DiPLO

OEWG and Cybersecurity Negotiations at the United Nations:

Issues, Dynamics, and Divides

Andrijana Gavrilovic | Stefania Grottola | Pavlina Ittelson
Anastasiya Kazakova | Salome Petit-Siemens | Vladimir Radunovic
Jeanne-Louise Roellinger | Ilona Stadnik

DIPLOMACY AND TECHNOLOGY

OEWG and Cybersecurity Negotiations at the United Nations

Issues, Dynamics, and Divides

Andrijana Gavrilovic

Stefania Grottola

Pavlina Ittelson

Anastasiya Kazakova

Salome Petit-Siemens

Vladimir Radunovic

Jeanne-Louise Roellinger

Ilona Stadnik

OEWG and Cybersecurity Negotiations at the United Nations

Publisher
DiploFoundation (2025)
www.diplomacy.edu
diplo@diplomacy.edu

Authors: Andrijana Gavrilovic, Stefania Grottola, Pavlina Ittelson, Anastasiya Kazakova, Salome Petit-Siemens, Vladimir Radunovic, Jeanne-Louise Roellinger, Ilona Stadnik

Design and layout: Viktor Mijatovic

KaiZen publishing

This book uses the KaiZen publication approach, which draws inspiration from the Japanese word Kaizen, meaning continuous improvement. Publication evolves in real-time through a blend of human expertise and AI updates. Once a year, the author consolidates updates into a new version of the printed publication.

KaiZein version: July 2025

ISBN 979-8-9898028-1-4

Note to readers: This publication comprises analyses written by our team of experts spanning 2021-2025. It brings together previously written texts, grouped thematically but presented in their original form, preserving the context in which they were written. This format allows readers to trace the evolution of negotiations on each topic and gain insight into how positions and dynamics unfolded over time.

Table of contents

Introduction

A brief history of UN discussions on cyber aspects of international peace and security

The First Committee of the UN has been home to deliberations about the cyber aspects of international peace and security since the late 1990s. In 1998, the Russian Federation introduced the draft resolution on Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the UNGA, which was adopted without a vote (A/RES/53/70).[1]

Growing recognition among states of escalating threats emerging from cyberspace prompted the establishment of the UN Group of Governmental Experts (GGE) in 2004.[2] The GGE consisted of experts from several states suggested by the Office of the High Representative for Disarmament Affairs to the Secretary-General who decides, taking into account not only geographical and political balance, but a demonstrated interest in the topic, the number of times a country has served on other GGEs, whether they are currently serving on a different GGE. Although the initial GGE concluded its work without producing a final report, its mandate was subsequently renewed multiple times: 2009–10, 2012–13, 2014–15, 2016–17, and 2019–21 (together referred to as the GGEs).[3]

In 2010, the GGE produced a report which contained recommendations for further dialogue among states to reduce the risk and protect critical national and international infrastructure; confidence-building, stability and risk reduction measures; information exchanges on national legislation and strategies, and capacity-building measures; elaboration of common terms and definitions related to information security, and capacity-building in less developed countries.[4]

A breakthrough occurred in 2013 when the final report of the GGE (adopted by consensus of the, then 15, countries of the GGE) confirmed the agreement of the participating states that 'international law, and in particular the UN Charter, is applicable and is essential to

[1] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/53/70) adopted 4 January 1999, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F53%2F70&Language=E&DeviceType=Desktop&LangRequested=False.
[2] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/58/32) adopted 18 December 2003, https://dig.watch/resource/resolution-ares5832-developments-field-information-and-telecommunications-context-international.
[3] Digital Watch Observatory, 'UN Group of Governmental Experts and Open-Ended Working Group Processes,' accessed 1 August, 2025, https://dig.watch/processes/un-gge
[4] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/65/41), adopted 8 December 2010, accessed 5 August, 2025, https://dig.watch/resource/un-gge-report-2010-res-a65201.

maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment.'[5]

The 2015 GGE report was another breakthrough document: 20 countries represented in the GGE, including the USA, China, Russia, France, the UK, and Germany, specified the voluntary and non-binding normative framework of state behaviour, and agreed on a set of voluntary norms. The UNGA subsequently endorsed all the reports in the form of resolutions.[6]

The 2016–17 GGE, which was expanded to include 25 countries, was unable to reach a consensus on its final report due to, in particular, the disagreement over what options states have to respond to cyberattacks (i.e. the right to respond to wrongful international acts and the right to self-defence under Article 51 of the UN Charter).[7]

In 2018, the UNGA adopted two resolutions (one sponsored by the USA (A/RES/73/266), the other by Russia (A/RES/73/27)), which set in place two mechanisms for discussing the applicability of international law to cyberspace, and the further development and implementation of voluntary norms.[8] The first resolution set up the continuation of the GGE in 2019–21. The second resolution established the UN Open-Ended Working Group (OEWG) for 2019–20, which was open to all interested UN member states, allowed inputs from other stakeholders, and reported directly to the UN Secretary-General. While the GGE and the OEWG worked in parallel throughout 2019 and 2020 in somewhat different settings, considerable cooperation between the chairs of the two groups was established, and many countries played an active and constructive role in both.

---

[5] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/68/243) adopted 27 December 2013, https://dig.watch/resource/un-gge-report-2013-a6898.

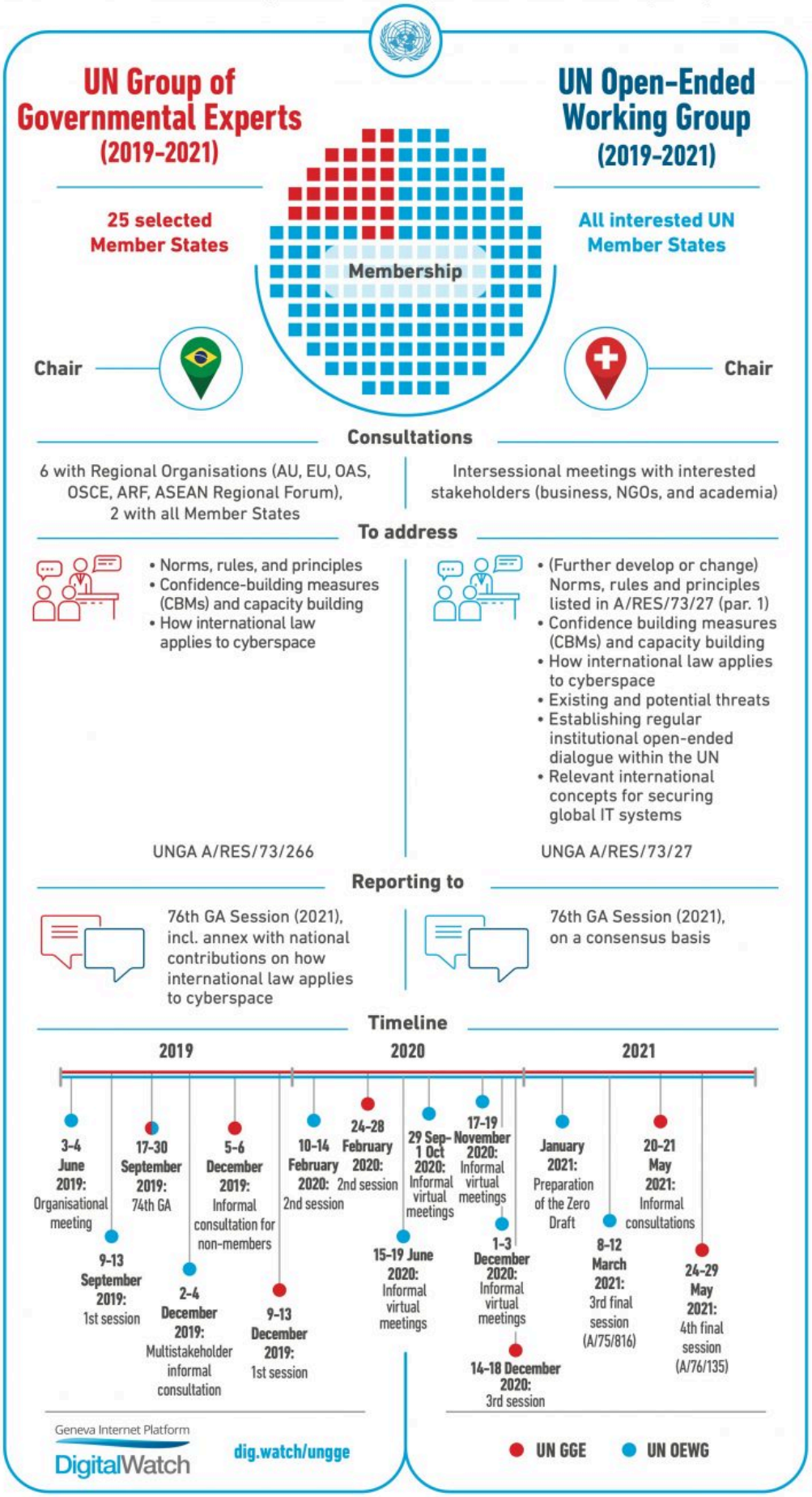
[6] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/70/174, adopted 23 December 2015, https://dig.watch/resource/2015-un-gge-report-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-a-res-70-174.

[7] Digital Watch Observatory, 'UN GGE: Quo Vadis?' *Digital Watch newsletter – Issue 22 – June 2017*, https://dig.watch/newsletter/june2017#UN-GGE-Quo-Vadis-.

[8] United Nations General Assembly, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/RES/73/266) adopted 5 December 2018, https://dig.watch/resource/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international, and United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security* (A/RES/73/27) adopted 5 December 2018, https://dig.watch/resource/un-ga-resolution-establishment-oewg-ares7327.

Comparative Survey

of the two UN-based processes on responsible behaviour in cyberspace



In December 2020 – before the end of the mandate of the first OEWG – the OEWG was renewed for a period of five years, i.e. 2021–25 (A/RES/75/240). The OEWG remained open to all interested states and decided based on consensus. Organisationally, it could have decided to establish thematic subgroups and to 'interact, as appropriate, with other interested parties, including businesses, non-governmental organisations and academia.'[9] Importantly, the final report of the OEWG 2019–20 recommended that regular institutional dialogue should continue under the auspices of the UN, including the 2021–25 OEWG, with equal state participation, although opening the door for other types and formats of processes, also.

OEWG 2019-2020 concluded in March 2021, adopting a final report that reaffirmed the results of the previous reports of the GGE, as well as that international law, and in particular the Charter of the UN, is applicable to cyberspace.[10] The GGE 2019-2020 finished its work in May 2021, reaffirming the acquis, and adding the OEWG 2019-2021 to the acquis. The report also developed an additional understanding of the 11 voluntary GGE 2015 norms, prescribed elements for the attribution of cyberattacks, and encouraged states to consider appointing dedicated PoCs at the policy, diplomatic, and technical levels.[11]

The UNGA Resolution A/RES/76/19 of December 2021, tabled jointly by the USA and Russia along with other countries, which adopted the GGE 2019–21 and OEWG 2019–20 reports, also confirmed the mandate of OEWG 2021–25. This established it as a sole ongoing process of institutional dialogue.[12]

The OEWG 2021-2025 was mandated to 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; to consider initiatives of states aimed at ensuring security in the use of information and communications technologies; to establish, under the auspices of the UN, regular institutional dialogue with the broad participation of states; to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of ICT by states, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the General Assembly at its eightieth session.

