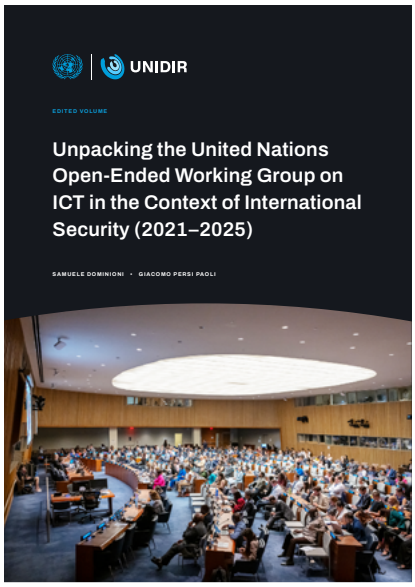
Chapter title **Rules, norms and principles of responsible State behaviour**

Chapter author **Dr Andraz Kastelic**



Extracted from the UNIDIR publication:

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

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.

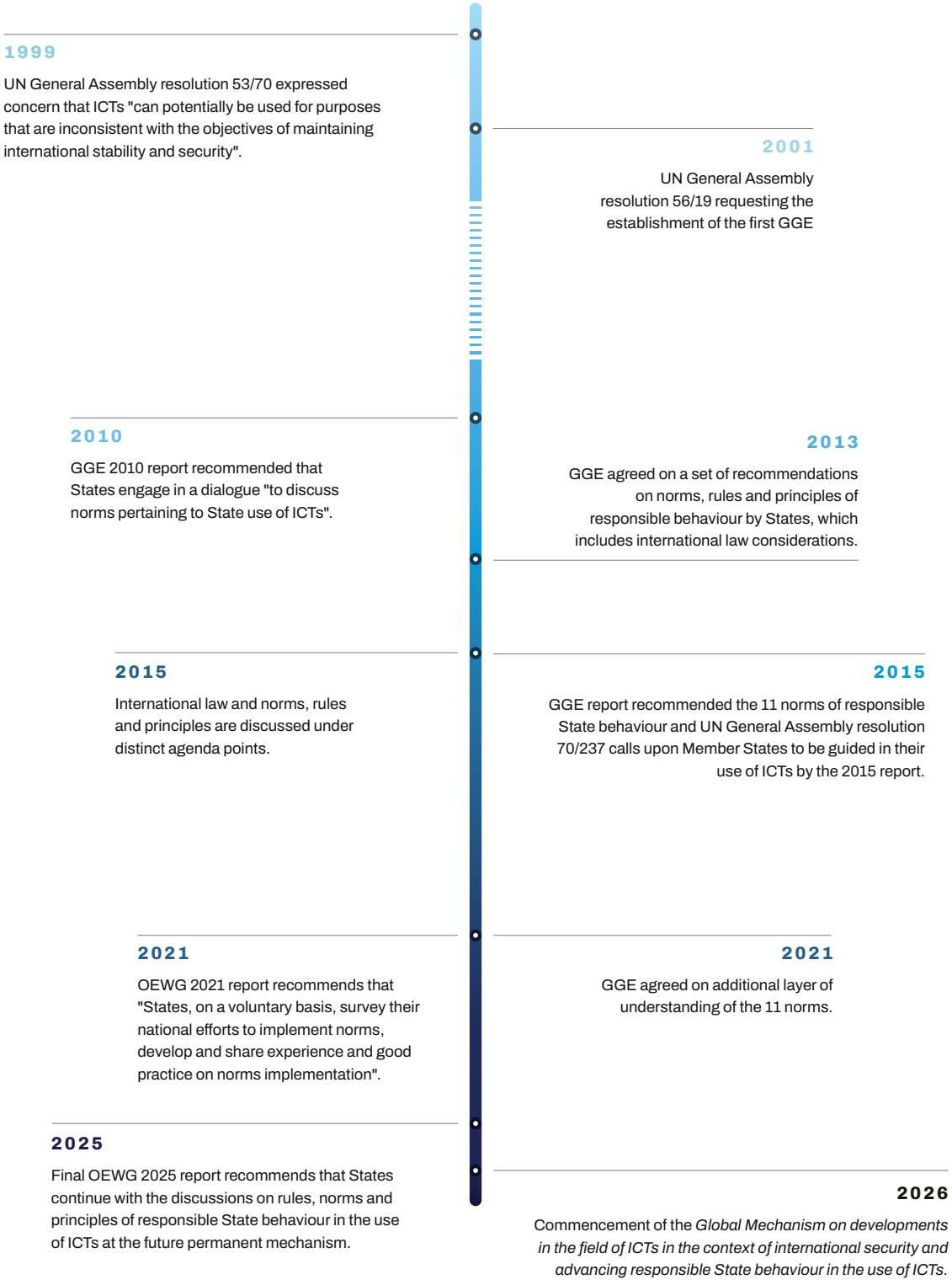
19 A/79/214; A/80/257.

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).

