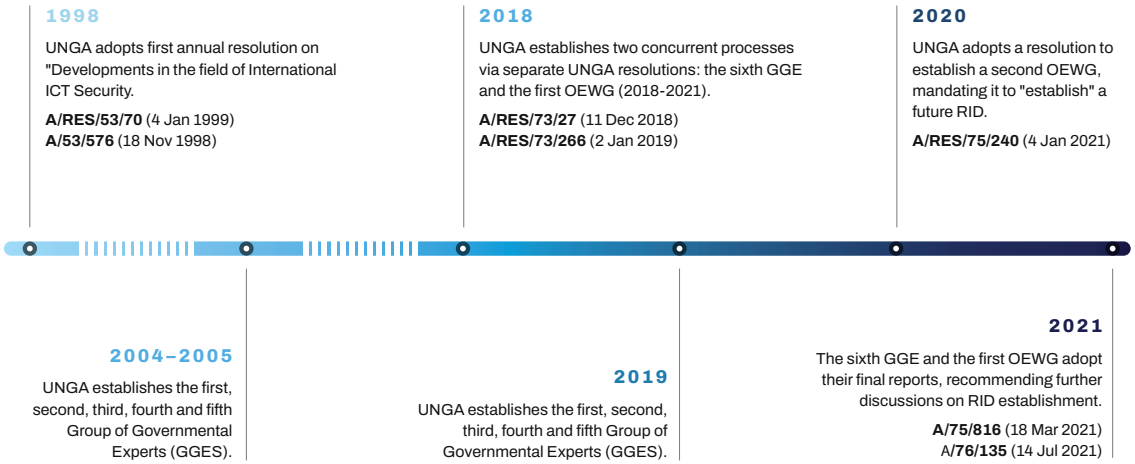
8 General Assembly, resolution 75/240, 2021.

opposed by some delegations)[9] together with concurrent proposals for a permanent PoA[10] indicated that there was not yet consensus on whether future RID should continue through time-bound processes or transition to a standing, permanent United Nations mechanism.

The final report of the OEWG 2018–2021, adopted by consensus, recommended the continuation of RID under United Nations auspices and encouraged further consideration of proposals for future institutional arrangements, including the PoA.[11] When the successor OEWG 2021–2025 was established pursuant to General Assembly resolution 75/240, the mandate explicitly included the task "to establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States".[12] Establishment of a future United Nations process on international ICT security was thus embedded within the mandate of the OEWG 2021–2025 from the outset. However, the form that such a dialogue would take remained open to negotiation.

FIGURE 1.

Timeline of institutionalization of United Nations discussion on international ICT security, foundational period and first OEWG / 6th GGE, 1998–2021[13]



9 Draft resolution A/C.1/75/L.8/Rev.1 was adopted with 104 votes for, 50 against and 20 abstentions. See General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security", Report of the First Committee, A/75/394, 2020, paragraph 10(c).

10 "The Future of Discussions on ICTs and Cyberspace at the UN", Submitted by France et al.

11 A/AC.290/2021/CRP.2, paragraphs 75–78.

12 Resolution 75/240, paragraph 1.

13 Acronyms used in the figure: GGE - Group of Governmental Experts, OEWG - Open-ended Working Group, POA - Programme of Action, RID- Regular Institutional Dialogue, UNGA - United Nations General Assembly; UNGA established five GGES between 2003 and 2015 through the following resolutions and decisions: first GGE (A/RES/58/32, 18 December 2003); second GGE (A/RES/63/37, 9 January 2009); third GGE (A/RES/66/24, 13 December 2011); fourth GGE (A/RES/68/243, 9 January 2014); fifth GGE (A/72/327, 30 December 2015).

Katherine Prizeman, Izumi Nakamitsu and Ambassador Burhan Gafoor prior to the 10th substantive session of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, New York, 2025. Credit: UN Photo / Loey Felipe.

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

The evolution of discussions on regular institutional dialogue within the OEWG 2021–2025 reflects a gradual movement from States proposing various, and sometimes divergent, RID proposals to convergence around consensus elements that would come to define the architecture of the Global Mechanism. As outlined above, the second OEWG did not operate in a political vacuum. It functioned as a single-track process following the experience of parallel OEWG and GGE tracks in 2018–2021. At the same time, both the OEWG and GGE processes had issued recommendations on establishing RID, including guiding principles that informed subsequent discussions within the second OEWG.[14] These consensus outcomes, endorsed by the United Nations General Assembly, affirmed the need for continued regular dialogue, recommended an inclusive, transparent, consensus-driven and results-based process, and noted various RID proposals, including the PoA.[15]

This section traces how convergence around a concrete institutional architecture for RID evolved across four negotiation cycles of the OEWG 2021–2025 (see Figure 3).

CYCLE 1	CYCLE 2	CYCLE 3	CYCLE 4
SESSIONS 1–3	SESSIONS 4–5	SESSIONS 6–8	SESSIONS 9–11
Institutional possibilities for RID	Designing the format, structure and modalities of RID	Alignment around core elements of the future permanent mechanism	Final consolidation into the Global Mechanism
Initial examination of institutional options and clarification of States' expectations	Consolidation of proposals and narrowing of institutional preferences	Progressive alignment and compromise around core elements of a future mechanism	Resolution of outstanding issues and agreement on outstanding, final modalities for the Global Mechanism

14 A/AC.290/2021/CRP.2, paragraphs 75–79; A/76/135, paragraph 96.

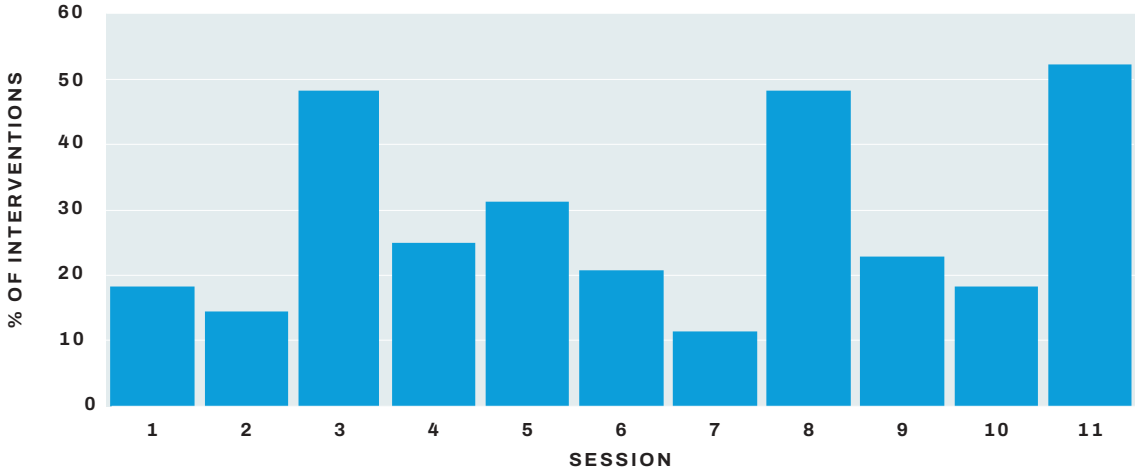
15 A/AC.290/2021/CRP.2, paragraphs 68–79; A/76/135, paragraph 97.

16 Organisational Session held on 1–2 June 2021 at UNHQ in NYC.

Together, these phases show how States translated broad agreement on the need for RID into a consensus outcome by navigating varying institutional proposals and gradually converging on the structure and format of a single permanent Global Mechanism.

FIGURE 2

Proportion of state interventions on RID topics by session[17]



2.1. Cycle 1 – Institutional possibilities for RID

From the outset of the OEWG, States diverged on how its mandate to establish RID should be realized. The main divergence centred on whether this should be accomplished through the PoA proposal or by a continuation of the OEWG format.

These competing visions quickly manifested in a polarizing debate over the inclusion of non-governmental stakeholders in the second OEWG's deliberations, shaped in part by the experience of the first OEWG, where the vast majority of stakeholders had been prevented from participating in formal sessions. This debate led to the failure of the organizational session to adopt the OEWG's programme of work. While the substance of the proposed programme of work was not itself contested in principle during the organizational session, its adoption would have effectively concluded the session, making any reopening or renegotiation of modalities governing stakeholder participation within this OEWG more difficult at a later stage. Agreement was only reached at the second substantive session, following a proposal on modalities for stakeholder participation by the Chair.[18] This carefully balanced compromise resolved the immediate procedural impasse by retaining the non-objection procedure for stakeholder accreditation while encouraging States to apply objections

17 Proportions reflect state interventions matched against at least two key terms from a thematic dictionary search of topics relating to rules, norms and principles.

18 Chairperson OEWG 2021–2025, Letter, 22 April 2022, https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf.

judiciously and in a transparent manner.[19] However, the episode highlighted underlying differences among States on key features of future RID and foreshadowed the continued sensitivity of stakeholder modalities in subsequent RID negotiations.

Apart from stakeholder inclusion, several other legacy considerations from previous processes informed the discussion. First, the time-limited nature of successive OEWG and GGE mandates required periodic General Assembly negotiations to define new processes. While such negotiations reflected the sovereign prerogatives of Member States, they also introduced uncertainty and led, at times, to divisive votes within the General Assembly. A permanent mechanism could ensure continuity without the need for recurrent mandate renewals by the General Assembly. Second, the dual-track experience of the OEWG and GGE of 2018–2021 and the General Assembly voting over competing resolutions[20] underscored the value of a single, inclusive forum. Consolidation into a single-track process was therefore suggested as both a practical and a political objective of future RID.[21]

During this initial stage, delegations advanced diverging visions for future RID and discussions remained focused on the exchange of positions and preferences around various proposals. Some delegations supported the adoption of a permanent Programme of Action.[22] Others preferred maintaining the time-bound OEWG format.[23] In early debates, one delegation highlighted the need to ensure that future RID had flexibility, suggesting that periodic reviews could serve to reconcile the permanent nature of RID with the need for adaptability by allowing the mechanism to evolve over time.[24] Early debates around the structure and modalities of RID were also closely tied to proposals concerning its substantive functions: that is, whether the future mechanism should prioritize implementation of existing commitments, further develop norms and international law, elaborate new legally binding obligations, or pursue work on all pillars of the Framework in an integrated, policy-oriented and cross-cutting nature.

Initial debates within the OEWG concerning the name of the mechanism became closely intertwined with these differing orientations. Whether described as a "Programme of Action",

---

19 The Chair's compromise modalities retained the non-objection procedure for stakeholder accreditation while introducing additional transparency and inclusivity elements. Accredited stakeholders were permitted to attend formal sessions, make oral statements during a dedicated stakeholder session and submit written inputs, while States were encouraged to apply objections judiciously. Objecting States could, on a voluntary basis, provide the Chair with the general basis for their objections, which the Chair could share with other Member States upon request. The modalities also reaffirmed the intergovernmental character of the OEWG, specifying that negotiations and decision-making remained the exclusive prerogative of Member States.

20 The OEWG 2018–2019 was created by General Assembly resolution **73/27**, adopted on 5 December 2018 with 119 votes in favour, 46 against and 14 abstentions; the GGE 2018–2019 was created by General Assembly resolution **73/266**, adopted on 22 December 2018 with 138 votes in favour, 12 against and 16 abstentions. See General Assembly, Official Records, **A/73/PV.45**, 2018, 4; General Assembly, Official Record, **A/73/PV.65**, 2019, 13–14.

21 For example, Costa Rica (session 1, meeting 9).

22 For example, European Union (session 1, meeting 9); Argentina (session 1, meeting 9); Egypt (session 2, meeting 9); Republic of Korea (session 3, meeting 8). On the Programme of Action, see also "Working Paper for a Programme of Action (PoA) to Advance Responsible State Behavior in the Use of ICTs in the Context of International Security", Submitted by a group of States, 2021, **https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf**.

23 For example, Russian Federation (session 1, meeting 9); Iran (Islamic Republic of) (session 2, meeting 9).

24 For example, Japan (session 2, meeting 9).

a renewed OEWG-type process, or more generically as "regular institutional dialogue" or a "future mechanism", a delegation's choice of terminology conveyed whether the intended emphasis was on implementation, further development or a balance of both approaches. For some delegations, giving a name to RID functioned as an expression of underlying visions for the mechanism's purpose and objectives.[25] At the same time, many delegations avoided explicit endorsement of any single institutional label, instead supporting elements drawn from different proposals.[26]

The first APR reflected this exploratory stage. It acknowledged the importance of continuity in United Nations discussions and encouraged further exchange of views on RID among States.[27] At the same time, the APR did not reflect any agreed design features of the future mechanism, with core political, structural and procedural questions remaining open and subject to future negotiations.

2.2. Designing the format, structure and modalities of RID

Between the first and second APRs, the political environment surrounding RID discussions became increasingly difficult. During this period, the General Assembly adopted two resolutions related to RID through votes. One resolution, submitted by the supporters of the PoA,[28] advanced the PoA concept by mandating the Office for Disarmament Affairs to produce a report on possible institutional architecture for the programme based on Member States' input. Through this resolution, the General Assembly also decided to hold a dedicated conference to establish the PoA in 2026, after the end of the OEWG.[29] A second resolution, advanced by the proponents of the OEWG format,[30] reaffirmed support for the OEWG process and called on States to elaborate all proposals, including those on RID, within the OEWG by consensus.[31] The adoption by the General Assembly of both of the proposals[32] related to the means of establishing RID – one within the OEWG and another through a separate conference – raised concerns around the possibility of dual-track processes and intensified calls to ensure a single-track process.[33]

---

25 For example, France (session 1, meeting 9); Switzerland (session 2, meeting 9); Egypt (session 2, meeting 9).

26 For example, India (session 1, meeting 9); Pakistan (session 2, meeting 9).

27 General Assembly, First Annual Progress 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 18.

28 Resolution 77/37 was tabled by France and had a total of 74 sponsoring States. The full list of sponsors and additional sponsors is available at: https://digitallibrary.un.org/record/3991743?v=pdf.