---

[9] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/75/240), adopted 30 December 2020, https://dig.watch/resource/developments-field-information-and-telecommunications-context-international-security

[10] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/AC.290/2021/CRP.2) adopted 16 December 2021, https://dig.watch/resource/oewg-2021-report.

[11] Andrijana Gavrilovic, 'What's new with cybersecurity negotiations? The UN GGE 2021 Report,' *DiploFoundation Blog*, 6 June, 2021, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/

[12] United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies* (A/RES/76/19), adopted 6 December 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/48/PDF/N2137748.pdf

In July 2025, the OEWG 2021-2025 finished its mandate. The group adopted its final report, which calls for continued discussions and deepening the understanding of all topics on the OEWG's mandate, including tangible outcomes of the OEWG 2021-2025, such as the Global Points of Contact (PoC) Directory and corresponding Template for Communication. In all of the areas, the final report puts great emphasis on the capacity building efforts in its recommendations for future work.[13]

The report set in place a single permanent mechanism under the First Committee, called 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. The base of this new process was set in the third Annual Progress Report (APR) of the OEWG 2021-2025 (Annex C), with additional modalities set out in the final report.[14] The work of the Global Mechanism is structured in five-year cycles, with two biannual cycles followed by a one-year review cycle. The work will be undertaken in annual substantive sessions, dedicated thematic groups (one general, one on capacity building) and in a review conference every five years. The organisational meeting for the Global Mechanism is scheduled for March 2026, with the first substantive session in June 2026.[15]

[13] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*, July 2025, https://dig.watch/resource/oewg-report-2021-2025.
[14] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR)*, July 2024. https://dig.watch/resource/open-ended-working-group-on-security-of-and-inthe-use-of-information-and-communicationstechnologies-2021-2025
[15] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

Organisational issues

An unsettled start: The organisational session that left key questions hanging

As discussed in June 2021[16]

On 1-2 June 2021, the UN Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies in 2021–2025, ***held its organisational session to determine how and when it will conduct its work.***

The OEWG 2021-2025 started less than three months after the first one finished. Its chair, **Mr Burhan Gafoor**, Ambassador and Permanent Representative of Singapore to the UN in New York, ***was elected with no objections from other delegates*** (in UN-speak: by acclamation).

However, **Gafoor** noted something quite interesting in his first address as the chair of the OEWG: ***he had found out only a few days prior that he was nominated for the post***. Gafoor stated that he hadn't had the time to reach out to as many delegations as he would have wanted. It could explain why the session lasted one instead of two days – the chair might have wished to familiarise himself with the delegations' positions. ***In the end, the organisational session ended with more questions than answers.***

Acting on consensus?

At the very beginning of the session, Russia threw a curveball, suggesting that the organisational note be amended ***to limit the consensus requirement only for the decisions of the cyber OEWG.***[17] Practically speaking, states would not have to agree on procedural and organisational matters unanimously. ***This would allow any country to limit which issues would be on the agenda.***

Still, for the most part, delegates stated that the work of the OEWG would be based on consensus. The chair stated that, as a subsidiary body of the UN General Assembly (UNGA), ***the OEWG will follow UNGA procedural rules, which include acting and taking all decisions on a consensus basis. The states adopted this without objection.***

---

[16] Andrijana Gavrilovic, 'What's New with Cybersecurity Negotiations? The Second Cyber OEWG's Organisational Session,' *DiploFoundation Blog*, 16 June, 2021. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-second-cyber-oewgs-organisational-session/

[17] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Organizational Note* (A/AC.292/2021/CRP.1), May 2021, https://docs.un.org/en/A/AC.292/2021/CRP.1 and Russian Federation, *Concept of work of the UN Open-ended Working Group on security of and in the use of information and communications technologies submitted by Russian Federation,* 1 June 2021, https://documents.unoda.org/wp-content/uploads/2021/06/Concept-paper-on-the-New-OEWG-ENG.pdf

How to facilitate other stakeholders' engagement?

Unsurprisingly, all delegations which touched upon multistakeholder dialogue expressed their support for it. However, less than a third spoke about the way it should be organised. ***Half of them suggested that the example of the first OEWG should be followed, where other stakeholders were involved via informal multistakeholder consultations. The other half suggested that non-government stakeholders have a more formalised mechanism to participate, whether through formal sessions or subgroups.***

To make everyone equally (un)happy, the working group can go for the common denominator: Businesses, NGOs with UN Economic and Social Council (ECOSOC) consultative status, and academia would be included in intersessional consultations, with no role in decision-making.

Would there be thematic subgroups in the OEWG?

The resolution which created the second cyber OEWG allows for the possibility of thematic subgroups, and this was the most addressed topic of the session. Several proposals were voiced on creating subgroups, from setting up equal thematic subgroups to creating a hierarchy between the subgroups. However, a detailed discussion did not take place.

No proposals were made about the membership of these groups or the way these would operate. Over the course of the first OEWG, over 100 delegations took the floor, and 66 delegations took the floor during its last substantive session in March 2021.[18] If the participation in subgroups were open to all delegations (as it should be), it would hinder the functioning of the subgroups and further strain the resources of small and developing countries participating in the OEWG.

What is clear is that the subgroups would meet between substantive sessions, which is a good way to keep delegations continuously engaged in the OEWG process over a long period of time—four years to be precise.

However, ***it remains unclear what mechanisms can be put into place to ensure the timely input of subgroup discussions into the substantive discussions.*** Several delegations brought up the idea that each subgroup should elect two chairs, one from a developed and one from a developing nation, who would communicate the results to Gafoor. The notion that the chair of the OEWG should be the lynchpin and preside over all subgroups was also brought up, but did not gain the support of more than two countries.

It was noted by a few delegates that subgroups, if established, should be held sequentially to respect the needs of small delegations, as they cannot attend many parallel meetings.

An observation could be made here; It would be up to each delegation to decide whether they would want to send multiple representatives to each follow the work of a subgroup, or one representative to follow the work of all subgroups. The formation of subgroups would most likely mean in-depth discussions on pre-set topics, and it is **unlikely that all countries**

[18] Andrijana Gavrilovic, 'A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers,' *DiploFoundation Blog*, 18 March, 2021, https://www.diplomacy.edu/blog/new-landmark-global-cybersecurity-negotiations-un-cyber-oewg-in-numbers/

have the expertise and presence in New York necessary to meaningfully participate in discussions.

Fears about subgroups fragmenting discussions – as the topics discussed are mutually interdependent and one cannot be deemed more important than the other – ***and the consensus, were repeated incessantly.*** Six delegations rejected the idea of subgroups for these reasons.

As the OEWG is acting under consensus, it seemed likely that thematic subgroups either won't be established, or if established at all, they will be held sparsely, perhaps cutting into the possibility of delving in depth into discussions.

Open questions

At the end of the organisational session, a few questions were left open, and left for the chair and the delegations to settle in the six months between the organisational session and the first substantive session:

- How should APRs be put together?
- Are there any elements from the previous working group on which the second OEWG should work?
- Which state initiatives aimed at the secure use of ICTs does the second cyber OEWG need to consider?
- How to enhance the participation of stakeholders while prioritising consensus?
- Are thematic groups necessary for conducting thematic discussions? If so, how and when should they be established?

However, questions would be addressed in informal discussion, which underlined that this is, in the end, a state-driven process. It would have been up to the chair to keep the process as transparent as possible, and to keep interested independent observers and stakeholders apprised. Otherwise, it would have been a step back from the democratic and inclusive reputation of the process.

Organisational issues persisted: The issue of multistakeholder engagement in OEWG 2021-2025

As discussed in December 2021[19]

The first substantive session of OEWG began with a hot debate on the pending issue of modalities of multistakeholder participation in formal meetings, as it was not agreed upon during the organisational meeting in June 2021.

[19] Digital Watch Observatory, *Modalities of multistakeholder participation*, 13 December, 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation

Modalities of multistakeholder participation

When it was time to consider the item of organisation of work, **the UK** raised its concerns about the modalities of work and stated that it could not adopt the provisional program of work, due to the lack of consensus. This opened ***a discussion during which Gafoor asked the delegations to provide their positions on multistakeholder participation and identify potential solutions towards building the consensus.***

Notably, **Gafoor** mentioned that, in his letter to delegations dated November, he ***suggested maintaining the precedent of the first OEWG with regard to the participation of stakeholders in formal meetings.*** As occurred during the previous OEWG, the OEWG can continue to engage stakeholders in informal consultative meetings.'[20] He also received an open letter from 40+ delegations and other stakeholders in December. The letter contained the principles of MS participation, including:

- Non-governmental stakeholders should be able to meaningfully participate in formal OEWG meetings
- A transparent process regarding any objection from a member state to the accreditation request should be in place
- In the event that an interested non-governmental stakeholder is denied accreditation to formal OEWG sessions, there should be other channels for such stakeholders to regularly express their views and for those views to be available for review to all accredited delegations
- A hybrid format of participation should be used for formal and informal meetings to facilitate the participation of delegates and stakeholders who cannot travel to New York in person[21]

The exchange of views was attended by 36 delegations. ***The majority favoured meaningful multistakeholder participation in formal OEWG meetings, as well as a transparent accreditation process for non-governmental entities, so that any objections by member-states would be known to the delegations.*** **Australia**, **Brazil**, **Canada**, **Chile**, **Colombia**, **Costa Rica**, **the Czech Republic**, **Denmark**, **Ecuador**, **the EU**, **Estonia**, **Finland**, **France**, **Germany**, **Greece**, **Ireland**, **Italy**, **Korea**, **Mexico**, **the Netherlands**, **New Zealand**, **Poland**, **Slovenia**, **Switzerland, Turkey**, **the UK** and **the USA** were among them.

The Netherlands reminded that the last OEWG allowed substantive input from the NGOs, but only with the ECOSOC consultative status. The delegate stated that there have been several UN processes which provided better transparency of the procedures for participation of non-ECOSOC accredited NGOs. In most cases, this included a provision which required states to make the basis of their objections known to the group through the Secretariat. For

[20] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 15 November 2021*, 15 November 2021, https://documents.unoda.org/wp-content/uploads/2021/11/OEWG-2021-2025_Chairs-letter_final.pdf.
[21] Multistakeholder group, *Letter for the OEWG Chair on Modalities*, December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Multi-Stakeholder-Letter-for-OEWG-Chair-on-Modalities-.pdf.

example, in the UN Secretary-General's Our Common Agenda', an inclusive multilateral system is mentioned, too.[22]

France provided its own examples of multistakeholder initiatives, such as the Paris Call and the Christchurch Call, which preserved the position of states without losing their privileges, while gaining from other stakeholders' experience.[23]

Colombia and other states stressed the necessity of a hybrid format for formal and informal meetings with the goal of facilitating greater participation, both for delegates as well as the stakeholders, especially in the face of restrictions derived from the pandemic.