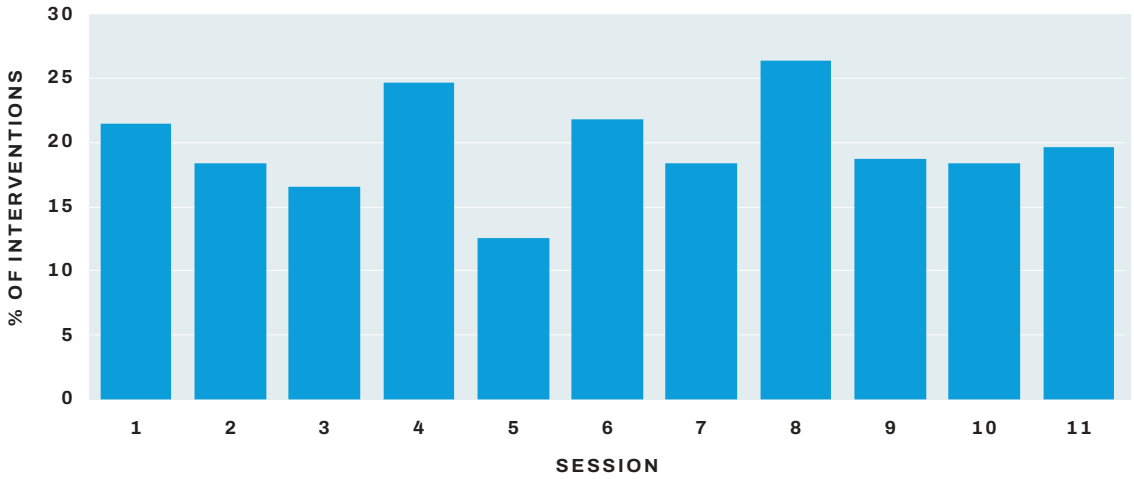
The third APR acknowledged that, while States had discussed new norms, they had not reached consensus on any of them; the report noted that "several proposals were put forward for possible new norms which are still being discussed by States".[49] In addition to the commitment to continue discussing existing 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).

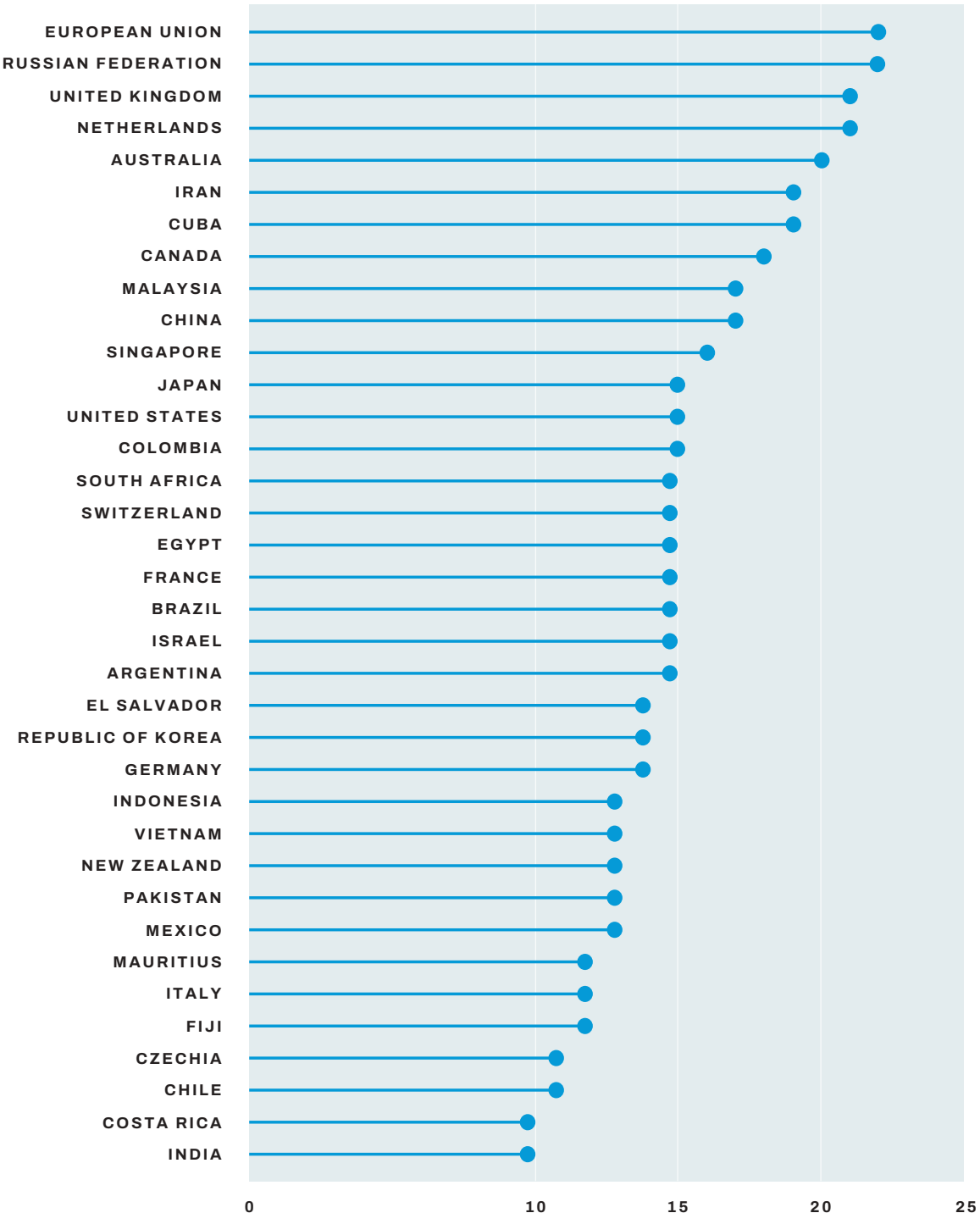
52 Contrast, for example, Pakistan (session 10, meeting 3) and Cuba (session 10, meeting 3) against the United States (session 9, meeting 4) and Israel (session 10, meeting 3).

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		