29 General Assembly, resolution 77/37, 2022.

30 Resolution 77/36 was tabled by the Russian Federation and had a total of 28 sponsoring States. The full list of sponsors and additional sponsors is available at: https://digitallibrary.un.org/record/3991885?ln=en&v=pdf.

31 General Assembly, resolution 77/36, 2022.

32 Resolution 77/37 was adopted on 12 December 2022 by 156 votes in favour, 7 against and 14 abstentions. Resolution 77/36 was adopted on 12 December 2022 by 112 votes in favour, 52 against and 8 abstentions. See General Assembly, Official Record, A/77/PV.46, 2022, 6–7.

33 For example, Russian Federation (session 4, meeting 9); Ireland (session 4, meeting 9); South Africa (session 4, meeting 9); India (session 4, meeting 9); Nicaragua (session 4, meeting 10).

Against this backdrop, discussions within the OEWG began to narrow, with delegations increasingly seeking to reconcile these parallel tracks and avoid a return to dual-process arrangements that marked the period of the first OEWG and sixth GGE. At the same time, the growing preference to further elaborate proposals on RID, including the PoA, within the OEWG and by consensus increasingly shifted attention towards identifying a single institutional framework capable of accommodating elements from across existing proposals.[34]

A growing number of delegations emphasized the importance of avoiding fragmentation and called for a single inclusive forum under United Nations auspices.[35] While some delegations continued to advance their institutional preferences, including for a Programme of Action or an OEWG-type format,[36] others increasingly focused on describing the features of a future mechanism without explicitly aligning with any one proposal.[37] As a result, discussions began to shift from models perceived as being in competition with one another towards identifying common modalities and selecting features from across proposals that could enjoy broad support.

Building on this shift towards identifying common elements, discussions began to show early convergence around several foundational structural features of a future mechanism. At this stage, these shared and largely uncontested design parameters of future RID featured inclusivity, consensus-based decision-making, complementarity with prior GGE and OEWG outcomes, and operation under the General Assembly. During this period, delegations increasingly spoke in favour of establishing a permanent mechanism.[38] Specifically, discussions began to focus on how a future mechanism could be structured to ensure continuity,[39] flexibility[40] and non-duplication with existing United Nations processes.[41] Although delegations continued to debate substantive prioritization – that is, implementation versus further development – discussions also increasingly focused on practical questions of the mechanism's institutional design.

The second APR captured this shift from exploratory exchanges and competing proposals towards a more focused discussion on shared structure and format elements of a future mechanism. States agreed to continue to "identify some common elements that could

---

34 For example, Iran (Islamic Republic of) (session 4, meeting 9); China (session 4, meeting 9); Cuba (session 4, meeting 9); Belgium (session 4, meeting 9); Ireland (session 4, meeting 9); New Zealand (session 5, meeting 5).

35 For example, Brazil (session 4, meeting 9), South Africa (session 4, meeting 9), India (session 4, meeting 9), Nicaragua (session 4, meeting 10), Czechia (session 5, meeting 5); Indonesia (session 5, meeting 5).

36 For example, France (session 4, meeting 9); Egypt (session 4, meeting 9); Russian Federation (session 4, meeting 9); European Union (session 4, meeting 9).

37 For example, Brazil (session 4, meeting 9); Viet Nam (session 4, meeting 9); Ghana (session 4, meeting 10); Philippines (session 5, meeting 5).

38 For example, Russian Federation (session 4, meeting 9); Denmark (session 4, meeting 9); Romania (session 4, meeting 9); Argentina (session 4, meeting 9); Viet Nam (session 4, meeting 9); Republic of Korea (session 4, meeting 9); Israel (session 4, meeting 9); Australia (session 4, meeting 9); Nicaragua (session 4, meeting 9).

39 For example, Côte d'Ivoire (session 4, meeting 9); Russian Federation (session 4, meeting 9); Nicaragua (session 4, meeting 10).

40 For example, Denmark (session 4, meeting 9); France (session 4, meeting 9); Egypt (session 4, meeting 9); United States (session 4, meeting 9); Costa Rica (session 4, meeting 10).

41 For example, Côte d'Ivoire (session 4, meeting 9); Pakistan (session 4, meeting 9); Russian Federation (session 4, meeting 9); Egypt (session 4, meeting 9); Nicaragua (session 4, meeting 10).

underpin the development of any future mechanism"[42] among existing proposals. At this stage, States also agreed that a future mechanism would be a "single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee",[43] grounded in consensus reports and aimed at promoting an "open, secure, stable, accessible, peaceful and interoperable ICT environment".[44] Furthermore, states confirmed that the future mechanism would be "open, inclusive, transparent, sustainable and flexible"[45] and capable of evolving in accordance with States' needs and in line with developments in the ICT environment. Notably, "flexibility", which had not gained wide support the previous negotiation cycle, was now supported by many delegations[46] and adopted through the second APR as a key guiding principle of the future mechanism.

2.3. Alignment around core elements of the future permanent mechanism

A decisive shift in OEWG deliberations occurred in the period leading up to the third APR. Discussions increasingly centred around specific questions concerning the institutional design of RID, such as functions, structure and modalities. This recalibration was influenced in part by the Chair's guiding questions,[47] and in part by the report by the Office for Disarmament Affairs mandated by the General Assembly resolution on the PoA.[48] This report, which compiled views from approximately 40 States on future RID, provided a structured overview of States' existing preferences and areas of convergence across several key design features of future RID, including guiding principles, scope and functions, structure, and modalities. At this stage, many delegations started to explicitly reference their preferences along similar thematic categories in their interventions.[49]

Throughout this period, questions of sequencing and prioritization of specific functions and programmatic priorities of the future mechanism continued to feature in the discussion. Some delegations emphasized functions related to implementation, capacity-building and voluntary reporting.[50] Others underscored the need to preserve space for continued normative and

---

42 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, paragraph 53.

43 **A/78/265**, paragraph 55(a).

44 **A/78/265**, paragraph 55(d).

45 **A/78/265**, paragraph 55(d).

46 See, for example, Denmark (session 4, meeting 9); France (session 4, meeting 9); Egypt (session 4, meeting 9); United States (session 4, meeting 9); and Costa Rica (session 4, meeting 10).

47 Chairperson OEWG 2021–2025, Letter, 22 November 2023, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_22_November_2023.pdf**, Annex B, "Revised Non-exhaustive List of Guiding Questions"; Chairperson OEWG 2021–2025, Letter, 20 February 2024, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_20_February_2024.pdf**, Annex A, "Revised Non-exhaustive List of Guiding Questions".

48 General Assembly, "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security", Report of the Secretary-General, **A/78/76**, 2023.

49 For example, European Union (session 6, meeting 9); Egypt (session 6, meeting 10); Cuba (session 6, meeting 10); United States (session 6, meeting 10); Mauritius (session 6, meeting 10).

50 For example, Bangladesh (session 6, meeting 10); Mauritius (session 6, meeting 10).

legal development, including the possible elaboration of additional commitments.[51] At the same time, delegations discussed how specific functions could be operationalized within a single process through the creation of dedicated subsidiary bodies or working groups, rather than through parallel or separate processes.[52]

Related discussions focused on the structure and modalities of the mechanism. Delegations exchanged views on the appropriate number of institutional layers within the mechanism. This included the potential role of a periodic review cycle or conference,[53] the role and frequency of plenary sessions,[54] and the potential establishment and scope of subsidiary bodies or working groups.[55] Some proposals and interventions also addressed leadership arrangements, including how to reflect equitable geographical representation in leadership structures in practice, and the duration of negotiation cycles.[56] Discussions of modalities continued to address stakeholder participation, including the extent and format of engagement.[57] They also touched upon the decision-making procedures and the application of the principle of consensus,[58] including whether certain procedural matters (e.g., stakeholder accreditation) might require alternative decision-making arrangements in specific circumstances. Across these exchanges, delegations increasingly framed their positions in terms of specific modalities, often drawing on and combining features from different proposals, including the PoA and the proposal for a permanent OEWG.[59]

These structured exchanges informed the consolidation of agreed elements on RID in Annex C of the third APR, which captured where States had converged around key "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security" across guiding principles, scope and functions, structure, and modalities.[60] The mechanism's provisional title itself reflected compromise without aligning the mechanism explicitly with the name of a previously submitted proposal: "Open-Ended" safeguarded universal, inclusive participation and reflected preferences of some delegations for

---

51 For example, Russian Federation (session 6, meeting 9); Cuba (session 6, meeting 10); China (session 6, meeting 10).

52 For example, Egypt on behalf of the Arab Group (session 6, meeting 10); Cuba (session 6, meeting 10).

53 For example, China (session 6, meeting 10); Russian Federation (session 8, meeting 4).

54 For example, China (session 6, meeting 10); France (session 7, meeting 10); United States (session 7, meeting 10).

55 For example, Egypt (session 7, meeting 10).

56 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies", Submitted by Belarus et al., **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_paper_on_a__Permanent_Decision-making_OEWG.pdf**, 3; Chairperson OEWG 2021–2025, "Draft Elements", 2024, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_1_May_2024_0.pdf**, paragraph 18(c). See also, for example, El Salvador (session 7, meeting 10).

57 For example, United Kingdom (session 6, meeting 10); Switzerland (session 6, meeting 10); United States (session 7, meeting 10); Netherlands (session 8, meeting 4); Australia (session 8, meeting 4).

58 For example, Brazil on behalf of the IBSA (India, Brazil and South Africa) Dialogue Forum (session 6, meeting 10); Bangladesh (session 6, meeting 10); Malaysia (session 6, meeting 10); South Africa (session 6, meeting 10); China (session 7, meeting 10); Israel (session 8, meeting 5); United Kingdom (session 8, meeting 7).

59 On the proposal of a permanent OEWG, see "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al.

60 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, Annex C.

a renewed OEWG-type body; "Action-Oriented" captured the shared aspiration of States to move beyond deliberative formats and integrated the proposed intent of the PoA to focus on advancing implementation in a practical manner. Annex C of the third APR also stabilized agreement across several key design elements of the new mechanism, including the length of its negotiation and review cycles, structured engagement with non-governmental stakeholders, and reporting to its parent body, the General Assembly.

The majority of operational modalities were also delineated at this stage. The permanent mechanism would function as a subsidiary body of the General Assembly, report to the First Committee and convene formal meetings at the United Nations Headquarters in New York. The Office for Disarmament Affairs would serve as its Secretariat and create a dedicated e-portal to ensure transparency.[61] Annex C further specified that all decisions would be taken based on the principle of consensus and outlined transitional arrangements, including the mechanism's organizational session in early 2026 to elect leadership, establish dedicated thematic groups (DTGs) and adopt remaining modalities.[62] While certain elements (e.g., the precise configuration of DTGs and detailed stakeholder modalities) were left for finalization through the OEWG final report, States effectively discussed and consolidated key institutional and operational elements of the future mechanism throughout the third OEWG negotiation cycle.

2.4. Final consolidation into the Global Mechanism

Following adoption of the third APR, negotiations entered a final consolidation phase. With core elements agreed, States' discussions turned to resolving remaining modalities and translating agreed "elements" into an institutional framework capable of seamless transition from the OEWG. Outstanding issues were limited in number but politically significant. These included the name of the mechanism, the number and substantive focus of dedicated thematic groups, detailed modalities for stakeholder participation, and procedural arrangements for formal establishment.

Discussions on DTGs revealed differing views regarding how substantive work within the future mechanism should be organized. Proposals in this negotiation cycle were broadly clustered around four approaches:

a. **Cross-cutting approaches:** DTGs organized around broader policy challenges, with norms, international law, confidence-building measures (CBMs), threats and capacity-building discussed in an integrated manner across each group[63]

b. **Pillar-based approaches:** DTGs aligned with the Framework's five pillars, including proposals for a dedicated international law group or separate normative tracks[64]

---

61 A/79/214, Annex C, paragraph 15.

62 A/79/214, Annex C, paragraph 17.

63 For example, France (session 9, meeting 9); Canada (session 9, meeting 9); European Union (session 9, meeting 9); Germany (session 9, meeting 10); Ireland (session 9, meeting 10).

64 For example, Russian Federation (session 9, meeting 9); Singapore (session 9, meeting 9); China (session 9, meeting 10).

A Representative of Malaysia (on screen) speaks during the eleventh substantive session (7–11 July) 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.

c. **Combined approaches:** proposals seeking to integrate cross-cutting practical groups with a dedicated legal or normative component[65]

d. **Capacity-building focused approaches:** proposals emphasizing capacity-building either as a dedicated DTG or as a standing element across all thematic workstreams[66]

The configuration ultimately agreed in Annex I of the final report of OEWG 2021–2025 reflected elements from several of these approaches. It proposed a streamlined model of two integrated, policy-oriented and cross-cutting DTGs drawing on the five pillars of the Framework:[67]

I. Address specific challenges in the sphere of ICT security in the context of international security (DTG1)

II. Accelerate ICT security capacity-building (DTG2)

States also agreed on the final title of the mechanism: the "United Nations 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". This choice reflected a carefully balanced synthesis. The term "Global Mechanism" underscored universality without explicitly privileging any previously advanced proposal.

Stakeholder participation – among the most sensitive issues across the mandate – was addressed by replicating the modalities for stakeholder accreditation from OEWG 2018–2021 with some adjustment:[68] new provisions were added to ensure greater transparency in States'

65 For example, Egypt (session 9, meeting 9); Switzerland (session 9, meeting 10); Finland (session 10, meeting 10); South Africa (session 11, meeting 4).