China, **Cuba**, **Iran**, **Nicaragua**, **Pakistan**, **Russia**, **Syria**, **and Venezuela** ***were against the extended multistakeholder participation. They supported the Chair's position of using modalities from the last OEWG.***

Russia, in particular, insisted on the in-person format of meetings because 'it expands our possibilities of finding common ground, expands opportunities for a true democracy'. However, **Russian** and **Syrian** delegates raised the issue of obtaining the visas in due time, leading to a significant number of delegations not being able to be present in New York. The USA was blamed for using its stance as a host country to project political tensions and provide obstacles for equal states' participation in the OEWG. Also, it was stressed that the priority for participation in OEWG should be given to states, as the OEWG is an intergovernmental process. Moreover, **Russia** pointed out that the current mandate of the OEWG 'does not make it possible to involve stakeholders in formal meetings or have any kind of obligations to work to cooperate with them.' All the NGOs that are interested in the intergovernmental negotiating process can follow the formal meetings of the OEWG through online broadcasting. If they wish to express their views on any of the issues touched upon, they can submit their written statements to the chair, who will later circulate them for consideration by the states, as well as convey them throughout the intersessional consultative meetings.

At the end of the first meeting, Gafoor concluded that there was still no consensus on the issue. He reminded that OEWG does not have an option to vote on a particular item of the agenda to adopt it. That is why it was important for the delegations to come to a consensus regarding the multistakeholder participation. An informal consultation during lunch break was decided upon to come to a decision on how to continue this substantive session. Finally, delegations decided to continue discussing other agenda items and return to the contentious issue at the end of the session.

At the ninth meeting, the chair decided to bring this question up to the agenda again, formally. The chair informed that the seven-point proposal he submitted on the first day was met by a mix of approvals and disapprovals by various delegations, which made him informally consult many delegations towards a possible compromise. In the meantime, he also held an informal virtual consultation with over 100 non-state actors. The chair then submitted a revised proposal to the delegations on the third day of the meeting, reminding

[22] Digital Watch Observatory, *Our Common Agenda*, September 2021, https://dig.watch/resource/our-common-agenda
[23] Digital Watch Observatory, *The Christchurch Call,* May 2019, https://dig.watch/resource/christchurch-call, and Digital Watch Observatory, *The Paris Call for Trust and Security in Cyberspace*, November 2018, https://dig.watch/resource/the-paris-call-for-trust-and-security-in-cyberspace.

them that the OEWG is supposed to reach decisions by consensus, and expressed his feeling that there was no opposition to greater engagement of other stakeholders in the OEWG.

To agree on modalities for MS participation and make them functional for the second substantive session, starting on 28 March 2022, the chair suggested the following steps:[24]

1. The chair will continue informal consultations with delegations till mid-January.
2. The chair will provide the final proposal to all delegations on 18 January 2022, allowing a silence procedure till 25 January 2022.
3. If the silence procedure is not broken, UNODA will start the two-month-long process of applications and accreditation, to complete it in time for the second substantive session. If the silence procedure is, however, broken, discussions will have to continue.

Though many delegates who took the floor clarified that they are not fully satisfied with it, almost all expressed support for the revised chair's proposal and the suggested timeline for sake of achieving the consensus: **the EU, France, South Africa, the USA, Switzerland, Turkey, Egypt, Mexico, Italy, Indonesia, Japan, Latvia, Korea, Costa Rica, Columbia, Brazil, Jordan, Germany, Argentina, Australia, Iraq, Israel, UK, Poland, Malaysia, Slovenia, the Netherlands, Denmark, Ireland, Estonia, Dominican Republic, and Czech Republic**. Without supporting the proposal, **Russia** expressed its readiness to work constructively on this matter and noted that it would provide detailed thoughts on it, in accordance with the timeline specified by the chair. Similarly, **China** stated that it would work with other states on this matter.

Modus operandi: From informal to formal participation of stakeholders

Many countries, such as **the EU**, **the US**, **Chile**, **Latvia**, **Austria**, **Costa Rica**, and **Israel,** called for the formal participation of other stakeholders in the OEWG meetings, allowing them to present views and contributions in the official meetings and substantive sessions, as well as during the intersession periods.

Iran, however, reiterated the need for preserving the intergovernmental character of the OEWG and making sure that all the UN member states get the opportunity for interaction, while preserving informal consultative meetings introduced to the previous OEWG as a mechanism for inputs from other stakeholders. **China** followed the same line of thought, reminding that the OEWG is an intergovernmental process led by member states, and arguing that the current arrangement of meetings, in particular the informal multistakeholder consultations as set up by the previous OEWG, has already provided enough time and opportunities for NGOs to air their views.

[24] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 17 December 2021*, 17 December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Chairs-letter-17-December-2021.pdf.

Modalities of multistakeholder engagement: Blocking the process?

Russia argued that the initiative of a number of states to reach an immediate decision on stakeholder participation was an organised action which threatened to block the work of the OEWG. **The Czech Republic**, however, argued that the issue of multistakeholder participation had already been raised by **Canada** at the organisational session and that bringing it up had not disrupted the OEWG work since the group managed to go through the entire agenda of the first substantive meeting. **Mexico** stated that the discussion is not only a decision on modalities or on who would be in the room, but rather a discussion on the possibilities to make progress.

In terms of the next steps and the timeline proposed by the chair, **the UK** made it clear that it considers the 25 January deadline non-negotiable, noting that, in case states block the deal and the Secretariat cannot begin the accreditation processes, the OEWG will be prevented from continuing the substantive work in March.

Recurring stumbling block: Modus operandi

As discussed in April 2022[25]

The very first speaker at the second substantive session in March 2022, **the UK** stressed that undecided modes of multistakeholder participation are an obstacle to adopting the programme of work of the second session.

Why was it important to adopt a programme of work? Because it is UN practice to switch to an informal mode of work, otherwise. In this OEWG, a switch to an informal mode of work brought about a lot of confusion, namely, whether it is in line with the OEWG mandate and the allocated budgets, and whether delegations' inputs would be taken into account when writing the first APR. The informal mode of work may have contributed to a more open exchange of opinions between the states and the setting of priority issues that have not been discussed in detail before.

While the collective West (**the USA**, **the EU**, and allies) was supporting the switch to informal mode, those that typically disagree with them, e.g. **Russia** and **Cuba**, were against it.

Interestingly, the Chair took a long time to say it was, in fact, his proposal to work in informal mode – he only clarified this during the third meeting of the session, and proceeded to suspend the formal meeting, effectively switching to informal mode. From there on, even as there was no consensus on working in informal mode, each meeting was opened and soon formally closed, and discussions then proceeded in informal mode.

Explainer: Informal vs formal mode

[25] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session,' *DiploFoundation Blog*, 25 April 2022. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-second-substantive-session/.

Informal consultations encompass communication between delegates, including social interaction and interaction about the business of the conference. Most agreements are reached in informal mode.

Formal processes include opening and closing meetings, adopting work plans and documents, providing the context for informal exchanges, and making decisions – often based on previously reached informal agreements.

(Undecided) Modes of multistakeholder participation

The oft-mentioned proposal by India was apparently to ***use the modalities of the OEWG 2019-2021, i.e. engage with non-governmental stakeholders in sessions in consultations separate from formal sessions, for one year. Chair's Rev.1 document was also mentioned.*** However, neither of these two documents seems to be available to the public, which hurts the transparency of the process. Ultimately, neither of the proposals was adopted.

Another option mentioned was to follow what the OEWG on conventional ammunition has done in this regard. To the best of our ability to research it, the mode this OEWG used was to

- allow organisations that have observer status with the General Assembly and are ECOSOC-accredited to participate
- allow other relevant non-governmental organisations to apply to the Secretariat for accreditation, the Secretariat circulates the list of such organisations, and the OEWG considers and takes decisions on applications that states objected to at the beginning of each of its sessions[26]

However, when the modalities in the OEWG on ammunition were elaborated, it was stressed that they would not serve as an example for other UN processes.

Russia and **Iran** were claiming the collective West wanted to distract the OEWG from discussing substantive issues, and in the case of the second session, the discussion on modalities did delay the substantive discussions.

[26] United Nations, *Letter dated 31 January 2022 from the Chair Designate of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, 31 January 2022, https://documents.unoda.org/wp-content/uploads/2022/02/2022-01-31-Letter-from-the-Chair-Designate_organizational-matters_enclosures.pdf.

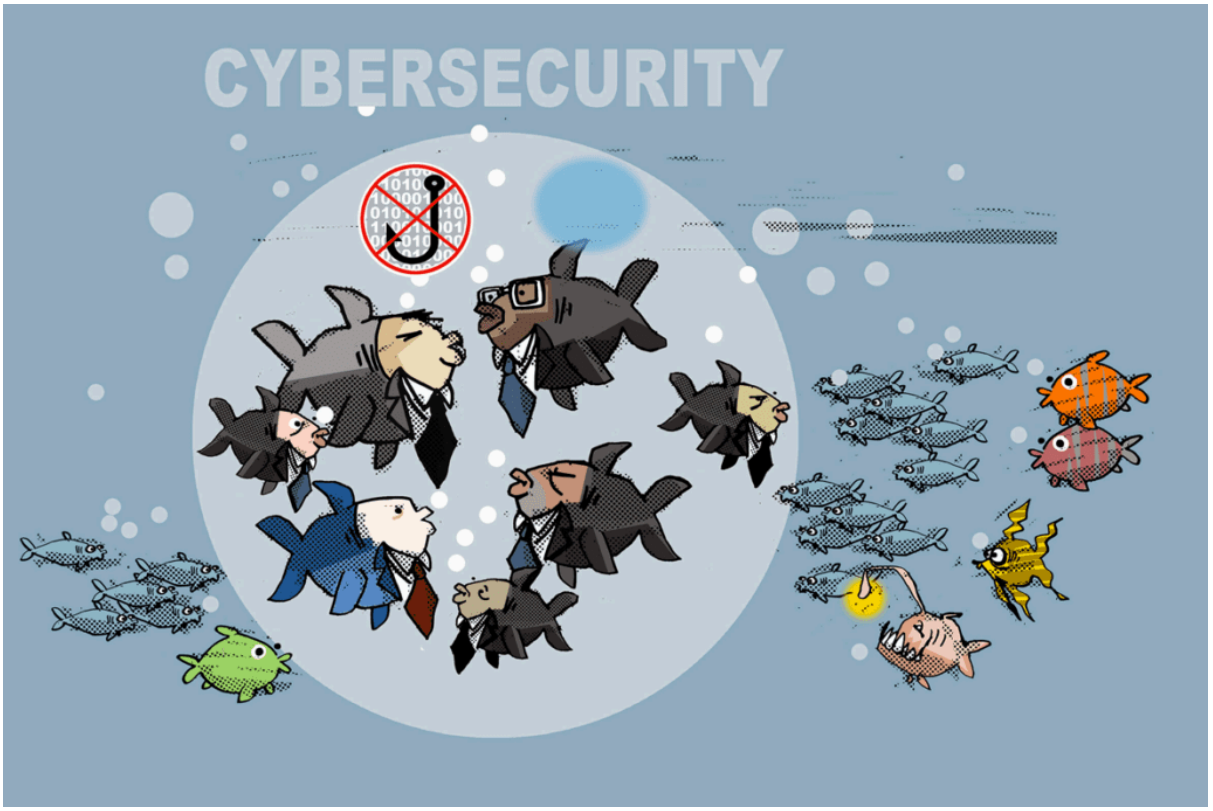


Image credit: Vladimir Veljasevic.

It is relevant to observe that, probably also due to the lack of agreed working modalities, **some states turned to self-organising into ad-hoc groups**. **Germany**, along with a number of other countries, **convened an open cross-regional group on the implementation of CBMs**, focused on cross-regional exchange within the OEWG. According to the conveners, the group was open to all interested states to join, and many countries expressed support and interest in participating in such a group. Interestingly, the group also announced a report on its current findings to be submitted to the OEWG website.

Whether more groups would self-organise in the future to discuss specific topics and open questions, and whether this would enhance cooperation and productivity or cause further challenges for the working modalities, remained unclear at this point. The Chair, as well as several states, expressed hope that the issue would be solved by July so that delegations could adopt the programme of work at the third substantive session (25-29 July 2022).

Modalities adopted: A step forward for multistakeholder engagement

As discussed in July 2022[27]

In the run-up to the third substantive session, stakeholders – businesses, NGOs, academia, and the technical community- applied to provide input to the OEWG. The states had the possibility to veto the participation of stakeholders that did not have the UN ECOSOC consultancy status. Many such stakeholders (27) have been vetoed by **Russia**, which triggered a discussion on stakeholder participation.

Among the countries that used the veto, **Russia** and **Ukraine** ***shared their reasoning.*** **Russia** said that the states have the sovereign right to work in the area of ICT security and that Russia's actions were strictly in accordance with the modalities for members of the OEWG, which state that the countries are not obliged to inform the Chair of the reasons for their veto – it is only voluntary. **Russia** had proceeded ***based on appropriateness and relevance in terms of the OEWG mandate in considering the stakeholder applications.*** **Ukraine**, which blocked some of the Russian stakeholders, noted that ***a few organisations from Russia are 'clearly state-affiliated entities',*** while the OEWG should benefit from contributions made by independent NGOs.

The delegations also discussed stakeholder inputs and their relevance with regard to specific issues – international law, existing and potential threats, the CBMs, and capacity building.

New Zealand, **Croatia**, **Italy**, **Estonia**, **Ireland**, the **UK**, **Romania**, **Finland**, **Latvia**, **Denmark**, **Canada**, the **EU**, **Switzerland**, **Chile**, and others ***expressed their support for the stakeholders to be part of the discussion and encouraged*** **Russia** ***to provide an explanation of its position on stakeholder engagement.***

Regarding stakeholder engagement in general, **El Salvador** highlighted the contributions of academia, NGOs, and civil society through the generation of specialised documents. **Iraq** stressed the need to benefit from the important role of stakeholders and to tackle potential threats in cyberspace and in the ICT sector in general, given their experience in this field. **Peru** highlighted the need for stakeholders' engagement in the OEWG process according to the agreed modalities.

China noted that ***discussions by any regional organisation are not more important than deliberations at the UN.*** **Kenya** highlighted the ***central role played by sub-regional and regional bodies in the sharing of technical information, including relevant threat intelligence.***

Costa Rica noted that information about threats and the response to incidents is an area where stakeholders such as CERTs, communities, and tech companies have greatly added value.

---

[27] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted', *DiploFoundation Blog*, 13 August 2022, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/

China and **Nicaragua** noted that ***the development of the common understanding on international law remained the exclusive prerogative of states***, and **China** asked to ***delete the text on inputs from interested stakeholders, including business and non-governmental organisations and academia.***

The Netherlands, on behalf of the international law group of states, ***noted that the development of common understandings on international law remains the exclusive prerogative of states,*** and proposed that ***discussions at the OEWG could benefit from experts*** from the International Committee of the Red Cross and the UN such as the International Law Commission, ***as well as interested stakeholders, including business, non-governmental organisations, and academia.*** The **Republic of Korea** stated that the ***understanding of how international law applies can also be further developed by other entities, such as academia***, through legal interpretation of international law, and that a useful way of developing such a common understanding is through voluntary sharing of national views on how international law applies in the use of ICTs.

Costa Rica wanted the OEWG to dedicate sessions or establish subgroups to study specific issues of international law.

Iran stated that the ***national systems, mechanisms, and priorities should be ensured in any engagement with stakeholders on aspects of confidence-building measures.*** Iran also noted that only those stakeholders whose accreditation has already been approved by states on a known objection basis, according to the agreed modalities, can engage capacity building aspects.

Brazil stated that briefings with experts, particularly such expert organisations that have a standing invitation to participate as observers in the work of the OEWG, are welcome. The same opinion on expert briefings was requested by **Canada**, **Australia**, **Mexico**, and the **Republic of Korea**. **Iran** prefers to include briefings from relevant bodies within the UN, such as the International Law Commission, instead of expert briefings.

The outcome: The modalities of stakeholder engagement in the OEWG were adopted by consensus. Accredited stakeholders were given the possibility to attend formal OEWG meetings without addressing them, speak during a dedicated stakeholder session, and submit written inputs for the OEWG website. Other relevant stakeholders were given the possibility to apply by providing information on their purpose and activities; they may be invited to participate as observers, subject to a non-objection process. A state had the right to object to the accreditation of specific non-ECOSOC-accredited organisations. The objecting state had the obligation to notify the OEWG Chair of its objections. The state had the possibility to, on a voluntary basis, share with the Chair the general basis of its objections.[28]

[28] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 22 April 2022*, 22 April 2022, https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf

Existing and potential threats

Facing cyber threats: The role of cooperation, capacity-building, and norms

As discussed in December 2021[29]

Delegations shared examples of urgent and challenging, existing and potential threats that states are facing. Most states which spoke on the subject emphasised threats to critical infrastructure and ransomware attacks. Other threats the states are concerned with include: cybercrime, violent extremism and cyberterrorism, fake news, deepfakes, misinformation and disinformation, data security, the use of ICTs for military purposes, state-sponsored malicious cyber activities, cyberattacks affecting democratic institutions, attacks on the supply chain, threats against OT and IoT, developments in new technologies (such as AI, Blockchain, etc.), crypto and digital currency, human rights, child safety online, the digital divide, internet fragmentation, and unilateral coercive measures.

The delegates also spoke about ***possible cooperative measures*** to prevent and counter threats in the sphere of international security.

In this regard, ***many states underlined the importance of capacity-building***. According to **South Africa**, raising the general level of states' ICT capacities would also raise the overall resilience of states to cyber threats. This was echoed by **Canada**, **Chile**, and **Colombia**. **Brazil** noted that states should cooperate to build capacities for mitigating threats to critical infrastructure.

Some of the countries underlined the significance of the OEWG in such capacity-building efforts. The **UK** stressed that a crucial element of the OEWG's work is supporting states in developing the capacities and structures required to prevent, detect and respond to threats at the national level. **Iran** stressed that the OEWG should focus on capacity-building under the auspices of the UN, as this would ensure security, safety, and integrity of ICT supply chains. The **Netherlands** suggested that the OEWG can help ensure that capacity-building is sensitive to the different impacts the threats have on different states, as well as increase states' resilience. **Chile** suggested that the OEWG could recognise the work of various international cyber capacity-building initiatives (such as the GFCE) and work jointly with them. **Indonesia** also noted that the OEWG could encourage states to strengthen their institutional capacity, legal and policy frameworks, and technical capabilities. Further, the country proposed that the OEWG consider developing comprehensive guidelines covering aspects of prevention, protection, and countermeasures for both the data users and systems. Such guidelines can then be used as a reference in helping states become better prepared for tackling threats in the sphere of information security. The OEWG could also assist states in incorporating such guidelines into domestic policies.

---

[29] Digital Watch Observatory, *UN OEWG 2021–2025 – Existing and potential threats*, 14 December, 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/existing-and-potential-threats

The necessity for the establishment of the rules, norms, and principles of responsible behaviour of states**,** which meet the challenges in the ICT sphere, was highlighted by **Iraq**. **Russia** stated that, to counter the existing and potential new threats, there is ***a need for a global system of international information security under the aegis of the UN***, which should be forged based on the respect of the principles of equitable safety and security of states, and equitable dispute resolution of disputes that arise from the use of ICT.

Nigeria underlined the need to ***legalise the already agreed-upon norms*** to ensure responsible behaviour. The **Netherlands** also noted that states should, at all times, respect the agreed-upon norms in their use of ICTs. The application of those norms could be enhanced by concrete implementation. **France** noted the importance of exchanges on the implementation of norms of responsible behaviour in cyberspace. **Brazil** and **France** underlined the exchanges of best practices in protecting critical infrastructure.

All of the UN member states should make efforts to counter any and all cyberattacks which could damage their sovereignty and undermine their good relations with other countries, **Iraq** underlined. **Ukraine** also noted that states should each increase their own ability to resist internet-based threats and enhance common cyber resilience policies.

The establishment of a ***multilateral mechanism for the attribution of cyber incidents*** within the context of the UN to unequivocally and impartially determine the source of incidents was suggested by **Cuba**. **France** emphasised the state's due diligence obligations in the face of malicious activity conducted by non-state actors in their territory. The country also suggested that the OEWG could consider how to better control the malicious cyber tools.

On ***countering misinformation***, **Pakistan** underlined the need for cooperation with the UN and relevant agencies, international cooperation, and multidimensional and multistakeholder responses. Those efforts must be consistent with international law, including humanitarian rights law. Online platforms and social media companies should ensure that their commercial objectives do not undermine human rights, and that their business models, data collection, data processing practices, and advertisement policies are compliant with international human rights law.

On the ***protection of personal and other data***, **Russia** stated that defining the principles for the processing of personal data, in a manner uniform for all UN member states, is needed. This would significantly help raise the level of personal data protection and strengthen legislation for the protection of personal data in those states which may display shortcomings in this matter.

In efforts to address ICT threats, ***states should not inadvertently inflict other types of harm or further marginalise vulnerable groups***, **Costa Rica** emphasised. Governments must engage with the local civil society organisations to gain an understanding of how cyber threats impact different segments of society.

Nigeria underlined the ***importance of robust incident management frameworks***, including operationalisation of Computer Emergency Response Teams (CERTs) capacity building, different levels of multistakeholder-based engagement, and the whole of society approach to implementation of cybersecurity, cooperation between states, as well as legalising agreed upon norms to ensure responsible behaviour.

Israel noted that ***a certification scheme for supply chain security*** and compliance officers that would guarantee cross-border interoperability could help build trust and greatly contribute to cyber hygiene. Israel also noted that ICT companies should build products which are secure by design, meaning that the end user would, by default, get a safer version of the product with less attack surface.