66 For example, Brazil (session 9, meeting 9); Argentina (session 10, meeting 10); Uruguay (session 11, meeting 4).

67 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, Annex I, paragraph 7.

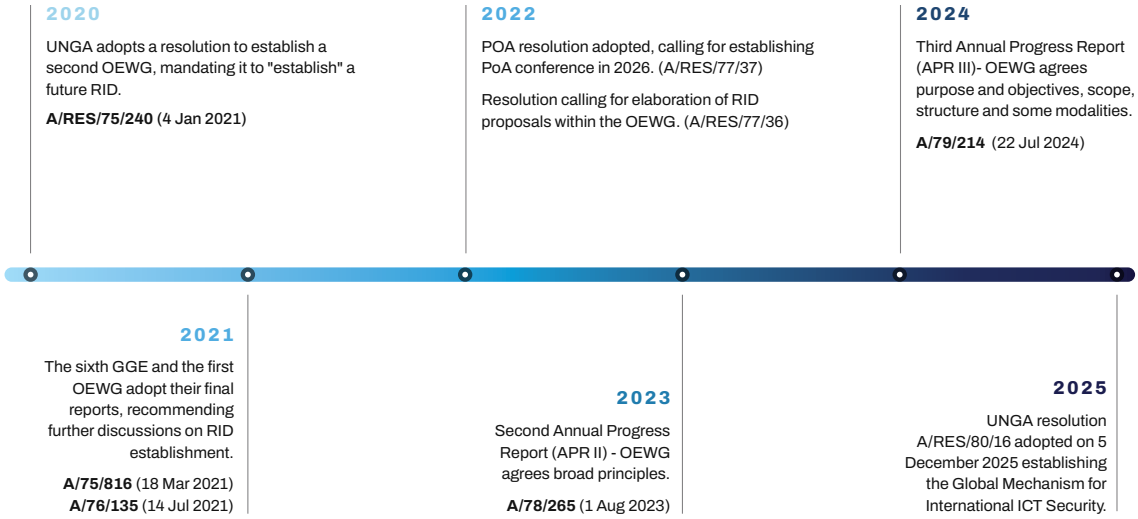
68 A/80/257, Annex I, paragraph 15(d).

potential objections to the participation of individual stakeholders as well as Chair-facilitated consultations to address concerns related to such objections.[69] Importantly, the final report further clarified that all DTG meetings would take place in hybrid format and that, "in accordance with United Nations practice, hybrid meetings are considered informal".[70] This settled at least one important operational aspect of the DTGs and reinforced their distinct character within the broader structure of the Global Mechanism. At the same time, the final report reaffirmed the intergovernmental and State-led nature of the Global Mechanism, while also signalling the openness of the DTGs to stakeholder participation and contributions.[71] Importantly, the final report maintained consensus as the governing basis for the Mechanism's work and did not explicitly introduce alternative decision-making modalities.[72]

With the adoption of the Final Report in July 2025, the OEWG fulfilled its mandate on RID under resolution 75/240. The evolution through the four cycles illustrates a gradual transformation: from at times polarizing exchange of positions and diverging preferences around various proposals (Cycle 1); via gradual convergence around foundational design parameters and political objectives, such as flexibility, permanent nature and single-track mechanism (Cycle 2); to alignment around remaining structural and operational elements (Cycle 3); and on to resolution of the final, outstanding modalities (Cycle 4).

FIGURE 3.

Timeline of institutionalization of United Nations discussion on international ICT security, second OEWG, 2020–2025[73]



69 A/80/257, Annex I, paragraph 15(l).

70 A/80/257, Annex I, paragraph 10.

71 A/80/257, Annex I, paragraph 15.

72 A/80/257, Annex I, paragraph 15(g).

73 Acronyms used in the figure: GGE - Group of Governmental Experts, ICT - Information and Communication Technology, OEWG - Open-ended Working Group, PoA - Programme of Action, RID - Regular Institutional Dialogue, UNGA - United Nations General Assembly.

3. Trends and major themes addressed during the mandate

Although discussions on regular institutional dialogue were not formally organized around fixed categories, five recurring macro themes can be identified in the OEWG discussions: purpose and objectives, guiding principles, scope and functions, structure, and modalities. These macro themes provide the analytical framework used in this section for understanding how States approached the task of institutional design within the OEWG 2021–2025. This allows the mapping of proposals advanced by Member States during RID discussions in greater detail and the identifying of specific subthemes that emerged under each theme over the course of States' deliberations. Some of these subthemes cut across more than one macro theme; for example, inclusivity was discussed both as a guiding principle and as a question of modalities. The analysis below therefore does not treat the five macro themes as rigidly separate, but rather as organizing headings under which related debates can be clustered. The chronological evolution of these issues is addressed separately in Section 2.

3.1. Purpose and objectives

"Purpose and objectives" refer to the broader goals that States hope to achieve via a future permanent mechanism. These can include advancing the implementation or further development of the Framework, operationalization of additional CBMs, or coordination of capacity-building. Debates on purpose and objectives formed the conceptual anchor of OEWG discussions on RID.

From the inception, delegations broadly agreed on the purpose of the future mechanism, which should act as an intergovernmental forum for United Nations deliberations on ICTs in the context of international security. The primary objective of the mechanism would be to promote international peace, security and stability in the ICT environment by advancing the evolving and cumulative Framework, rather than "starting from scratch".[74] Some delegations proposed that such advancement should take place in an "action-oriented manner".[75] Proposals and statements submitted by various States and groups of States also suggested that, in addition to a deliberative role, the future mechanism could also serve decision-making,[76] coordination and facilitation purposes.

Across submissions and interventions, several recurring subthemes emerged under this macro theme. These included implementation and further development of the Framework; development and operationalization of additional CBMs; continued discussions on the

74 For example, European Union (session 3, meeting 8); France (session 4, meeting 9); Slovakia (session 6, meeting 10).

75 For example, India (session 1, meeting 9); Egypt (session 1, meeting 9); Netherlands (session 2, meeting 9); Canada (session 2, meeting 9).

76 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al.

application of international law;[77] negotiation of additional commitments, including legally binding obligations; and coordination of capacity-building efforts.

For some delegations, the principal purpose of the future mechanism was to support implementation of the agreed Framework.[78] Others placed greater emphasis on preserving space for continued normative and legal development, including further discussion on international law and, in some proposals, negotiation of additional[79] However, many delegations resisted treating these priorities as mutually exc.[80]

While these objectives appeared in multiple submissions in different configurations, States expressed a wide range of views regarding their relative prioritization and appropriate sequencing. For a number of delegations, the principal objective of a future mechanism was to prioritize the implementation of the previously agreed cumulative and evolving Framework.[81] In this view, regular dialogue would provide a structured and action-oriented platform to translate agreed norms, CBMs and capacity-building commitments into practical effect. This implementation-oriented perspective was closely associated with – but by no means limited to – proposals framed as a "Programme"[82], representing a standing platform focused on implementation under United Nations auspices.

Other delegations identified the further development of the Framework as a central priority for any future mechanism.[83] While not dismissing the importance of implementation, they underscored the need to preserve dedicated space for continued study, clarification and, where appropriate, further elaboration of the Framework across all its pillars. In this context, specific proposals were made for the development of additional norms and the possibility of negotiating new legally binding obligations.[84]

A recurring subtheme across many interventions was the need to reconcile implementation and further development of the Framework within a single institutional architecture. Many delegations resisted framing implementation and development as mutually exclusive or as processes that could not proceed concurrently.[85] Instead, they advocated for a flexible mechanism capable of advancing implementation of existing commitments while retaining the ability to further develop the Framework, as appropriate, in response to the evolving ICT threat landscape and technological change.[86]

---

77 A/78/76, paragraph 29.

78 For example, Switzerland (session 1, meeting 9); France (session 4, meeting 9); Canada (session 4, meeting 9).

79 For example, Russian Federation (session 1, meeting 9); Iran (Islamic Republic of) (session 1, meeting 9); Pakistan (session 1, meeting 9).

80 For example, India (session 1, meeting 9); United Kingdom (session 1, meeting 9); South Africa (session 2, meeting 9).

81 For example, Switzerland (session 1, meeting 9), France (session 4, meeting 9); Canada (session 4, meeting 9).

82 For example, "Working Paper for a Programme of Action (PoA)", Submitted by a group of States.

83 For example, India (session 1, meeting 9); Pakistan (session 1, meeting 9); Thailand (session 2, meeting 9).

84 For example, Russian Federation (session 1, meeting 9), India (session 1, meeting 9); Iran (Islamic Republic of) (session 1, meeting 9); Pakistan (session 1, meeting 9).

85 For example, India (session 1, meeting 9); United Kingdom (session 1, meeting 9); South Africa (session 2, meeting 9).

86 For example, France (session 1, meeting 9); Australia (session 1, meeting 9); Colombia (session 6, meeting 10); Latvia (session 6, meeting 10).

Taken together, discussions on purpose and objectives revealed a spectrum of institutional visions, ranging from implementation-focused models to development-oriented approaches, as well as hybrid arrangements seeking to accommodate both. These differing orientations, in turn, shaped debates on institutional design across guiding principles, scope and functions, structure, and modalities.

3.2. Guiding principles

In parallel with discussions on purpose and objectives, States proposed various guiding principles intended to inform the character and functioning of a future mechanism. Across submissions and statements, several foundational principles were repeatedly invoked as essential to the legitimacy and effectiveness of regular institutional dialogue.

Among these, inclusivity featured as a prominent subtheme. Delegations consistently emphasized that the mechanism should be open to all United Nations Member States.[87] This reflected the universal relevance of international ICT security and States' consensus that such matters should be addressed in an inclusive format beyond the GGE expert format. While inclusivity itself was widely supported, discussions revealed differing views on how it should be translated into practice, particularly with respect to stakeholder participation and the ability of all delegations to engage meaningfully in the proceedings.

Flexibility was another commonly referenced subtheme, particularly by delegations seeking to strike a balance between implementation and further development of the Framework. Given the dynamic nature of technological change and the evolving ICT threat landscape, many States underscored the importance of designing a mechanism capable of adapting over time.[88] Flexibility was therefore understood as enabling the process to evolve without requiring repeated structural renegotiation of time-bound mandates, which had proven challenging in the past.

Closely related was the subtheme of complementarity, frequently expressed alongside the notion of non-duplication. Delegations emphasized that a future mechanism should operate as a "single-track process",[89] should build upon previous GGE and OEWG outcomes, and should coordinate with other relevant processes rather than duplicate, in part or in whole, existing efforts within the United Nations system.[90] This principle reflected sensitivity to the risk of fragmentation within the United Nations system, the prior experience of parallel GGE and OEWG processes, and the desire to promote coherence.

Over the course of OEWG discussions, the subtheme of permanence emerged with increasing frequency. While initially embedded in specific proposals,[91] permanence eventu-

87 For example, A/78/76, paragraph 14.

88 For example, A/78/76, paragraph 15.

89 For example, A/79/214, paragraph 56(b).

90 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al., 2; "Working Paper for a Programme of Action (PoA)", Submitted by a group of States, 4.

91 For example, "Working Paper for a Programme of Action (PoA)", Submitted by a group of States; "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al.

ally came to be framed more broadly as essential to ensuring continuity, predictability and institutional memory within the United Nations' engagement on international ICT security. A related and frequently cited principle was sustainability, often invoked to underscore that financial provisions would need to be made for the continuity and long-term viability of any permanent mechanism. Although broadly supported, sustainability remained linked to specific questions about how institutional ambition would align with available resources and sustained political commitment.

Transparency was similarly referenced as a subtheme, particularly in relation to reporting, information-sharing and the openness of discussions. Compared with the closed-door format of the GGE processes, the first OEWG established a comparatively higher degree of procedural transparency, which was continued from the outset by its successor, the OEWG 2021–2025. Written submissions and proposals were made publicly available, substantive sessions were webcast, and draft reports were circulated to delegations and uploaded to the website of the Office for Disarmament Affairs. In discussions on RID, delegations emphasized that transparency should remain a feature of any future mechanism.[92]

Beyond these broadly shared principles, additional considerations were raised across various proposals. Some delegations underscored the importance of respect for sovereignty, preserving the intergovernmental nature of the process, non-interference in the internal affairs of States,[93] human rights,[94] gender[95] and capacity-building.[96]

While many of these guiding principles were not themselves contested, discussions revealed differing perspectives on how they should be operationalized and balanced in practice through specific functions, structure and modalities, including modalities for decision-making and stakeholder participation. The various principles guided the concrete institutional design proposals that were advanced and debated.

3.3. Scope and functions

The term "functions" is used here to refer to specific programmatic activities to be undertaken within the future mechanism to support the attainment of agreed objectives. For example, to advance implementation, specific functions could include voluntary reporting; mapping challenges faced by States when implementing the Framework identifying good practices and solutions to support national implementation efforts; conducting the Framework gap analysis; or exchanging lessons learned. If discussions on purpose addressed the overarching goals of a future mechanism (see Section 3.1), debates on scope and function concerned the substantive focus of the process and the specific activities through which

92 For example, India (session 1, meeting 9), European Union (session 1, meeting 9), Iran (Islamic Republic of) (session 1, meeting 9), South Africa (session 4, meeting 9), Bangladesh (session 6, meeting 10); Pakistan (session 6, meeting 10).

93 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al., 2.