Argentina underlined the ***exchange of information on vulnerabilities*** between the public and private sectors, better international judicial cooperation, and awareness-raising.

Poland wanted to see ***national and European experiences and tools expanded to the global level*** for the benefit of all UN member states.

The OEWG could hold ***dedicated meetings on specific norms of responsible state behaviour in light of specific threats*** the international community faces, **the EU** suggested. Such discussions would contribute to a better understanding of the cyber threat landscape, the challenges to be addressed, and would help identify concrete solutions to advance the implementation of responsible state behaviour in cyberspace. A similar suggestion, made by **Switzerland** and **Chile,** was that the OEWG could organise ***dedicated meetings, seminars, workshops, or conferences on specific threats***. In **Chile's** view, the OEWG could ***recommend conducting a study on threats***, in coordination with regional organisations.

Threats vis-à-vis Ukraine conflict

As discussed in April 2022[30]

The start of Ukraine crisis heavily impacted the discussion on threats, with the majority of participants calling on Russia to stop cyberattacks on Ukraine's information resources and fake news campaigns.

Russia, on the other hand, ***brought up two new threats to states in cyberspace: disconnecting a country from the internet and cutting it off from the international payment system.*** It was referring to the fact that it was cut off from SWIFT, noting that it is 'technically possible because the management of such a system is in the hands of just one or a very narrow group of countries'. This is the first time that such examples were brought into OEWG discussions, as such events were unprecedented. Along those lines, Iran and Cuba warned that states should refrain from adopting unilateral coercive measures that might restrict or prevent universal access to ICT.

[30] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.'

Defining scope: How extensive should the list of threats be in the first APR?

As discussed in July 2022[31]

In July 2022, states met at the third substantive session to adopt the group's first APR.[32] The key question during the discussions on threats was ***how exhaustive the list of threats in the report should be***. **France** noted that the APR needs to contain a description of threats, and that some threats could be recalled more explicitly. **The USA** and **Canada** similarly stated that more work on the section is needed. Canada noted that this section lays the table for the rest of the report, which is basically about how to address the threats, while **the USA** highlighted that discussions about best practices and network defence lie outside of the OEWG's remit. **Brazil**, **Argentina**, **Mexico**, **Sri Lanka**, and **the EU** noted that an exhaustive list of threats would be impossible to agree upon.

There were strong calls for ***the protection of critical infrastructure (CI) and critical information infrastructure (CII)*** made by **the Philippines**, **the Netherlands**, and **Singapore**, with Singapore underlying cross-border CII. Adding measures to solve vulnerabilities in OTT and IoT technologies was suggested by Singapore, while **Israel** also noted threats against OT and added SCADA to the discussions. **The EU** cautioned that the proposal to agree on the list of critical infrastructures will not allow for consensus discussion between states.

Other threats were brought up as well. For instance, **Kenya** put forward ***violent extremism and terrorist activities***, as well as ***online threats to child safety*** and vulnerable groups. The security implications of ***new and emerging technologies*** were noted by **the USA**, **Brazil**, and **Germany**. **Pakistan** underlined that measures to ***counter disinformation and fake news***, and ***measures for the timely disclosure of vulnerabilities***, should be added to the text.

Cameroon suggested the ***creation of a permanent platform for support and discussions on new threats***, as well as an ***urgent response to emergencies***.

The outcomes: The first APR notes that the ever-evolving properties and characteristics of emerging technologies also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. Malicious use of ICTs by terrorists is also mentioned in the report.

Ransomware as a threat to critical infrastructure should be added under the threats section of the report, **Canada**, **Costa Rica**, **the EU**, **Mauritius**, **Colombia**, **the Czech Republic**, **Israel**, and **the ICC** noted. **China** volleyed back: By discussing the issue of ransomware, is the OEWG discussing ***cybercrime***? **Russia** also stated that it considers ransomware a cybercrime. **Brazil** underlined a ***context-based approach: ransomware is relevant for the OEWG when it reaches the level of threat to international security***, and in most cases, ransomware will be more pertinent to cybercrime. **Australia** agreed with this view, saying that the inclusion of ransomware in the wording of the annual report is not a red

---

[31] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.'
[32] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*, July 2022, https://dig.watch/resource/oewg-2021-2025-first-annual-progress-report-apr.

line, and that it is more important to capture the evolving nature of threats. **Jordan** thought that ransomware should be present in the report of this OEWG and in the cybercrime treaty.

The outcome: Shockingly, the first APR does not contain a single mention of ransomware, which has long featured as the threat most countries were concerned about.

The ***inclusion of data security*** as one of the topics that is under the OEWG's mandate was welcomed by **China** and **Kenya**. However, **the EU** noted that welcoming discussion on data security initiatives remains premature.

The outcome: Data security has remained in the first APR as a part of the OEWG's mandate.

The fact that ***the context of armed conflict due to the war in Ukraine should be reflected in the report*** was brought up by **Ukraine** itself, **New Zealand**, **the USA**, **Canada**, **the Netherlands**, and **Australia**. **Germany** also highlighted the military use of the ICTs, **Japan** highlighted malicious use of the ICTs in conjunction with military action, while Vietnam added threat, or the use of force, as elements that the report should contain.

The outcome: The first APR acknowledges 'a challenging geopolitical environment with rising concern over the malicious use of ICTs by state and non-state actors targeting critical infrastructure and essential service', but does not explicitly state it is due to Ukraine war.

Emerging threats in focus: Ransomware, interference, and new technologies

As discussed in December 2022[33]

Many states – including **Switzerland, El Salvador, Netherlands, Israel** and **Ireland** – expressed ***dissatisfaction with the fact that ransomware was not included in the first APR.***

Activities that undermine trust and confidence in political and electoral processes and public institutions were underlined by the **Netherlands**. **Iran** highlighted: (a) use of the ICTs to destabilise and interfere in the internal systems and processes of a state and create conflict among nations, races and ethnic minorities, (b) unilateral coercive measures against a state in the ICT domain, (c) disinformation campaigns, fabricated image building and xenophobia against states through the use of ICT, (d) lack of responsibility of the private sector and platforms with extraterritorial impact in ICT domain. **Russia** similarly noted **unlawful restrictive measures against particular states** and the need to counter deploying in the national information space of states free access tools for conducting cyberattacks.

---

[33] Andrijana Gavrilovic, Pavlina Ittelson, Salome Petit-Siemens, Vladimir Radunovic, Jeanne-Louise Roellinger, and Ilona Stadnik, 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs', DiploFoundation Blog, 16 December 2022, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-informal-oewg-consultations-on-cbms/

Israel ***underlined the risks of hacking-as-a-service, provided by cybercriminals and cyberterrorists as proxies of states***. Information sharing among defenders should be enhanced, and common cybersecurity standards for different industries should be developed, in particular for the civil aviation and maritime industries which are at great risk. ***Application of new technologies was also noted as a concern***, with the **Netherlands** putting forward the application of new technologies in cyber operations and **Ireland** highlighting the use of quantum computing to crack encryption.

Redefining scope: How extensive should the list of threats be in the second APR?

As discussed in March 2023[34]

Malicious activity in cyberspace is on the rise, member states agreed time and time again. Well, when has it not been the case? Yet, as the threat landscape is ever-evolving, member states were invited in March 2023 to identify the ones that should make it to the second APR.

The **EU**, **Denmark**, **Finland**, **Iceland**, **Norway**, **Sweden**, the **Nordic countries**, the **Czech Republic**, and **Germany** highlighted the ***spill-over effects of Russian cyberattacks on Ukraine***. These attacks have led to significant risks associated with escalating cyberspace threats, particularly affecting European energy and IT infrastructure.

The over-reliance on digital infrastructure since the COVID-19 pandemic has increased the risks of ***supply chain disruption***, a concern shared by many countries.

Countries like **El Salvador**, **Germany**, and the **Czech Republic** highlighted the impact of ***AI-powered cyber instruments*** on international peace, security, and stability. The accelerated use of ICTs and the intransparency of algorithms may cause lower levels of human control and oversight over ICTs, leading to risks in the security domain, these countries noted.

The **Czech Republic** proposed that the OEWG develop a more detailed discussion on ***responsible state behaviour in developing new technologies***.

Another salient theme was the growing ***prevalence of ransomware and cybercrime***. Ransomware had previously been the topic of discussion at the OEWG – it has been the most commonly mentioned cyber threat – but, surprisingly, it didn't make it into the APR. **El Salvador** stated that ransomware continues to be one of the greatest threats to the security of information and data, a sentiment echoed by **the USA**, **the EU**, **Kenya**, **Denmark**, and **Argentina**.

Kenya proposed ***establishing a repository of common threats, vectors, and actors*** under the auspices of the UN. **Russia, Germany, Samoa, the Netherlands, Fiji, and**

[34] Andrijana Gavrilovic, Stefania Grottola, Pavlina Ittelson, Anastasiya Kazakova, Salome Petit-Siemens, Ilona Stadnik, 'What's new with cybersecurity negotiations? OEWG 2021–2025 fourth substantive session', *DiploFoundation Blog*, 23 March 2023, accessed 23 July 2025, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-fourth-substantive-session/

others welcomed this idea and expressed willingness to explore it further during the OEWG work. **The Philippines** proposed a similar idea for ***a portal***, which could be modelled after the Cybercrime Repository under the UN Office on Drugs and Crime and building on the existing Cyber Policy Portal of the UN Institute for Disarmament Research. The **EU** proposed taking stock of the work of the International Counter Ransomware Initiative and ***formulating a common position on issues such as ransomware***.

Assessing the threat landscape: From ransomware to AI and strategic proposals

As discussed in May 2023[35]

Kenya *elaborated* upon its March 2023 proposal for creating a UN-run threat repository to enhance global coordination in preventing and responding to cyber threats.[36] The repository would serve as a centralised platform for sharing information on new and emerging cyber threats, facilitating informed responses, and improving cyber resilience. The UN Office of Disarmament Affairs would oversee the repository, ensuring data integrity while providing searchable databases, real-time updates, and assistance mechanisms for member states. **Bangladesh**, **France**, **Colombia,** and the **Netherlands expressed their willingness to explore the proposal further.**

And as it always happens when a new mechanism or body is proposed, ***calls for taking stock of what already exists followed***. The **UK** and **Argentina** suggested **mapping existing mechanisms that counter threats in cyberspace**, like the Counter Ransomware Initiative.[37] **Argentina** also highlighted the CERT and CSIRT networks, the Forum for Existing Response and Security Teams (FIRST), Lithuania's Malware Information Sharing Platform, and India's Trident ransomware resilience platform. The **UK** further suggested that diplomatic and technical Points of Contact (PoCs) should communicate with their own counterparts to avoid duplicating the functions of CERT or CSIRT networks.

Russia, on the other hand, stressed the lack of a universal methodology for identifying perpetrators and the need to develop new measures to counter the range of threats to information security.

AI and ransomware top concerns

The surprising omission of ransomware in the first OEWG APR, despite the widespread acknowledgement of its significance as a threat by most countries, has led to its continued prominence in the ongoing discussions. Several countries, including the **UK**, **Czechia**, **South Korea** and **Singapore**, raised concerns about the ever-growing **ransomware threat** in ICT security and stressed the need for a better

---

[35] Andrijana Gavrilovic, Anastasiya Kazakova, and Salome Petit-Siemens, 'What's new with cybersecurity negotiations? The informal OEWG consultations on capacity building,' *Diplo Foundation Blog*, 24 July, 2023.
[36] Kenya, *Draft Working Paper on the Establishment of a Threat Repository within the United Nations*, 22 May 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated22May23_Kenya_Draft_Working_Paper_Threat_Repository.pdf
[37] Counter Ransomware Initiative, accessed 21 July 2025, https://counter-ransomware.org/aboutus

understanding of these risks. **Argentina**, **Chile**, **El Salvador**, and **New Zealand** called for the recognition of ransomware as a major threat in the next APR, highlighting its evolution into an advanced persistent threat.

Bangladesh drew attention to the numerous emerging threats such as ransomware attacks, deepfakes, quantum computing, and digital identities as vectors for future cyberattacks.

The dawn of generative AI also brought AI into the discussions. **Bangladesh** and **Czechia** particularly drew attention to the dangers of AI-powered hacking and AI manipulation of humans' emotions and thoughts.

Additionally, **El Salvador** put forward a statement on AI as emerging and potential threat, aligning its development with government frameworks to ensure AI safety. They emphasised the importance of implementing regulations to promote awareness among individuals regarding AI-generated photos and videos (especially deepfakes). Moreover, El Salvador acknowledged the significant potential of AI applications in nuclear deterrence and security doctrines, cautioning against the risks they pose to strategic stability by potentially escalating unintentional nuclear use.

It was to be anticipated that AI would continue to gain momentum in ongoing discussions within the OEWG. The extent of AI as an existing threat had been further formulated since the sessions in March, with a greater focus on the impact of AI on individuals and the need for government legislation around AI development. As a result, further proposals to operationalise tools and mechanisms for managing AI-related risks were likely to arise. When it comes to responding to the threat of ransomware, a key consideration remained uncertain: whether the focus will be on creating new tools or prioritising the coordination and enhancement of existing ones.

Mapping the threat landscape: Trends and priorities

As discussed in July 2023[38]

In July 2023, states met at the fifth substantive session to adopt the group's second APR.[39] ***New expected consensual additions*** were praised by most countries, including the ***reference to the use of ICTs in current conflicts and the inclusion of ransomware***, despite the latter not being considered relevant by some countries during previous sessions.

Regarding critical infrastructures, ***South Korea's proposal to add the energy sector to the list of sectors of particular concern*** was supported by many states. It made it to the report, whereas the ***proposal to add financial institutions to the list of threats*** went unheeded. Finally, while **China** and **Kazakhstan** resisted the ***reference to malicious ICT activities targeting humanitarian organisations***, it still made it into the APR.

---

[38] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik, 'OEWG's fifth substantive session: The highlights', *Digital Watch Observatory*, 15 May 2024, https://dig.watch/updates/oewgs-fifth-substantive-session-the-highlights.
[39] Digital Watch Observatory, *OEWG 2021–2025 Second Annual Progress Report (APR)*, July 2023, https://dig.watch/resource/oewg-2021-2025-second-annual-progress-report-apr.

The outcome: South Korea's proposal to add the energy sector to the list of sectors of particular concern was included in the second APR. While China and Kazakhstan resisted the reference to malicious ICT activities targeting humanitarian organisations, it still made it into the second APR. The proposal to add financial institutions to the list of threats went unheeded.

An old dispute: Data security

As an item listed in the OEWG mandate, **China**, supported by **Syria**, ***requested the group to have a more focused discussion on data security***. The Netherlands, followed by several other states (e.g. **Malaysia**, **Croatia**, **the UK**, **New Zealand**, and **Belgium**), expressed concerns regarding this reference as 'it is not clear how this impacts international security' and proposed referencing it in para. 14, along with the potential impact of new emerging technologies. While **Australia** suggested reverting to the language of the OEWG 2021 report on the issue, **the USA** requested the deletion of that reference, as 'it could be interpreted as elevating the issue' along with other issues perceived as more critical. Similar criticisms were addressed to the ***references to misinformation, disinformation and deepfakes***.

The outcome: These contentious references do not appear in the second APR.

Concrete proposals

Most of the new proposals were watered down or did not make it into the APR. Among them, **Kenya's** ***proposal for a threat repository*** received support from many delegations that expressed interest in furthering discussions on the issue. However, **Austria**, **the UK**, and **Mexico** recommended that ***this proposal be moved to the CBM section***, as echoed by **the USA**. The latter, supported by **Chile**, expressed concerns related to this initiative duplicating other technical forums among practitioners (such as CERT to CERT channels). **Nicaragua**, on behalf of **Belarus**, **Burundi**, **China**, **Cuba**, **North Korea**, **Iran**, **Russia**, **Syria** and **Venezuela**, ***strongly opposed the proposal and described it as a tool for the politicisation of ICT security issues***. At the same time, **Cuba** added that 'it could be used for false attributions or accusations for political ends'.

The outcome: The proposal for a threat repository didn't reach the second APR, threat, or CBM sections.

Many delegations also expressed their ***concerns regarding the impact of the development of new technologies*** (notably AI, quantum computing and cloud technology) on cybersecurity. **New Zealand**, **South Africa**, **the Netherlands**, **the Czech Republic**, **Ireland**, **Croatia**, **Singapore**, **Vietnam**, **Belgium** and **Bangladesh** also supported the ***proposal to hold an intersessional meeting dedicated to these emerging technologies***. **The USA** and **Russia** opposed this, arguing that several UN initiatives on emerging technologies (such as the GGE on LAWS) already cover these issues. **Austria** recommended having a ***focused discussion on how these technologies specifically affect cyber***. Finally, **Colombia**, supported by **Fiji**, proposed a ***meeting where states victims of cyberattacks could share their experiences***, lessons learned, protocols and best practices.

The outcomes: Any reference to these new technologies was deleted from the second APR. A less focused intersessional meeting 'on existing and potential threats to

security in the use of ICTs' with relevant experts' participation was recommended as the next step.

From innovation to governance: Emerging technologies, sovereignty, and data sharing

As discussed in December 2023[40]

The risks and challenges associated with emerging technologies, such as AI, quantum computing, and IoT, were highlighted by several countries. Numerous nations expressed concerns about ***ransomware attacks' increasing frequency and impact on various entities***, including critical infrastructure, local governments, health institutions, and democratic institutions.

The need for ***capacity building efforts to enhance cybersecurity capabilities globally*** was emphasised by multiple countries, recognising the importance of preparing for and responding to cyber threats.

Russia raised concerns about the ***potential for interstate conflicts*** arising from using information and communication technologies (ICTs). It proposed discussions on a global information security system under UN auspices. **El Salvador** discussed ***evolving threats in the ICT sector, particularly during peacetime,*** indicating that cybersecurity challenges are not limited to times of conflict.

Delegates discussed the impact of malicious cyber activities on international trust and development, particularly in the context of ***state-sponsored cyber threats and cybercrime***.

Several countries, including **the UK**, **Kenya**, **Finland**, and **Ireland**, focused on the ***intersection of AI and cybersecurity***, advocating for approaches which consider AI systems' security implications.

Some countries, including **Iran** and **Syria**, expressed **concerns about threats to sovereignty in cyberspace**, including issues related to internet governance and potential interference in internal affairs.

Many countries emphasised the ***importance of international cooperation and information sharing*** to address cybersecurity challenges effectively. Proposals for ***repositories of information on threats and incidents*** were discussed. The idea of a ***global repository of cyber threats***, as advanced by **Kenya,** enjoyed much support.

---

[40] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens and Ilona Stadnik. 'OEWG's sixth substantive session: The highlights,' Digital Watch Observatory, December 28, 2023. https://dig.watch/updates/oewgs-sixth-substantive-session-the-highlights.

Frontline issues: AI, ransomware and elections

As discussed in March 2024[41]

The widespread availability of AI tools for different purposes led to delegations focusing on AI-enabled threats. AI tools may exacerbate malicious cyber activity, for example, by faster searching for ICT vulnerabilities, developing malware, and boosting social engineering and phishing tactics.

France, **the Netherlands**, and **Australia** spoke about ***the security of AI itself***, pointing to the vulnerability of algorithms and platforms and the risk of poisoning models.

2024 is the year of elections on different levels in many states. Large language models (LLMs) and generative AI spur the fake creation process and the proliferation of disinformation and manipulation of public opinion, especially during significant political and social processes. **Belgium, Italy, Germany, Canada, and Denmark** expressed concern that ***cyber operations are used to interfere in democratic processes***. Malicious use of cyber capabilities can influence political outcomes and threaten the process by targeting voters, politicians, political parties, and election infrastructure, thus undermining trust in democratic institutions.

Another prevalent threat highlighted by the delegations was ***ransomware***. Cybercriminals target critical infrastructure and life-sustaining systems, but states noted that the most suffering sector is healthcare. **Belgium** stressed that such attacks eventually lead to human casualties because of the disruption in providing medical assistance. The **USA** and **Greece** highlighted the increase in ransomware attacks because some states allow criminal actors to act from their territories with impunity. Also, now AI is an excellent leverage for malicious threat actors, providing unsophisticated operators of ransomware-as-a-service with a new degree of possibilities and allowing rogue states to exploit this technology for offensive cyber activities.

Ransomware attacks go hand in hand with ***IP theft, data breaches, violation of privacy, and cryptocurrency theft***. The **Republic of Korea, Japan, the Czech Republic, Mexico, Australia and Kenya** connected such heists with the proliferation of WMDs.

Delegations expressed concerns about a growing commercial market of ***cyber intrusion capabilities, 0-day vulnerabilities and hacking-as-service***. The **UK, Belgium, Australia**, and **Cuba** considered this market capable of increasing instability in cyberspace. The **Pall Mall process** launched by **France** and **the UK** aimed at addressing the proliferation of commercially available cyber intrusion tools was upheld by **Switzerland** and **Germany**.[42]

The growing IoT landscape expands the surfaces of cyberattacks, **Mauritius, India, and Kazakhstan** mentioned. Quantum computing may break the existing encryption methods,

---

[41] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik, 'OEWG's seventh substantive session: The highlights,' Digital Watch Observatory, 28 March, 2024, https://dig.watch/updates/oewgs-seventh-substantive-session-the-highlights.

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

leading to strategic advantages for those who control this technology, **Brazil** added. It could also be used to develop armaments, other military equipment, and offensive operations.

Russia once again drew attention to the ***use of information space as an arena of geopolitical confrontation and militarisation of ICTs***. **Russia, China,** and **Iran** have also highlighted certain states' ***monopolisation of the ICT market and internet governance*** as threats to cyber stability. **Syria and Iran** pointed to practices of ***technological embargo and politicised ICT supply chain issues*** that weaken the cyber resilience of states and impose barriers to trade and tech development.