94 For example, Argentina (session 6, meeting 9); Thailand (session 9, meeting 10).

95 For example, Brazil (session 8, meeting 4); Chile (session 10, meeting 9).

96 A/78/76, paragraph 31.

agreed objectives would be pursued. In this context, "scope" refers to the thematic coverage of the mechanism (e.g., CBMs), while the term "functions" denotes the concrete programmatic activities that the future mechanism would undertake under this agreed scope (e.g., implementation of agreed CBMs). In practice, discussions on both evolved in parallel and were closely interlinked.

Across submissions and statements, there was broad agreement that the mechanism's scope should encompass the Framework in a holistic manner. Proposals frequently referenced advancing discussions across Framework pillars, including identifying ICT-related threats;[97] supporting implementation of norms, international law and CBMs;[98] strengthening capacity-building efforts;[99] and further developing specific elements of the Framework. In addition to defining thematic scope, States proposed a range of concrete functions. While these proposals attracted differing levels of support and were not equally reflected in subsequent negotiated outcomes, they collectively illustrate the breadth of activities envisioned by different States for a future mechanism. These proposals included:

- **Mapping specific needs and challenges faced by States**[100] when implementing the Framework[101]
- **Identifying good practices, lessons learned and solutions** to support national implementation efforts[102]
- **Conducting voluntary reporting**[103] **and Framework gap analysis** across norms and international law[104]
- **Elaborating threat-mitigation and incident-response measures**[105]
- **Establishing a multilateral attribution cooperation mechanism** under the framework of the United Nations[106]
- **Strengthening communications channels** and elaborating procedures for de-escalation in the event of ICT incidents[107]

---

97 For example, European Union (session 9, meeting 9); Japan (session 9, meeting 9)

98 For example, Egypt on behalf of the Arab Group (session 6, meeting 10); European Union (session 9, meeting 9); Australia (session 10, meeting 10).

99 For example, European Union (session 9, meeting 9); Argentina (session 10, meeting 10); Australia (session 10, meeting 10).

100 For example, "Proposal on the Structure of the Future Mechanism for Regular Institutional Dialogue on Cyber Issues", Cross-regional working paper submitted by Albania et al., https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_cross-regional_working_paper_-_Future_UN_cyber_mechanism_for_2025_onward-vf_0.pdf, 2.

101 "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2.

102 "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2.

103 Chairperson OEWG 2021–2025, "Draft Elements", paragraph 16.

104 A/78/76, paragraph 28.

105 For example, Mexico (session 6, meeting 10); Singapore (session 9, meeting 9); Thailand (session 9, meeting 10); United Kingdom (session 9, meeting 10); Cameroon (session 10, meeting 9); Japan (session 10, meeting 9).

106 Statement submitted by China, 17 February 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/REMARK~1.PDF, 18.

107 For example, Netherlands (session 1, meeting 9); Netherlands (session 8, meeting 4).

- **Mobilizing and pairing available resources** with requests for capacity-building support[108]
- **Negotiating additional commitments,** including legally binding obligations, to increase international cooperation on ICT security[109]

Many States also called for the mechanism to report periodically to the General Assembly, consistent with the established practice of past OEWGs and GGEs.[110] This would imply a "reporting" function, although the proposals differed on the precise length and scope of this reporting cycle.

While most proposals referenced many of these functions, early differences were evident regarding prioritization, sequencing and the extent of ambition. Some delegations emphasized practical support for national implementation and capacity-building coordination.[111] Others underscored the importance of prioritizing space for normative or legal development.[112] These differing emphases also informed how delegations envisaged the prioritization of functions and sequencing of specific programmatic activities to fulfil those functions. For example, some supported an initial focus on functions related to reviewing implementation of existing norms and clarifying how international law applies (including identifying potential gaps) before considering whether additional norms or legally binding obligations would be needed.[113] Others placed greater emphasis on functions related to advancing normative and legal elaboration either in parallel[114] or as a primary function of the mechanism.[115]

Taken together, discussions on scope and function showed broad convergence around a comprehensive thematic scope covering all elements of the Framework, including threats, norms, international law, CBMs and capacity-building.[116] At the same time, divergences persisted regarding the specific functions the mechanism should perform within this scope, particularly the balance between implementation-oriented activities (e.g., capacity-building coordination, voluntary reporting and exchange of good practices) and more normative functions (e.g., norm development and negotiation of additional commitments). The agreed scope and functions of the Global Mechanism ultimately reflected a compromise by incorporating both implementation and further development as potential functions, while framing more sensitive or prescriptive programmatic activities in general terms or creating a space for their future inclusion through a dedicated review conference.[117]

---

108 "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2.

109 "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al., 1; "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2.

110 For example, Submission by Brazil, **https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Brazil-_EN--_website.pdf**, paragraph 11; **A/78/76**, Submission by Egypt, 39; Submission by Slovenia, 76.

111 For example, France (session 9, meeting 9); European Union (session 9, meeting 9).

112 For example, **A/78/76**, paragraph 28.

113 For example, Egypt on behalf of the Arab Group (session 6, meeting 9); Japan (session 6, meeting 10).

114 For example, European Union (session 6, meeting 9); France (session 6, meeting 9).

115 For example, Iran (Islamic Republic of) (session 9, meeting 9).

116 **A/78/76**, paragraph 9; **A/79/214**, Annex C, paragraph 9; **A/80/257**, Annex I, paragraph 6.

117 **A/79/214**, Annex C, paragraphs 8–11; **A/80/257**.

3.4. Structure

Three principal subthemes arose in discussions on the structure of the future mechanism.

First, various proposals supported the holding of plenary sessions open to all Member States within the new RID.[118] This would both reflect continuity with the OEWG practice and preserve the intergovernmental character of the mechanism as a forum for exchange of views among Member States and the adoption of formal outcomes. Specific proposals also suggested retaining other meeting formats that had been developed in the two OEWG processes, including dedicated multi-stakeholder dialogues and high-level round tables on specific thematic issues, such as capacity-building.[119]

A second, and related, structural subtheme concerned the overall format and temporal nature of the future mechanism. While some delegations supported a permanent standing arrangement under United Nations auspices,[120] others favoured retaining an OEWG-type model, in some cases with longer or rolling mandates.[121] These preferences reflected different views on how best to preserve inclusivity, flexibility and space for continued intergovernmental discussion and negotiation. In the agreed texts, the preference for a permanent mechanism ultimately prevailed, although elements associated with flexibility and continued review were also retained.

Third, numerous submissions and statements acknowledged the potential value of subsidiary bodies to facilitate more focused and technical exchanges. Proposals referenced intersessional working groups, thematic committees or dedicated subsidiary tracks tasked with addressing specific subject areas. These included working groups aligned with the pillars of the Framework to assess its implementation, examine developments in the ICT threat landscape, identify priority and provide strategic political guidance.[122] However, views differed on their of frequency of meeting, duration,[123] scope,[124] and relationship to plenary meetings and programmatic work.[125]

In terms of the institutional layers of the future mechanism, certain proposals envisaged a multi-tiered structure composed of review conferences, plenaries and intersessional thematic bodies.[126] Others favoured a more streamlined architecture limited to one or two

---

118 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al., 2; "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2; Chairperson OEWG 2021–2025, "Draft Elements", paragraph 9.

119 For example, "Proposal on the Structure of the Future Mechanism", Cross-regional working paper, 2; Chairperson OEWG 2021–2025, "Draft Elements", paragraph 21.

120 For example, European Union (session 1, meeting 9); Indonesia (session 1, meeting 9); Colombia (session 1, meeting 9).

121 For example, Russian Federation (session 1, meeting 9); Iran (Islamic Republic of) (session 2, meeting 9).

122 For example, Japan (session 2, meeting 9), South Korea (session 6, meeting 10), European Union (session 7, meeting 10); United States (session 7, meeting 10).

123 For example, Egypt (session 6, meeting 10); Ghana (session 10, meeting 10).

124 For example, Egypt on behalf of the Arab Group (session 6, meeting 10); France (session 7, meeting 10). See also A/78/76, Annex, Submission by Australia, 16.

125 For example, Egypt (session 6, meeting 9); France (session 7, meeting 10).

126 For example, A/78/76, Annex, Submission by Australia, 17; Submission by Egypt, 38; Submission by Belgium, 20.

layers, typically centred on plenaries with the possible establishment of subsidiary working groups.[127] For example, some proposals outlined a three-tier structure comprising review conferences held every four to six years, biannual plenaries and working groups convened.[128] One proposal suggested adopting biennial progress reports without creating an review layer.[129]

Some submissions and statements also addressed the subtheme of the potential leadership structure of the new mechanism. A group of States proposed a leadership bureau composed of a chair and vice-chairs, specified the duration of appointment of these officeholders, and made references to specific arrangements for ensuring regional balance.[130] While some submissions did not elaborate in detail on leadership design, others referenced a regionally representative bureau.[131]

Structural preferences were closely linked to expectations regarding the mechanism's functions. Proposals that envisaged broader thematic work tended to favour a more layered architecture, including plenaries, subsidiary bodies and periodic review meetings. Other proposals placed greater emphasis on plenary-based political negotiations and streamlined reporting, preferring leaner configurations with fewer subsidiary bodies and less institutional layering.

In the agreed texts, several structural preferences were retained, but often in a streamlined form. The final architecture of the Global Mechanism preserved plenary meetings open to all Member States,[132] confirmed the Office for Disarmament Affairs as Secretariat,[133] established subsidiary bodies[134] periodic review cycle.[135] At the same time, the agreed design did not reproduce the most elaborate multilayered proposals in full: instead, it settled on only two initials DTGs,[136] annual plenary sessions,[137] and a five-year cycle combining two biennial phases followed by a one-year period, including a Review Conference.[138] Leadership arrangements were also retained in simplified form through cycle-based chairs implicitly through the possibility of selecting geographically representative co-facilitators for the DTGs.[139] In contrast, competing institutional formats, including alternative or parallel models outside the agreed permanent mechanism, were not included in the final design.

---

127 For example, **A/78/76**, Annex, Submission by Canada, 25; Submission by Norway, 70.

128 For example, **A/78/76**, Annex, Submission by Egypt, p38; Submission by Belgium, 21–22.

129 **A/78/76**, Annex, Submission by Czechia, 33.

130 For example, Bangladesh (session 7, meeting 10), Iran (Islamic Republic of) (session 7, meeting 10); Kenya (session 11, meeting 4).

131 For example, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group", Submitted by Belarus et al., 3; Chairperson OEWG 2021–2025, "Draft Elements", paragraph 18(c). See also, for example, El Salvador (session 7, meeting 10).

132 **A/79/214**, 22 July 2024, Annex C, paragraph 12(a).

133 **A/79/214**, Annex C, paragraph 15(c).

134 **A/79/214**, Annex C, paragraph 12.

135 Ibid.

136 **A/79/214**, Annex C, paragraph 7.

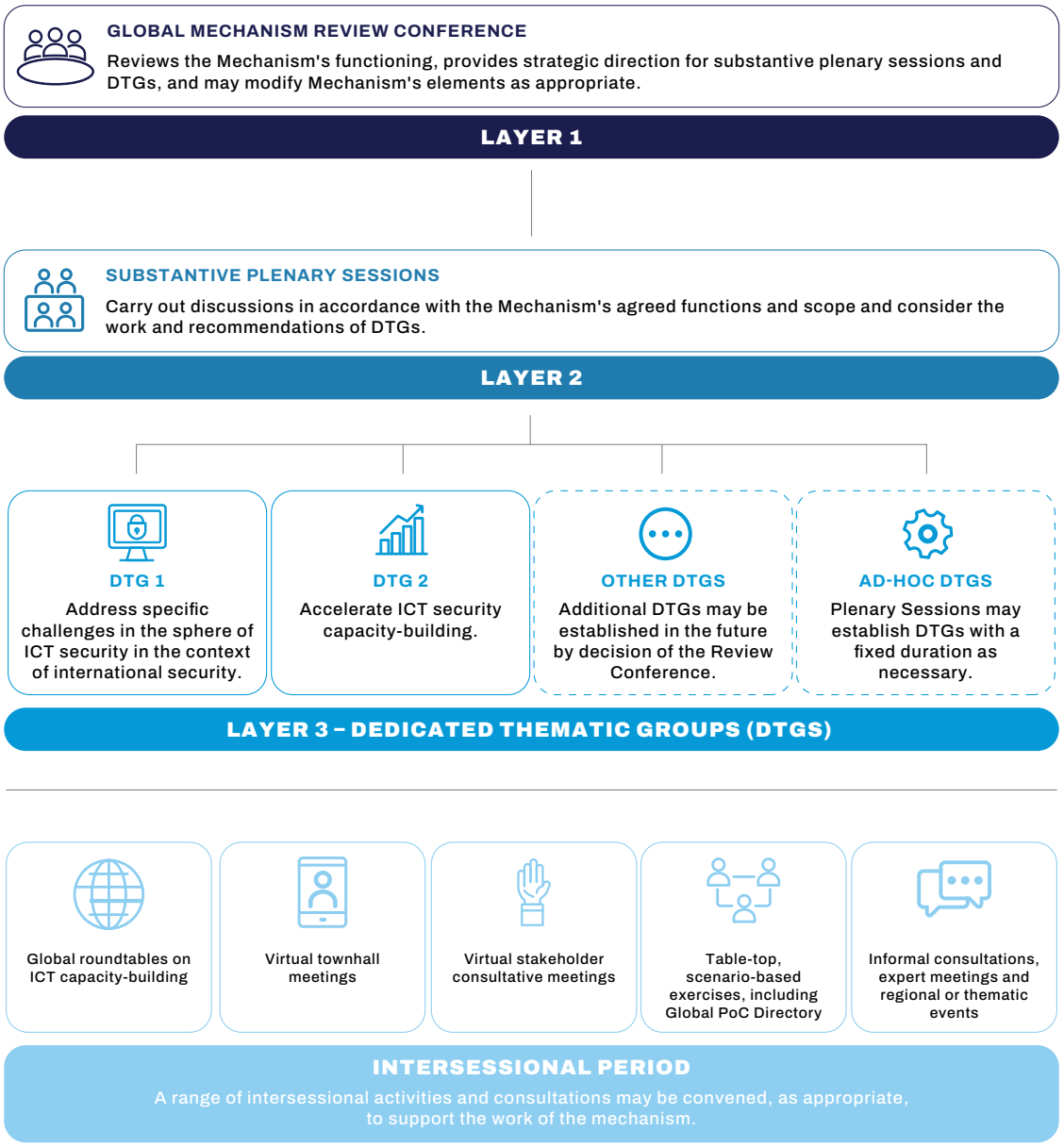
137 **A/79/214**, Annex C, paragraph 12(a).