Key threats in focus: AI, ransomware, and critical infrastructure

As discussed in July 2024[43]

Ransomware and cryptocurrency theft

In July 2024, states met at the eighth substantive session to adopt the group's third APR.[44] Most delegations commended the more detailed language on the threats and harms posed by ransomware compared to the second APR and the inclusion of the threat of cryptocurrency theft. Some countries, including **the USA**, **the EU** and **South Korea**, went further to ask that the APR include an explanation of how these activities can contribute to the financing of terrorist activities and development of weapons of mass destruction, aligning with the joint statement of the UN open debate on cybersecurity published on 20 June.[45] Moreover, as **the Netherlands** pointed out, ransomware also affects public services.

However, **Nicaragua**, representing a group of states, and **Russia** raised ***doubts about the link between ransomware and cryptocurrency issues to international peace and security***. They posited that it was outside the purview of the group's mandate, as these activities were of a criminal nature and were financially motivated. **Australia**, **Canada** and **South Korea** ***reiterated their support for including these threats, noting that many delegations had testified that these threats affected critical infrastructure***, such as national healthcare and energy facilities. As such, these threats cause significant damage that cannot be simply dismissed as criminal activity. For this reason, the mention of ransomware and its effects was already included in the second APR.

The outcome: Ransomware and cryptocurrency theft were both included in the third APR, stating these threats 'could potentially' affect international peace and security while avoiding any reference to the proposal of the USA, the EU and South Korea to

---

[43] Andrijana Gavrilović, Anastasiya Kazakova, Jeanne-Louise Roellinger, and Salomé Petit-Siemens, 'OEWG's eighth substantive session: Third progress report adopted, what's next for ICT discussions?' Digital Watch Observatory, July 30, 2024, https://dig.watch/updates/oewgs-eighth-substantive-session-the-highlights.
[44] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR)*.
[45] Republic of Korea Ministry of Foreign Affairs, 'Statement at the Security Open Debate on Cyber Security (Foreign Minister Cho Tae-yul),' 20 June, 2024, https://overseas.mofa.go.kr/un-en/brd/m_26611/view.do?seq=158&srchFr=&amp%3BsrchTo=&amp%3BsrchWord=&amp%3BsrchTp=&amp%3Bmulti_itm_seq=0&amp%3Bitm_seq_1=0&amp%3Bitm_seq_2=0&amp%3Bcompany_cd=&amp%3Bcompany_nm= and Digital Watch Observatory, *Conclusions on the UN Security Council's Open Debate on Cybersecurity*, 21 June 2024, https://dig.watch/updates/conclusions-on-the-un-security-councils-open-debate-on-cybersecurity.

include the financing of terrorist activities and WMD development through cryptocurrency theft.

Artificial intelligence

Delegations commended the updated APR and its inclusion of concerns regarding new vectors, exploitation of vulnerabilities, and the data used for AI model training. Many countries also highlighted the benefits that new technologies like AI can bring to cyber resilience. ***Most Western delegations supported the need to implement and strengthen security-by-design approaches***, a terminology usually found in these countries' digital policies, while ***others***, like **China**, ***preferred to advocate for security through the life cycle, stating that security by design did not have consensus***. The choice of a broader (life cycle) term possibly ensures more flexibility and adaptability in policy implementation. Finally, **Finland** also proposed ***adding quantum technology in the same paragraph***.

The outcomes: The paragraph on AI was shortened in line with Australia's remarks to limit the scope of the paragraph to avoid duplications with other forums dedicated to AI and thus to only focus on the nexus of AI and cyber. Furthermore, security by design was not included; instead, the third APR uses the paradigm of 'security throughout the life cycle of these technologies'. The AI paragraph also mentioned quantum technologies.

Use of ICT by states inconsistent with their obligations

The first draft of this APR, specifically in paragraph 26, read that 'any use of ICTs by states in a manner inconsistent with their obligations under the framework of responsible state behaviour in the use of ICTs, which includes voluntary norms, international law, and confidence-building measures (CBMs), undermines international peace and security, as well as trust and stability between states.' This statement is taken from paragraph 19 of the second (2023) APR and, as such, is considered the previously agreed language that should not be reopened.

However, member states, including **the USA**, **Israel**, **Thailand**, and **Iran**, ***contended that voluntary norms and CBMs cannot be classified as obligations***. They argued that, by definition, voluntary norms are not obligatory and that CBMs, within the context of this OEWG, are also voluntary. Consequently, ***these states proposed revisions to the text to clearly differentiate between voluntary norms and CBMs on the one hand and obligations under international law on the other***. They emphasised that states cannot be held accountable for obligations arising from non-binding agreements.

The outcome: The paragraph – now renumbered as 27 – was not changed. Consequently, Iran distanced itself from paragraph 27, insisting that the text did not accurately reflect the international legal order.

Misinformation and disinformation

Delegations from **China**, **Iran**, and **Cuba** advocated for ***recognising misinformation and disinformation as significant threats within the ICT environment***. This perspective echoes previous discussions in the OEWG, where **Russia**, **China**, and **Iran**, among others, have highlighted the information space as a battleground for geopolitical confrontation and the militarisation of ICTs. **Pakistan** expressed concern that the malicious use of ICTs – particularly for disseminating disinformation and fake news by state and non-state actors –

jeopardised regional and global peace and security, often leading to social unrest. **Syria** emphasised the dangers of using the information space or cyber capabilities to undermine state sovereignty or to propagate misinformation and disinformation that fuels extremism and terrorism. Lastly, **Bangladesh** proposed the inclusion of misinformation and disinformation driven by advanced technologies, such as deepfakes, in the agenda for the APR discussions.

The outcome: The terminology in paragraph 18 on misinformation and disinformation remains unchanged from the second APR, specifically referring to 'covert information operations.' Additionally, the third APR does not reference misinformation and disinformation driven by advanced technologies, such as deepfakes.

Humanitarian organisations

Delegations highlighted the detrimental effects of ICT attacks on international humanitarian organisations, advocating for stronger language to better convey the disruptive nature of these attacks. The phrase 'international aid organisations' was included in the second revision of the text, however, delegations expressed concern that this terminology might restrict the reference to organisations that only provide goods.

The outcomes: All the proposals were implemented. The third APR notes that states also expressed concern regarding malicious ICT activity targeting international organisations and humanitarian organisations so as not to restrict the reference to organisations that only supply goods.

Legitimate use of commercially available ICT tools

Several delegations, including **the Netherlands**, **Switzerland**, and **Australia**, supported ***reintroducing language acknowledging the legitimate use of commercially available ICT tools in a manner consistent with international law*** initially present in draft zero of this APR.[46]

The outcome: The language was added about the legitimate use of commercially available ICT tools by evoking the tools that could be used in a manner consistent with international law.

Designation of critical infrastructure

Discussions centred on the designation of critical infrastructure, with ***some delegations applauding the reference to sectors like health and finance***. In contrast, ***others emphasised each state's autonomy in determining its critical infrastructure***.

The outcome: A compromise was reached by incorporating specific examples of critical sectors in the third APR while respecting each state's authority in defining its critical infrastructure.

[46] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 29 May 2024*, 29 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_29_May_2024.pdf

Candid discussions: A rapidly evolving threat landscape

As discussed in December 2024[47]

Discussions on threats became more detailed – almost one-fourth of the session in December 2024 was dedicated to this topic. The chair noted that this was reflection of the rapidly evolving threat landscape, but also a signal of a growing comfort among states in candidly addressing these issues.

What was particularly interesting about this session is that states have dedicated just as much—if not more—time to discussing cooperative measures to counter these threats as they have to outline the threats themselves.

Threats states face in cyberspace

Emerging technologies, including AI, quantum computing, blockchain, and the Internet of Things (IoT), took centre stage in discussions. Delegates broadly acknowledged the dual-use nature of these innovations. On one hand, they offer immense developmental potential; on the other, they introduce sophisticated cyber risks. Multiple states, including **South Korea**, **Kazakhstan**, and **Canada**, highlighted how AI intensifies cyber risks, particularly ransomware, social engineering campaigns, and sophisticated cyberattacks. Concerns about AI misuse include threats to AI systems (**Canada**), generative AI amplifying attack surfaces (**Israel**), and adversarial manipulations such as prompt injections and model exfiltration (**Bangladesh**).

Nations including **Guatemala** and **Pakistan** stressed the ***risks of integrating emerging technologies into critical systems***, warning that without regulation, these systems could enable faster and more destructive cyberattacks.

Despite the risks, states like **Israel** and **Paraguay** ***recognised the positive potential of AI in strengthening cybersecurity and called for harnessing its benefits responsibly.*** Countries like **Italy** and **Israel** called for international collaboration to ensure safe and trustworthy development and use of AI, aligning with human rights and democratic values.

Ransomware remains one of the most significant and prevalent cyber threats, as multiple delegations highlighted. **Switzerland** and **Ireland** flagged the growing sophistication of ransomware attacks, with the rise of ransomware-as-a-service lowering barriers for cybercriminals and enabling the proliferation of such threats. The **Netherlands** and **Switzerland** noted ransomware's profound consequences on societal security, economic stability, and human welfare. Countries including **Italy**, **Germany**, and **Japan** emphasised ransomware's disruptive impact on critical infrastructure and essential services, such as hospitals and businesses.

Critical infrastructure has become an increasingly prominent target for cyberattacks, with threats stemming from both cyber criminals and state-sponsored actors. Essential services such as healthcare, energy, and transportation are particularly affected. However, **the EU**, along with countries such as the **Netherlands**, **Switzerland**, and **the USA**, have

---

[47] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik, 'OEWG's ninth substantive session: Limited progress in discussions', Digital Watch Observatory, 30 December 2024, https://dig.watch/updates/oewgs-ninth-substantive-session-limited-progress-in-discussions.

also raised concerns about malicious activities disrupting essential services and international organisations, including humanitarian agencies.

Countries such as **Ireland, Canada, Argentina, Fiji** and **Vanuatu** have raised alarms about ***the rising number of cyber incidents targeting these critical subsea infrastructures***. These cables are vital for global communication and data transfer, and any disruption could have severe consequences. **Ireland** called for further examination of the particular vulnerabilities and threats to critical undersea infrastructure, the role of states in the private sector in the operation and security of such infrastructure, and the application of international law which must govern responsible state use and activity in this area.

Germany and **Bangladesh** ***highlighted the role of AI in automating disinformation campaigns***, scaling influence operations and tailoring misinformation to specific cultural contexts. Countries such as **China, North Korea** and **Albania** noted the rampant spread of false narratives and misinformation, emphasising their ability to manipulate public opinion, influence elections, and undermine democratic processes. Misinformation is weaponised in various forms, including phishing attacks and social media manipulation. Misinformation and cyberattacks are increasingly part of broader hybrid threats, aiming to destabilise societies, weaken institutions, and interfere with electoral processes (**Albania, Ukraine, Japan, Israel,** and the **Netherlands**). Several countries, including **Cuba**, **Russia**, and **Bangladesh**, stressed how cyber threats, including disinformation and ICT manipulation, are used to undermine the sovereignty of states, interfere in internal affairs, and violate territorial integrity. Countries like **Israel** and **Pakistan** warned of the malicious use of bots, deepfakes, phishing schemes, and misinformation to influence public opinion, destabilise governments, and compromise national security. **Bosnia** highlighted the complexity of these evolving threats, which involve both state and non-state actors working together to destabilise countries, weaken trust, and undermine democratic values.