138 **A/79/214**, Annex C, paragraph 12.

139 **A/79/214**, Annex C, paragraph 13.

FIGURE 4.

Agreed structure of the Global Mechanism on ICT Security



3.5. Modalities

If structure concerned the institutional architecture, modalities addressed the procedural rules governing how RID would operate in practice.[140] The future mechanism would, unless otherwise specified, be guided by the United Nations General Assembly's Rules of Procedure.

Within this macro theme, the main procedural subthemes concerned, decision-making and stakeholder participation to facilitate an "inclusive, transparent, consensus-driven, and results-based" process.[141] In practice, this meant that delegations discussed how principles such as inclusivity, transparency and consensus should be translated into concrete modalities, including decision-making and meeting arrangements (e.g., location and format). While inclusivity as a guiding principle was not broadly questioned by States, the precise modality for stakeholder engagement featured prominently in OEWG debates. Delegations supported engagement with civil society, the private sector and academia.[142] At the same time, States generally agreed that the permanent mechanism should preserve the State-led nature of the discussion and that stakeholder engagement should take place on the basis of the principle of "a voice, not a vote".[143]

Regarding stakeholder participation, states debated whether stakeholder participation modalities should apply uniformly across all components of the future mechanism. Some States preferred to opt for the existing accreditation procedures of the Economic and Social Council and for maintaining consistent accreditation modalities throughout the future mechanism.[144] Others supported a tailored accreditation procedure specific to the mechanism and differentiated approach under which DTGs,[145] particularly if operating in a more informal or expert-oriented manner, could allow broader and more flexible stakeholder engagement than substantive sessions of the plenary or review conference.[146] These discussions were linked to broader debates concerning the status of DTGs as formal or informal bodies, their working methods, and their intended role in supporting operational and technical exchanges.

In parallel, discussions also addressed the ability of States to participate meaningfully, including proposals for voluntary sponsorship arrangements to facilitate participation of capital-based experts from developing countries and smaller delegations.[147] These suggestions were linked to concerns about equitable geographic participation.[148]

---

140 **A/80/257**, paragraph 63.

141 **A/AC.290/2021/CRP.2**, paragraph 74.

142 **A/79/214**, Annex C, paragraph 6.

143 For example, France (session 7, meeting 9); United States (session 7, meeting 9); Brazil (session 8, meeting 4); Latvia (session 8, meeting 5); Latvia (session 8, meeting 5); Iran (Islamic Republic of) (session 10, meeting 9); China (session 10, meeting 10).

144 For example, Russian Federation (session 9, meeting 9); Iran (Islamic Republic of) (session 9, meeting 9); Ghana (session 10, meeting 10).

145 For example, Brazil (session 9, meeting 9).

146 For example, Canada and Chile co-coordinated, on behalf of a cross-regional group of States, the submission of a working paper on practical modalities to enable meaningful stakeholder participation in the future UN mechanism on cybersecurity. See **Practical Modalities for Stakeholders' Participation and Accreditation Future UN Mechanism on Cybersecurity**, 20 May 2025.

147 **A/80/257**, Annex I, paragraph 15(j).

148 For example, Brazil (session 8, meeting 4); Sierra Leone (session 9, meeting 10).

Consensus-based decision-making received broad support. Delegations emphasized the importance of the "principle of consensus" both in establishing the future mechanism and in guiding its subsequent decision-making.[149] Some understood this principle to apply to both procedural and substantive matters.[150] However, the precise scope of consensus, and whether narrowly defined exceptions should apply, remained under discussion. Discussions revealed differing interpretations of how consensus should function in practice. Alongside the need to preserve efficiency and effectiveness, concerns were expressed regarding the potential for a misuse of consensus to lead to gridlock or de facto veto dynamics.[151] Clarifications were also offered that the "principle of consensus" should not be equated with strict unanimity or individual veto power. In a more limited context, particularly concerning decisions on stakeholder participation, proposals suggested that majority voting could serve as a fallback where objections were not broadly shared.[152]

Discussions on modalities also addressed the locations of meetings. While formal plenary meetings would ordinarily be convened at United Nations Headquarters in New York,[153] some proposals advocated flexibility for informal and/or intersessional meetings.[154] This could include convening working groups at other United Nations regional offices (e.g. Bangkok, Geneva or Nairobi), holding meetings in additional locations,[155] or allowing host countries to organize intersessional sessions.[156] These proposals were frequently linked to considerations of inclusivity, cost-efficiency and broader participation (including capital-based experts and access to relevant institutional ecosystems outside New York). Hybrid participation modalities were also supported.[157] Concerns were raised about avoiding parallel meetings to enable meaningful participation by smaller delegations.[158] The extent of location flexibility for thematic or intersessional work was not addressed in the official outcomes and may resurface during future meetings of the Global Mechanism.

Beyond stakeholder participation, decision-making and location, discussions on modalities also addressed the future mechanism's reporting cycles, adoption of its programmes of work, possible timing of meetings and the procedural steps needed for the mechanism's formal establishment. Various proposals envisaged establishment through a General Assembly

---

149 For example, Nicaragua (session 4, meeting 10); Philippines (session 5, meeting 5); Netherlands (session 5, meeting 5); Brazil on behalf of the IBSA (India, Brazil and South Africa) Dialogue Forum (session 6, meeting 10); Bangladesh (session 6, meeting 10); Malaysia (session 6, meeting 10); South Africa (session 6, meeting 10); China (session 7, meeting 10); Israel (session 8, meeting 5); United Kingdom (session 8, meeting 7); Israel (session 9, meeting 10).

150 For example, Cuba (session 6, meeting 9); Israel (session 6, meeting 10).

151 For example, Submission by Brazil, paragraphs 5, 19.

152 For example, Portugal (session 10, meeting 10).

153 For example, Sri Lanka (session 7, meeting 10); El Salvador (session 7, meeting 10).

154 For example, Bangladesh (session 7, meeting 10); Czechia (session 7, meeting 10); Germany (session 8, meeting 7); France (Session 9, meeting 9); Viet Nam (session 10, meeting 10).

155 For example, Iran (session 7, meeting 10); France (Session 9, meeting 9); Switzerland (session 9, meeting 10).

156 For example, Czechia (session 7, meeting 10); Viet Nam (session 10, meeting 10).

157 For example, Argentina (session 8, meeting 7); Singapore (session 9, meeting 9); Indonesia (session 9, meeting 10); Argentina (session 9, meeting 10); China (session 10, meeting 10).

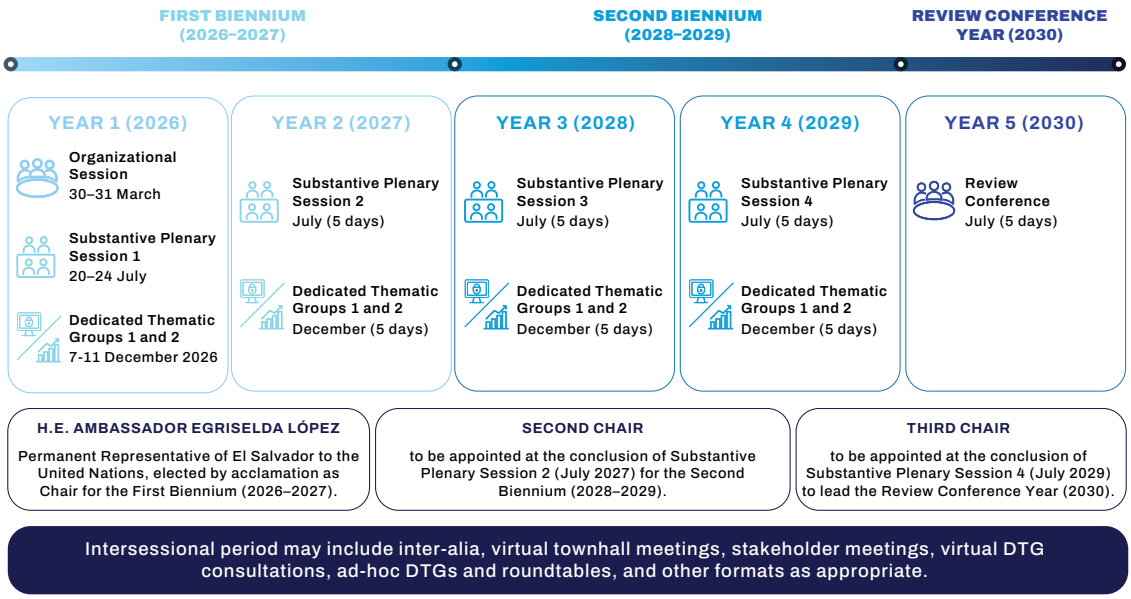
158 For example, Chile (session 9, meeting 10).

resolution, a decision or a dedicated conference.[159] Across these discussions, debate centred on how agreed principles should be translated into detailed operational arrangements.

The final design of the Global Mechanism established a five-year operational cycle structured around three leadership periods, annual substantive plenary sessions, DTG meetings and a periodic review conference, while also leaving space for intersessional consultations and additional working methods and practices to emerge over time (see Figure 5).

FIGURE 5.

The five-year cycle of the Global Mechanism[160]



159 Resolution 77/36; resolution 77/37.

160 The specific months shown for 2027–2030 are indicative and will be set by the Global Mechanism.

4. Insights beyond the official outcomes

This section distils key lessons from the negotiations by examining the challenges that complicated convergence, the practices that enabled consensus and the implications of these dynamics for the operation of the Global Mechanism.

4.1. Challenges

A first challenge stemmed from competing visions regarding how RID should be organized. Proposals for a PoA, a renewed or permanent OEWG-type process, or various hybrid arrangements integrating both proposals reflected deeper differences among States over the future trajectory of the Framework, particularly the balance between implementation and further normative or legal development. These differences were not merely procedural, but were substantive in nature, which made convergence on future RID more complex and, at times, slowed progress.

A second challenge concerned stakeholder participation, which emerged early as a procedural fault line and remained sensitive throughout the negotiations. Diverging views on how and to what extent non-governmental actors should be involved reflected broader questions about the intergovernmental character of the process, inclusivity and trust. The ongoing sensitivity and contentious nature of the stakeholder participation question throughout the OEWG process illustrated how procedural questions could become focal points for broader political differences.

A third challenge related to the tension between the ambitions of individual States and the requirement for consensus of the broader United Nations membership. Proposals that sought to introduce more ambitious programmatic activities (e.g., operationalizing a mechanism for attribution, detailed review of national implementation of the Framework, or specific mandates to facilitate development of additional norms or legally binding obligations) did not attract consensus by the end of the OEWG and were either deferred or excluded from agreed texts. This reflected a broader dynamic in United Nations negotiations whereby the requirement for consensus constrained the level of specificity and ambition that could be reflected in the Global Mechanism's institutional design.

A fourth development shaping the negotiations was the concurrent adoption of two General Assembly resolutions during the OEWG 2021–2025 negotiation cycle, which created a real possibility of dual-track processes following the conclusion of the OEWG. This prospect generated sustained pressure from many delegations to consolidate discussions within a single inclusive mechanism. In turn, the preference for a single-track process influenced both the direction and the pace of convergence, reinforcing efforts to avoid fragmentation and to anchor future RID within a single institutional framework.

4.2. Good practices and lessons learned

Despite these challenges, several good practices enabled States to gradually converge on a common institutional design.

First, a structured and step-by-step approach to negotiations proved useful. The Chair's use of guiding questions and phased discussions allowed States to move from initial positional exchanges towards more focused engagement on specific design elements. While early stages of the process provided space for delegations to articulate and defend their individual preferences, subsequent phases progressively focused discussions on core objectives, guiding principles, structure and modalities, and the thematic focuses of the DTGs. This step-by-step approach helped manage complexity and reduced the risk of early deadlock by avoiding the need to resolve all issues simultaneously. In practice, the Chair structured early outcomes around areas of convergence (i.e., guiding principles), while more difficult issues were addressed at a later stage of the negotiations (i.e., the focus of substantive work in the DTGs), which allowed agreement to build incrementally.

Second, the use of bridging formulations played an important role in enabling agreement, particularly in overcoming entrenched positions linked to specific institutional proposals. Over time, labels such as "Programme of Action" or "OEWG-type process" became associated with distinct political orientations. The gradual shift towards more neutral formulations, including references to a "permanent mechanism", helped depoliticize the debate. At the same time, composite language used in Annex C of the third APR – such as "open-ended", "action-oriented" and "permanent" – alongside references to flexibility and evolution of the permanent mechanism allowed different priorities to be reflected within a single framework. These formulations did not resolve underlying differences, but they did provide sufficient common ground for consensus by accommodating multiple interpretations and expectations.

Third, convergence was facilitated by a consolidation of elements drawn from different proposals. Through successive iterations, the Chair introduced composite formulations that helped bridge divisions. Rather than selecting a single model, States were able to combine elements from across existing proposals. The resulting Global Mechanism reflects some features associated with the PoA (e.g., an emphasis on implementation and periodic review) alongside elements associated with the OEWG format (e.g., inclusivity, plenary sessions and a State-led process). This integrative approach allowed States to move beyond binary choices and to focus on practical arrangements that could command broader support.

Fourth, the design of the Global Mechanism itself incorporated flexibility as a means of enabling consensus. While specific proposals for dedicated thematic groups that focused exclusively on implementation or negotiating new norms did not command consensus, the agreed structure allows for consideration of both objectives in the future. At the same time, the absence of specific DTGs on these issues does not preclude discussions on these issues within the Global Mechanism. This flexibility enabled States to support the overall design while preserving the possibility of advancing their priorities at a later stage.

Finally, the introduction of cross-cutting, policy-oriented thematic groups represents an innovation that may facilitate evolution of discussions beyond structured exchanges in plenary settings. By structuring work around integrated themes, such as capacity-building and ICT challenges, the Global Mechanism creates space for more focused, and potentially more technical, engagement across all pillars of the Framework.

4.3. Implications for the Global Mechanism

The outcome of the OEWG 2021–2025 have four main implications for the Global Mechanism on ICT Security: an "architecture-first" outcome; built-in flexibility; enhanced inclusiveness; and an integrated and cross-cutting nature of DTGs.

First, the OEWG negotiations resulted in an "architecture-first" outcome. States reached agreement on the structure, guiding principles and procedural modalities of the Global Mechanism, while leaving the precise nature and prioritization of substantive work within the DTGs open to further clarification. To some extent, negotiations on RID focused more on designing an inclusive and durable process than on defining in detail the concrete outcomes that the mechanism should ultimately deliver for international peace and security in cyberspace. This reflected both the complexity of reconciling different preferences and the need for strategic ambiguity. Such ambiguity enabled consensus around the mechanism's establishment despite continued differences regarding substantive priorities, including implementation, further normative development and operational cooperation. While this flexibility facilitated agreement on the Global Mechanism's design, it also means that the mechanism's long-term relevance and added value may depend less on its formal architecture. Rather, they will depend on how States choose to use it in practice and whether they are able to translate process continuity into substantive progress on ICT security and cyberspace stability over time.

FIGURE 6.

Timeline of institutionalization of United Nations discussion on international ICT security, transition of the global mechanism, 2025–2026[161]

161 Acronyms used in the figure: GGE - Group of Governmental Experts, OEWG - Open-ended Working Group, POA - Programme of Action, RID - Regular Institutional Dialogue, UNGA - United Nations General Assembly.

Second, and relatedly, flexibility is embedded as a core feature of the Global Mechanism. The inclusion of periodic review cycles and the possibility to establish or adapt thematic groups over time will allow the mechanism to evolve in response to the changing ICT threat landscape and the needs and priorities of Member States. At the same time, this flexibility may also lead to uneven progression of substantive work across the pillars of the Framework depending on levels of political will and Member States' convergence.

Third, the consolidation of discussions within a single-track, inclusive Global Mechanism responds directly to earlier concerns about fragmentation of United Nations processes on international aspects of ICT security. By establishing a single standing intergovernmental platform under the auspices of the General Assembly, States have created a durable architecture for ongoing dialogue on ICTs in the context of international security. While this may increase coherence within the United Nations system and reduce the risk of contentious General Assembly votes over mandate renewals, it may also generate greater expectations on the Global Mechanism to deliver meaningful outcomes.

Finally, the integrated and balanced nature of the agreed design reflects a key milestone in multilateral cyber diplomacy. The Global Mechanism combines permanence with adaptability, inclusivity with State leadership, and broad thematic scope with selective prioritization of activities for each of its five-year working cycles. In this sense, it is not designed to eliminate differences among States, but to provide a structured and sustainable framework within which those differences can be managed and, where possible, reconciled over time.

At the same time, several operational and procedural elements of the Global Mechanism remained only partially clarified at the conclusion of the OEWG mandate. These were left for further elaboration during the organizational session of the Global Mechanism in March 2026 and the subsequent operationalization phase. These include the frequency and sequencing of reporting by the DTGs to the plenary sessions and by the plenary to the General Assembly, the location of meetings, leadership and facilitation arrangements for the two initial DTGs as well as their working methods, expected outputs, and the role and use of intersessional periods for advancing DTGs work. Questions may also arise regarding the financial and institutional resources required to sustain the Global Mechanism over time, including how to support broad and meaningful participation by all Member States, particularly when engagement may require technical expertise and participation from capital-based experts beyond permanent missions in New York.

Overall, the consensus agreement to establish a permanent Global Mechanism on ICT Security reflects collective recognition that governance of ICT-related security challenges requires sustained focus, inclusivity and structured flexibility. In this sense, the Global Mechanism is both the product of past negotiations and a framework for future ones, embedding international ICT security discussions within a stable yet flexible institutional United Nations architecture.

Cross-sectional analysis and conclusions

Dr Samuele Dominioni and Dr Giacomo Persi Paoli

In the previous chapters, the authors identify key issues across the six agenda items of the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025. To identify some key factors that characterized States' negotiations during the OEWG, this chapter conducts a cross-cutting analysis of all of its sessions. Among these, it is possible to identify some factors that characterized the discussions across some or all sessions and agenda items, including broader trends observable in the evolution of the discussions and major themes (Section 1). Subsequently, the chapter looks at factors that facilitated consensus (Section 2) and those that prevented a more ambitious outcome (Section 3). Finally, the chapter closes with some concluding reflections (Section 4).

1. Key trends from the discussions

At least three trends largely underpinned the discussions throughout the OEWG 2021–2025.

From reaffirmation to anchored discussions

For most of the agenda items, States spent the early sessions of the OEWG 2021–2025 reaffirming the work of the previous OEWG and the six Groups of Governmental Experts (GGEs) on information and communications technology (ICT) security. In their statements, States stressed that the OEWG 2021–2025 did not commence from a blank slate and also acknowledged and reaffirmed the relevance, importance and cumulative nature of the framework of responsible State behaviour in cyberspace. Subsequently, in later sessions, States began discussing newer proposals, including some very specific ones (e.g., the establishment of the Global Intergovernmental Points of Contact (POC) Directory or the Chair's voluntary checklist for norms implementation), which anchored discussions in operationalization and implementation.

From general to grounded discussions

Similarly, States progressed from discussing substantive themes from a more general, abstract standpoint to a more reality-grounded perspective throughout the sessions. This trend was driven by several factors, including key external events and an increase in delegations' capabilities.

Among the external events that affected States' discussions were major incidents with an impact on international peace and security. These included the war in Ukraine, the pager explosions in Lebanon and the Syrian Arab Republic, and the SolarWinds malicious incident. There were also major technological breakthroughs, such as the fast global diffusion of large language models (e.g., OpenAI's ChatGPT) and advancements in quantum computing. All these external factors led States to address specific issues in a more grounded and informed way.

At the same time, delegations became better able to engage substantively in negotiations. Simulations and exercises served as one factor that helped States address and better understand specific issues through scenario-based practice. These included how international law applies to State use of ICTs[1] and how to practically engage with the Global POC Directory in case of an incident.[2]

Inclusivity and representation

A few trends can be observed in terms of inclusivity and representation throughout the OEWG 2021–2025.

The first concerns the overall number of States that took the floor across the 11 sessions, which increased moderately (see Figure 1). Breaking this data down by United Nations regional group (see Figure 2) shows a notable increase in the number of African States that intervened in the OEWG sessions, with a surge during the third (sessions 4–5) and fourth cycles (sessions 6–8). In some instances, the figure doubled. A smaller increase is observable among Eastern European States. In contrast, States of Latin American and the Caribbean and in the Western European and Others Group showcase a slightly opposite trend, with, on average, fewer States taking the floor during the fourth cycle. Asia-Pacific States varied less in the number of times that they took the floor across all the sessions. Moreover, it is possible to observe that more States took the floor during the substantive sessions (i.e., 1, 2, 4, 6, 7, 9, 10) than during the negotiation sessions (i.e., 3, 5, 8, 11). Overall, it is important to note that these numbers reflect only States that took the floor and do not include States that aligned with statements made by groups or regional organizations (e.g., the European Union).

1 In particular, UNIDIR conducted the workshop "International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities" in Geneva on 15 November 2023. See UNIDIR Security and Technology Programme, "International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities", Workshop summary, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNIDIR_International_Law_and_the_Behaviour_of_States_in_the_Use_of_ICT.pdf.

2 Office for Disarmament Affairs, "Simulation Exercise to Support State Participation in the Global Points of Contact Directory", ODA/2024-0017, 18 November 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20241118_NV-MS_support_Nov_2024.pdf.

FIGURE 1.

Number of States that took the floor, by OEWG session

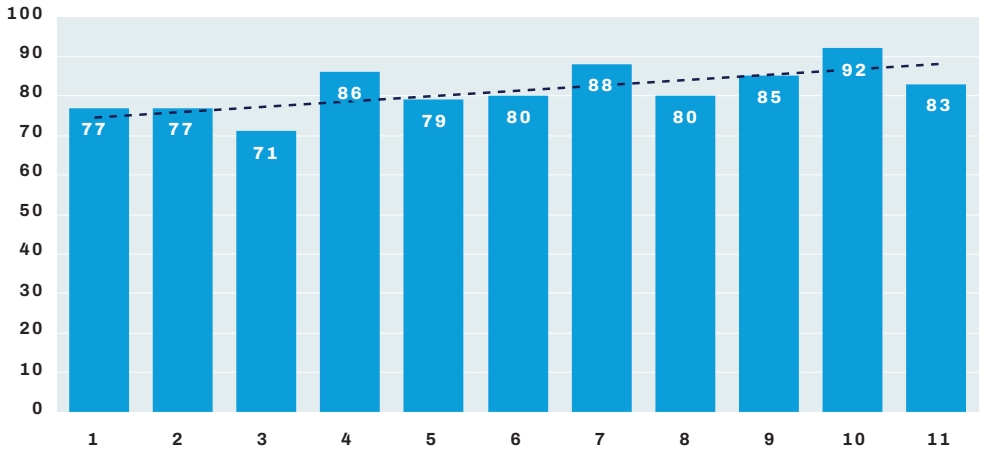
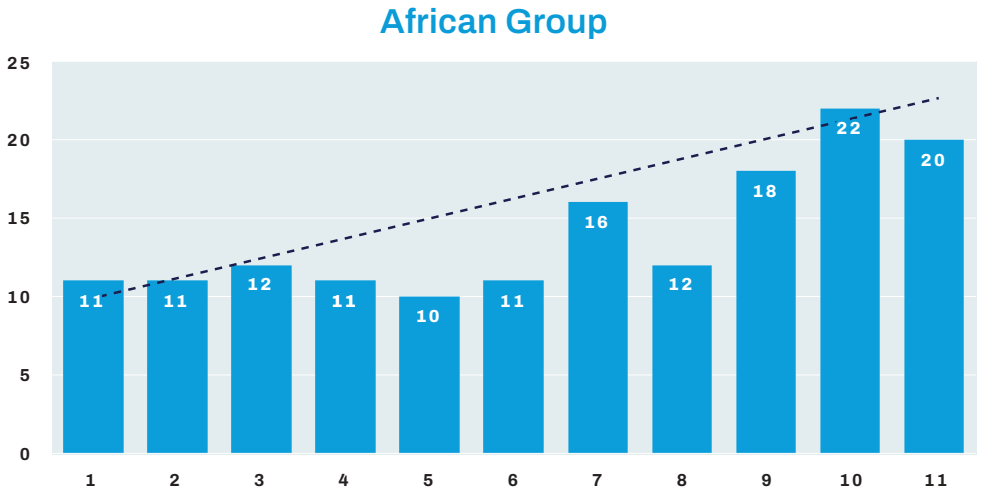
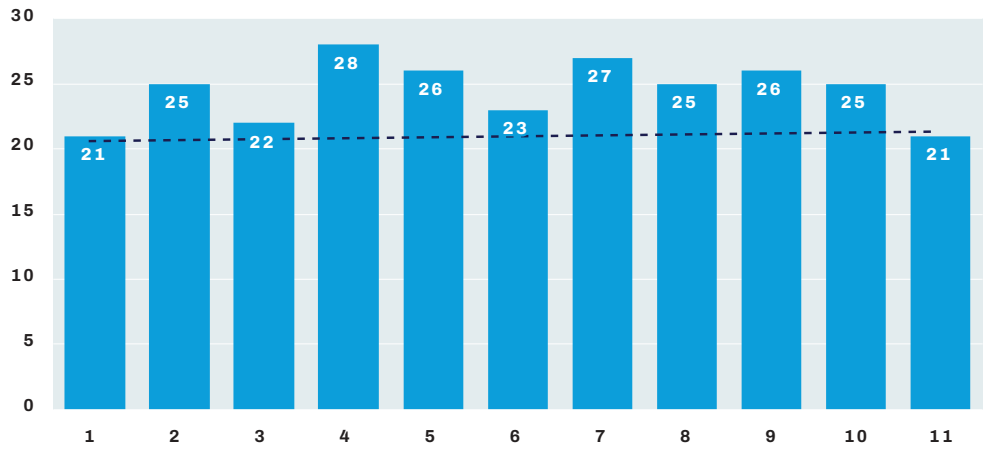


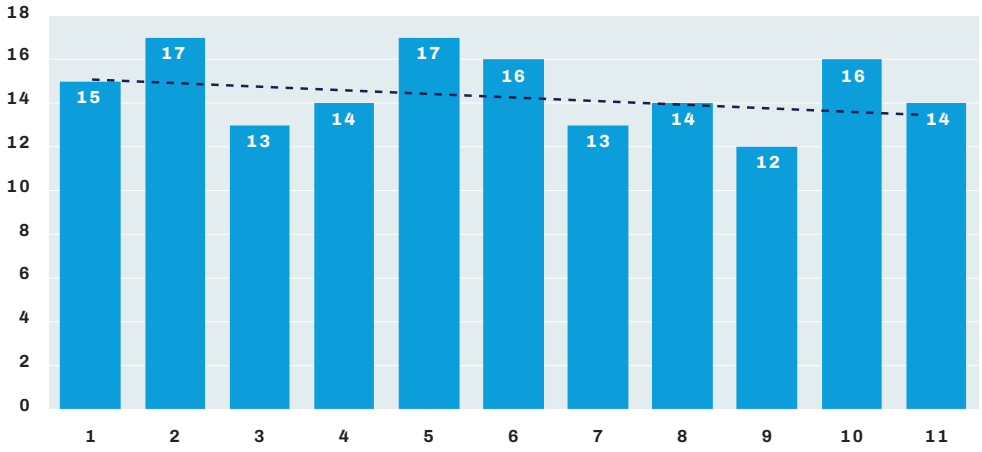
FIGURE 2.

Number of States that took the floor, by United Nations regional group

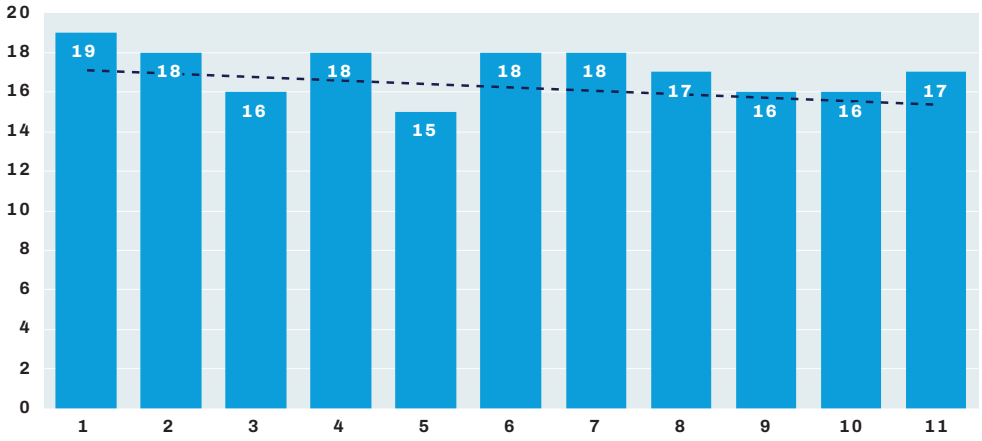




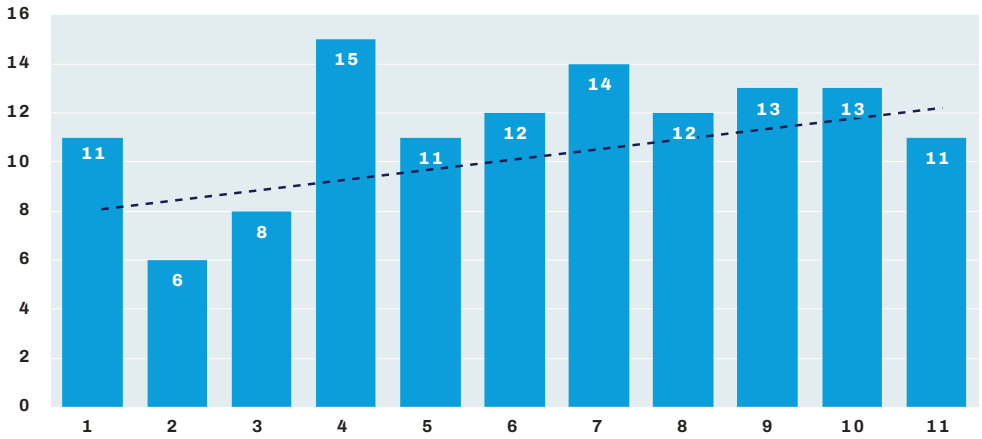
GRULAC



WEOG



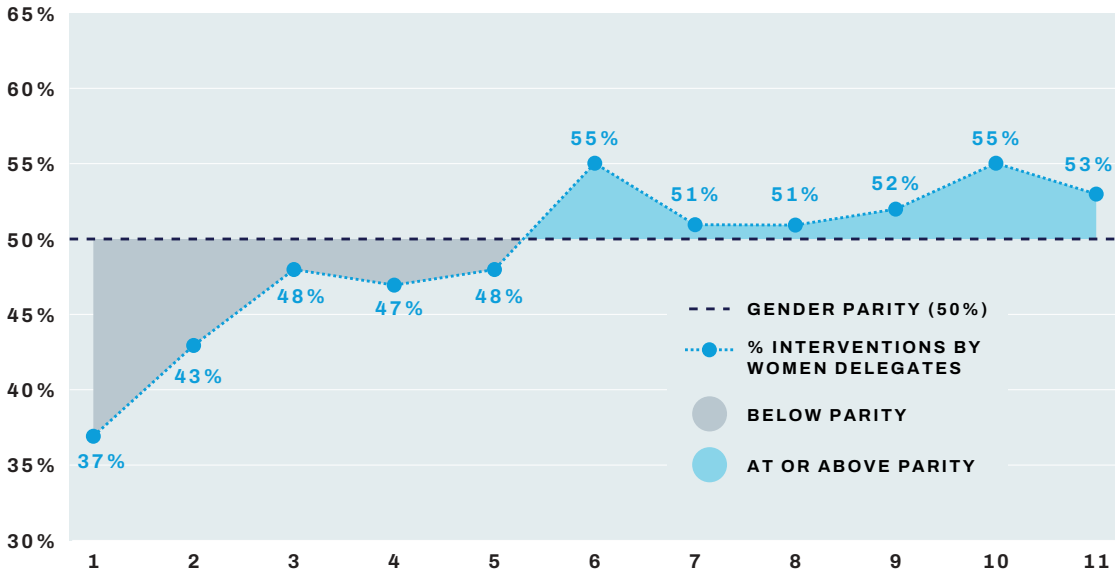
Eastern European Group



Another trend related to inclusivity and representation concerns the participation of women delegates: there was a marked increase in the number of women delegates taking the floor throughout the sessions. Indeed, there was a sharp increase from 37 percent in session 1 to a peak of 55 percent in session 6, and it remained above 50 percent in all subsequent sessions (see Figure 3).

FIGURE 3.

Proportion of interventions made by female speakers, by session



Overall, data concerning representation – geographical and gender – showcases positive trends throughout the sessions. Initiatives such as the Women in International Security and Cyberspace (WiC) Fellowship[3] played a direct role in this regard.

1.2. Cross-cutting topics

As outlined in the individual chapters of this volume, States addressed a wide variety of issues during the sessions of the OEWG 2021–2025, and some of these issues emerged in discussions under more than one agenda item. It would be impossible to capture all the cross-cutting topics here, but three that recurred most often are capacity-building, the multi-stakeholder approach, and protection of critical infrastructure.[4]

---

3 The WiC Fellowship is a capacity-building initiative and institutional support programme designed to strengthen the knowledge and skills of a group of women delegates and leaders from all regions on international cybersecurity and to support their full and meaningful participation in the OEWG sessions. See UNIDIR, "UNIDIR Delivers Training to Women in Cyber Fellows in New York", 15 August 2025, https://unidir.org/unidir-delivers-training-to-women-in-cyber-fellows-in-new-york/.

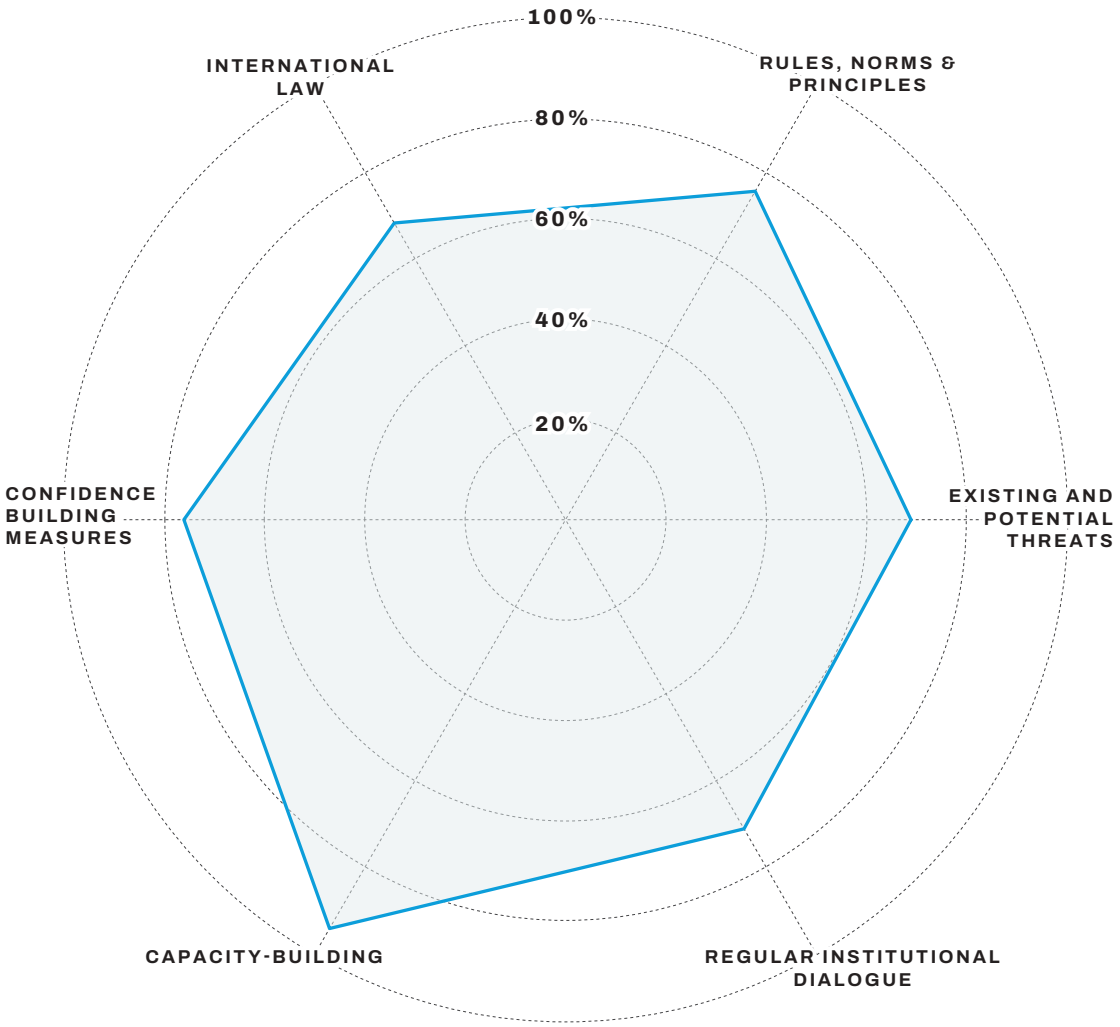
4 These topics have been selected based on observation of the most recurring issues raised during States' interventions. Subsequently, the relative prominence of the topics was determined using a keyword-dictionary-based search of interventions for each agenda item. Topics with relative prominence of at least 40 per cent across at least three agenda items are included here. Other topics considered included transparency, information-sharing, trust, sovereignty and gender.

Capacity-building

Despite there being an agenda item dedicated to capacity-building, States regularly referred to capacity-building activities across other agenda items (see Figure 4). For example, under the agenda item on confidence-building measures (CBMs), soon after States agreed to establish the Global POC Directory, they began discussing capacity-building issues to support the engagement of POCs in the directory.

FIGURE 4.

Proportion of interventions referencing capacity-building, by agenda item

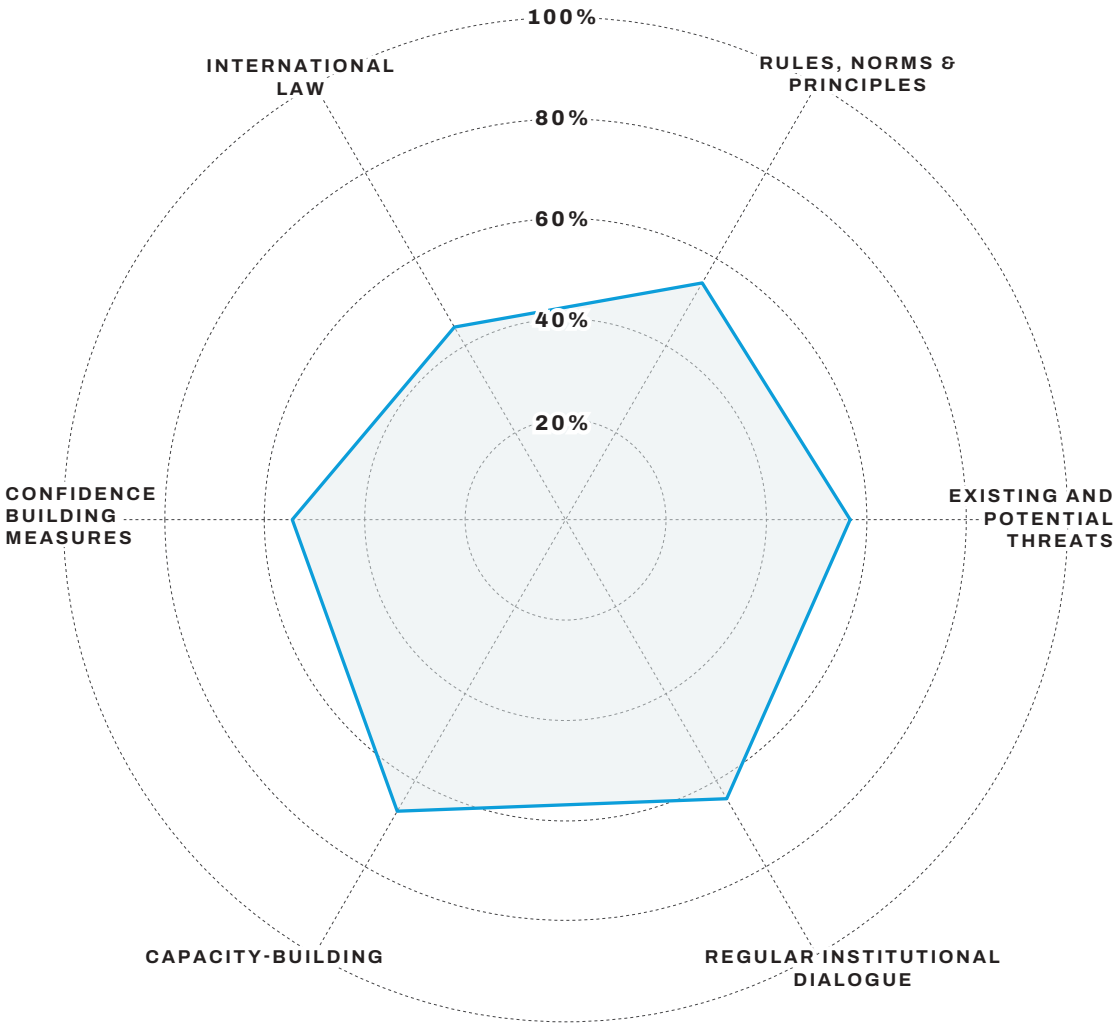


Multi-stakeholder approach

States addressed the issue of multi-stakeholders, including the participation of non-governmental actors in the OEWG, from the very beginning of the process. Despite being a contentious topic, many States referred to and discussed the role, function, and involvement of multi-stakeholders across all agenda items (see Figure 5). As such, the multi-stakeholder approach can be regarded as a continuing and whole-of-framework area of relevance.

FIGURE 5.

Proportion of interventions referencing multi-stakeholders, by agenda item

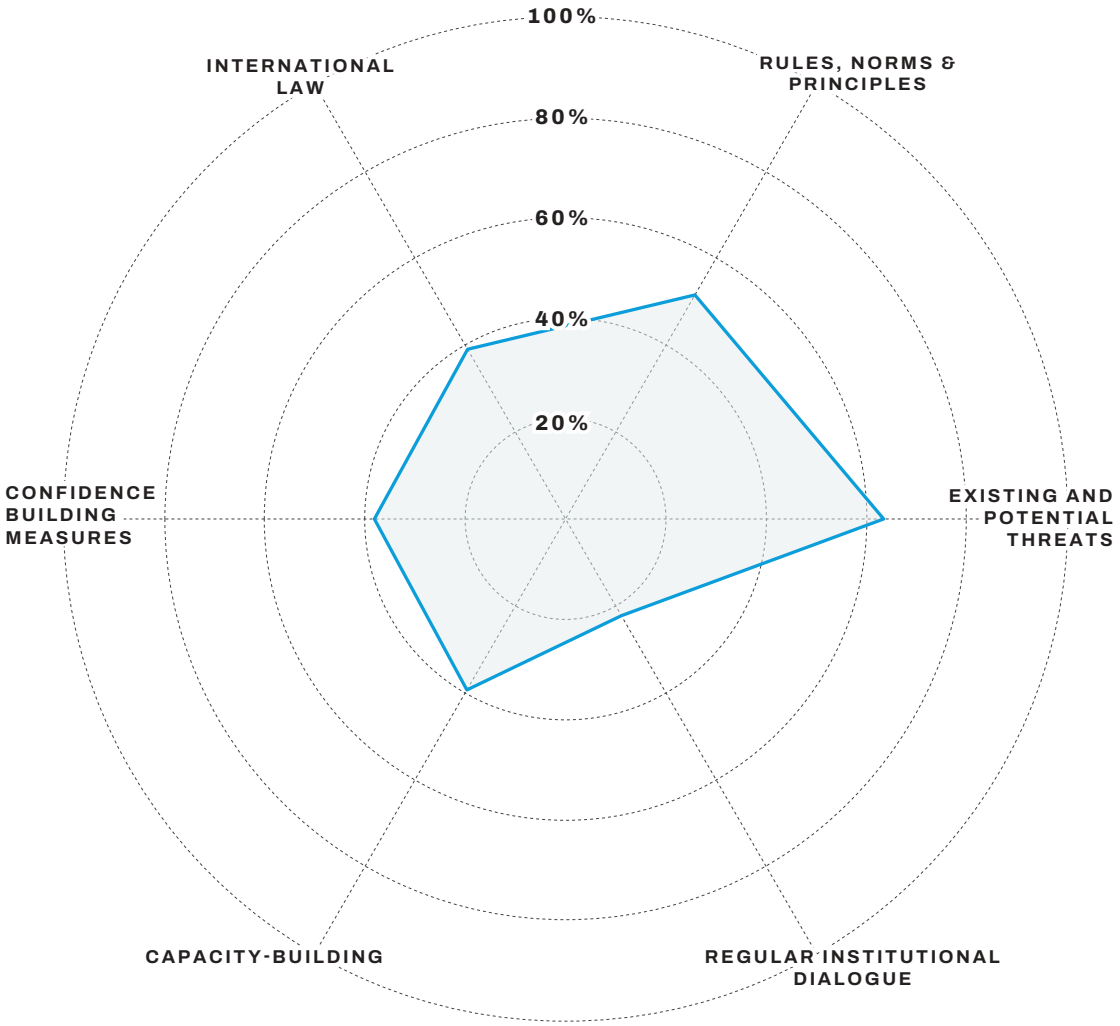


Critical infrastructure protection

The protection of critical infrastructure and critical information infrastructure has been a crucial and "historical"[5] priority for States since the very beginning of multilateral discussion on responsible behaviour in the ICT environment, and it was one of the top priorities for States throughout the OEWG 2021–2025. This topic emerged in multiple discussions across the different agenda items, particularly when discussing existing and potential threats and in the context of rules, norms and principles (see Figure 6).

FIGURE 6.

Proportion of interventions referencing critical infrastructure protection, by agenda item



5 The issue of protecting the integrity of infrastructure was already mentioned in the resolution establishing the first GGE. See General Assembly, resolution 58/32, "Developments in the Field of Information and Telecommunications in the Context of International Security", 8 December 2003.

2. What facilitated consensus

Analysis of the different agenda items also reveals that discussions, including substantive ones, often featured a diverse set of views and positions on multiple themes. Achieving consensus on the three annual progress reports (APRs) and the final report was not easy. A few factors can be highlighted as contributing to consensus across the OEWG 2021–2025 cycles.

The work of the delegates

There was intense and sustained work by the delegates who prepared for, substantially discussed, and negotiated the wide variety of items discussed during the 11 sessions. Themes and issues ranged from principles of international law to more technical aspects of existing and potential threats. Moreover, delegations demonstrated flexibility and openness to shared solutions and compromises as they navigated an increasingly tense geopolitical environment.

Moreover, some States worked to bridge contrasting views, to engage in sustained dialogue with States holding divergent views and to find compromise in stalemate situations. The work of these delegations was often a discreet endeavour. Nevertheless, it is an important role that deserves recognition.

Similarly, although outside the scope of this report, the continuous engagement of the multi-stakeholder community – including through written submissions and the organization of side events and informal meetings – helped delegations to better understand certain aspects of ICTs in the context of international security.

The work of the Chair and his team

The Chair, H.E. Ambassador Burhan Gafoor, played a key role in facilitating consensus through a step-by-step approach. This allowed States to take the time to reflect, unpack and address proposals, ideas and negotiation items in a more gradual, incremental manner. The Chair's approach thus enabled States to find common ground on many issues.

A distinct feature of the Chair's step-by-step approach was the use of guiding questions shared with delegations before each session. These questions helped delegations prepare their interventions to address relevant topics featured in the programme of work. As observed in some of the chapters, the chair's guiding questions also helped the debate to progress and to overcome stalemates on specific themes (e.g., multi-stakeholder involvement in capacity-building activities).

Supporting United Nations bodies

A third element that facilitated consensus was the role played by the Secretariat (the Office for Disarmament Affairs) and other supporting United Nations bodies, including UNIDIR and the International Telecommunication Union (ITU). In line with its mandate, the Secretariat

Participants at 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.

provided both administrative and substantive support to the Chair and to the process. For example, technical reports produced by the Secretariat, upon request from States, proved useful tools for States to navigate different positions and contributed to more focused discussions on specific topics.[6]

Moreover, other United Nations bodies (e.g., UNIDIR and ITU) proved to be supportive of States' discussions during the OEWG. UNIDIR, through its research,[7] tools[8] and other activities, including workshops and training for delegates, contributed to expanding States' understanding on a wide variety of issues discussed across the agenda items. ITU provided technical expertise and insights on specific capacity-building aspects and collaborated with the Office for Disarmament Affairs and UNIDIR to organize and deliver the first POC simulation exercise.

Overall, the work of the United Nations bodies helped States navigate complex political, technical, and procedural issues, thereby enabling delegations to engage more substantively and constructively in the consensus-building process.

---

6 See, for example, "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", Paper by the Secretariat, A/AC.292/2024/2, 22 January 2024; "Initial Background Paper on Capacities Required to Participate in a Global, Intergovernmental Points of Contact Directory", Paper by the Secretariat, A/AC.292/2024/3, 29 April 2024; "Initial Report Outlining the Proposal for the Development and Operationalization of a Dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal", Paper by the Secretariat, A/AC.292/2025/1, 14 January 2025.

7 See, for example, Samuele Dominioni and Giacomo Persi Paoli, *Unpacking Cyber Capacity-Building Needs, Part I, Mapping the Foundational Cyber Capabilities* (Geneva: UNIDIR, 2023), https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-i-mapping-the-foundational-cyber-capabilities/; UNIDIR Security and Technology Programme, *Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content* (Geneva: UNIDIR, 2023), https://unidir.org/wp-content/uploads/2023/09/UNIDIR_Drawing_Parallels_Multi_Stakeholder_Perspective_on_Cyber_PoA_Scope_Content_Structure.pdf; UNIDIR Security and Technology Programme, *Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations* (Geneva: UNIDIR, 2023), https://unidir.org/publication/use-of-icts-by-states-rights-and-responsibilities-under-the-un-charter/.

8 See, for example, the UNIDIR Cyber Policy Portal.

3. What prevented a more ambitious outcome

The positive outcomes of the second OEWG are enshrined in the three APRs and the final report. However, on certain agenda items, States did not manage to progress towards more ambitious outcomes; instead, they opted to postpone further negotiations to the new Global Mechanism on ICT Security. The analysis of some of the causes reveals three main factors.

Developing or implementing the framework

A recurring point of disagreement among States centred on whether the negotiations should focus on developing new elements of the framework of responsible State behaviour or on implementing the existing ones. This disagreement slowed down the discussions, particularly those under the agenda items on rules, norms, and principles, and on international law. As some States noted, these two approaches are not necessarily mutually exclusive, as the development of new elements can benefit from the implementation of existing ones.

The difficult international security environment

The international security environment in which States had to negotiate during the 11 sessions became increasingly difficult, marked by multiple crises including the outbreak of inter-State conflicts. This trend was particularly reflected in the negotiations on the agenda items on existing and potential threats, international law, and regular institutional dialogue.

States' caution

A third factor that hampered the achievement of a more ambitious outcome was States' reluctance and caution in developing more substantive and meaningful elements to implement or further advance the framework. In particular, on different occasions, States cautioned that these elements might raise sovereignty-related concerns, particularly insofar as they could be seen as intruding into or interfering with matters falling within national jurisdiction. This trend was particularly evident in confidence-building measures and capacity-building.

4. Conclusion

The conclusion of the OEWG 2021–2025 does not mark the end of multilateral discussions on ICTs in the context of international security. Rather, it represents a transition from time-bound negotiations to a more sustained phase of institutionalized dialogue in the Global Mechanism. In this respect, some of the most important legacies of the OEWG 2021–2025 lie in the working methods, good practices, and expertise that emerged throughout its mandate, in addition to the consensus outcomes that it produced.

The discussions demonstrated that progress remains possible even in a difficult international security environment, provided that delegations are given sufficient time, guidance, and support to engage with one another. The step-by-step approach adopted during the OEWG allowed States to move gradually from the reaffirmation of existing commitments towards more focused discussions on implementation, operationalization, and future institutional arrangements. This approach proved particularly useful in areas where positions remained divergent, as it enabled States to identify meaningful areas of convergence without requiring all underlying disagreements to be resolved at once. Ultimately, the OEWG (2021–2025) reaffirmed that international cooperation on ICT security is both necessary and possible. Its work underscored the value of dialogue, compromise, and incremental progress in advancing a common understanding among States.

The Global Mechanism on ICT Security inherits both the achievements and the unresolved questions of the OEWG 2021–2025. It will provide an opportunity for States to continue engaging in the implementation and operationalization of the agreed framework and to continue addressing areas where consensus has not yet fully emerged. To do so effectively, it will be important to preserve institutional memory of the path already travelled, ensuring that the progress achieved so far continues to guide multilateral efforts ahead.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais des Nations
1211 Geneva, Switzerland

UNIDIR.ORG