Cyber operations in the context of armed conflict are no longer a novel concept but have become routine in modern warfare, with enduring consequences, according to **New Zealand**. Similar observations were made by countries such as the **USA, Germany, Albania, North Korea** and **Pakistan**. A worrisome development was brought forth by **Switzerland**, which noted the involvement of non-state actors in offensive actions against ICTs within the framework of armed conflict between member states.

Countries also grew increasingly concerned about the growing sophistication of hacking-as-a-service, malware, phishing, trojans, and DDoS attacks**.** They are also concerned about the use of cryptocurrencies for enhanced anonymity. **Israel** also highlighted that the proliferation and availability of advanced cyber tools in the hands of non-state actors and unauthorised private actors constitute a serious threat. ***The proliferation of commercial cyber intrusion tools, including spyware, raised alarm*** among nations like **Japan**, **Switzerland**, the **UK** and **France**. The **UK** and **France** emphasised that certain states' failure to combat malicious activities within their territories exacerbates the risks posed by these technologies. Additionally, **Kazakhstan** warned about advanced persistent threats (APTs) exploiting vulnerable IoT devices and zero-day vulnerabilities.

Cuba ***rejected the militarisation of cyberspace, offensive operations, and information misuse for political purposes***. They called for peaceful ICT use and criticized media platforms for spreading misinformation. The **UK** emphasised ***states' responsibilities to prevent malicious activities within their jurisdiction*** and to share technical information to

aid network defenders. **Russia warned against hidden functions in ICT products used to harm civilian populations**, calling for accountability from countries enabling such activities. **Columbia** suggested that ***states which have been the victims of cyberattacks could consider the possibility of undertaking voluntary peer reviews***, where they would share their experiences, including lessons learned, challenges, and protocols for protection, response, and recovery.

Cooperative measures to counter threats

Most countries noted the role of capacity building in enabling states to protect themselves. **The EU** called for coordinated efforts to capacity building and for more reflection on best practices and practical examples. Capacity-building initiatives should align with regional and national contexts, **Switzerland** and **Kazakhstan** noted, focusing on identifying vulnerabilities, conducting cyberattack simulations, and developing robust measures, **Kazakhstan** noted. **Columbia** highlighted that states should express their needs for capacity building to adequately identify the available supply. **Malawi** and **Guatemala** advocated for capacity building, partnerships with international organisations, and knowledge-sharing between governments, the private sector, and academia. **Albania** emphasised the importance of UN-led training initiatives for technical and policy-level personnel.

The discussions highlighted the urgent need to bridge the technological divide, enabling developing countries to benefit from advancements and manage cyber risks. Vanuatu emphasised the importance of international capacity-building and cooperation to ensure these nations can not only benefit from technological advancements but also manage the associated risks effectively. **Zimbabwe** called for the OEWG to support initiatives that provide technical assistance and training, empowering developing nations to build robust cybersecurity frameworks. **Cuba** reinforced this by advocating for the implementation of technical assistance mechanisms that enhance critical infrastructure security, respecting the national laws of the states receiving assistance. **Nigeria** stressed the importance of equipping personnel in developing countries with the skills to detect vulnerabilities early and deploy preventive measures to safeguard critical information systems.

States also noted that the topic of threats must be included in the new mechanism. **Mexico** proposed creating a robust deliberative space within the mechanism to deepen understanding and foster cooperation, enhancing capacities to counter ICT threats. **Sri Lanka** supported reviewing both existing and potential ICT threats within the international security context of the new mandate. **Brazil** suggested the future mechanism should incorporate dedicated spaces for sharing threats, vulnerabilities, and successful policies**. Some countries gave concrete suggestions for thematic groups on threats under the new mechanism**. For instance, **France** highlighted that sector-specific discussions on threats and resilience could serve as strong examples for thematic groups within the future mechanism. **Colombia** called for a standing thematic working group focused on areas like cyber incident management, secure connectivity technologies (e.g., 5G), and policies for patching and updates. **Singapore** emphasised using future discussions to focus on building an understanding of emerging technologies and their governance. **Egypt** advocated for a flexible thematic group on threats within the mechanism, capable of examining ICT incidents with political dimensions. **New Zealand** recommended focusing discussions on cross-cutting

themes such as critical infrastructure, enabling states to better understand and mitigate threats. **Cuba** echoed the importance of the future permanent mechanism taking into account the protection of critical infrastructure, and underscored the importance of supporting developing countries with limited resources to protect critical infrastructure.

Delegations highlighted the Global Point of Contact (PoC) Directory as a key tool for enhancing international cooperation on cybersecurity. **Ghana**, **Argentina** and **Kazakhstan** emphasised its role in facilitating information exchange among technical and diplomatic contacts to address cyber threats. **South Africa** proposed using the PoC Directory for cybersecurity training and sharing experiences on technologies like AI. Chile stressed that the PoC Directory can play a central role in the for improved cyber intelligence capacity and coordinated responses to large-scale incidents. **Malaysia** called for broader participation and active engagement in PoC activities.

Several countries emphasised the importance of strengthening collaboration among national Computer Emergency Response Teams (CERTs). **Ghana** and **New Zealand** supported CERT-to-CERT cooperation, with **Ghana** calling for sharing best practices. **Nigeria** suggested creating an international framework for harmonising cyber threat responses, including strategic planning and trend observation. **Singapore** highlighted timely and relevant CERT-related information sharing and capacity building as key to helping states, especially smaller ones, mitigate threats. **Fiji** prioritised capacity building for CERTs.

Several nations, including **Argentina**, **Sri Lanka**, and **Indonesia**, ***called for establishing a global platform for threat intelligence sharing***. These platforms would enable real-time data exchange, incident reporting, and coordinated responses to strengthen collective security. Such mechanisms, built on mutual trust, would also facilitate transparency and enhance preparedness for emerging cyber challenges. **Switzerland** voiced support for discussing the platform but also noted that exchanging each member state's perception of the identified threats can happen through bilateral, regional, or multilateral collaboration forums, or simply by making a member state's findings publicly accessible.

Egypt noted that ***there must also be discussions on both the malicious use of ICT by non-state actors***, as well as the role and responsibilities of the private sector in this regard.

Countries like **El Salvador** and **Ghana** ***underscored the importance of integrating security and privacy by design approaches*** into all stages of system development, ensuring robust protections throughout the lifecycle of ICT systems.

Building shared resilience in cyberspace hinges on collective awareness of threats and vulnerabilities. **Bosnia** stressed collaboration as essential, while **Moldova** and **Albania** highlighted the need for education and awareness campaigns to engage governments, private entities, and civil society. **Vietnam** advocated using international forums and UN agencies like ITU to bolster critical infrastructure resilience. Similarly, **Paraguay** called for creating awareness on the use of covert information campaigns, which may become incident, cyber incidents and tools for cyberattacks. **Zimbabwe** emphasised the critical importance of operationalising CBMs to foster trust and cooperation among nations in cyberspace. **Belgium** and **Egypt** emphasised the need to focus on the human impact of cyber threats and to use methodologies measuring harm to victims.

Collective action: Key to counter threats

As discussed in February 2025[48]

The discussions at this session revealed a range of national perspectives on cybersecurity threats. Malicious use of AI, critical infrastructure attacks and ransomware remained central concerns.

Collective solutions for cyber threats

The consensus remained clear throughout the discussions: cyber threats are a shared challenge requiring collective solutions.

Nigeria underscored the importance of a comprehensive international framework to ***harmonise responses to cyber threats***. Collaboration between state Computer Emergency Response Teams (CERTs), strategic planning, and continuous monitoring of emerging threats were highlighted as essential components. **Albania** reinforced the value of ***cooperative approaches in incident management***, warning that cyberattacks could escalate tensions if misattributed. Albania also advocated for ***robust diplomatic dialogue*** through strengthened communication channels among CERTs and intelligence-sharing agreements. **Uruguay** and **Argentina** underscored ***the need for knowledge transfer and shared expertise*** in identifying and responding to cyber threats. **Malaysia** and **South Africa** further emphasised that ***fostering collaboration among technical experts, academia, and government officials*** would enhance cybersecurity preparedness. **Bosnia and Herzegovina** emphasised ***resilience-building through strategic communication and public awareness***.

Capacity building remained a priority for developing nations. **Mauritius** and **Malawi** stressed the urgent need for technical assistance, funding, and training to strengthen cybersecurity frameworks in regions facing resource constraints. **Indonesia** echoed this sentiment, advocating for increased knowledge sharing and technical cooperation to collectively address evolving threats. **Nigeria** advocated for capacity building in developing nations to reduce technological dependency and improve cybersecurity defences. **Ghana** called for greater investment in cybersecurity research and innovation to bolster national defences.

Australia pointed to ***cyber sanctions as a means to deter malicious actors*** and impose tangible consequences on cyber criminals. **Switzerland**, focusing on the increasing threat of ransomware, stressed the need for ***states to uphold international law, reinforce resilience, and enhance international cooperation***.

A particular concern was the spread of misinformation and disinformation, which **Nigeria** suggested should be countered through the ***circulation of accurate information without infringing on freedom of expression***.

How to best reflect discussions on threats in the final report

---

[48] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik, 'OEWG's tenth substantive session: Entering the eleventh hour', Digital Watch Observatory, 27 February 2025, https://dig.watch/updates/oewgs-tenth-substantive-session-entering-the-eleventh-hour.

Several delegations emphasised key issues for inclusion in the OEWG final report. **The EU**, **Croatia**, **New Zealand**, and **South Korea** supported continued references to ***ransomware***.

China's concerns for the final report include ***the risks of politicising cybersecurity and ICT***, which threaten global cooperation and digital integrity. It also highlights ***the rising cyber tensions conflict***, particularly with offensive strategies and attacks on critical infrastructure. China stresses the importance of addressing false claims about cyber incidents, which harm trust between nations. It called for ***secure ICT supply chains*** and the prevention of backdoors in products.

China advocated for a comprehensive, evidence-based approach to ***data security*** in the AI era, focusing on data localisation and cross-border transfer issues. **Malaysia** supported China on the importance of addressing data security, which should be included in the final report.

El Salvador urged that the APRs reflect the ***importance of safe and transparent data management*** throughout the whole life cycle, with practices that protect privacy, particularly relevant for generative AI models, which **Malaysia** supported.

El Salvador also believes that it's essential that the final report includes a reference to the development of ***cryptographic standards that are resistant in the quantum era***, which **Czechia** echoed.

The future permanent mechanism: How to tackle discussions on threats

As discussions moved toward the future of global cybersecurity governance**, the EU *proposed a dedicated thematic group under the Program of Action (PoA)*** to systematically assess threats, enhance security, and coordinate capacity-building efforts. **The USA** and **Portugal** reinforced the urgency of this initiative, calling for a flexible yet permanent platform to address cyber threats, particularly ransomware.

Several countries stressed ***the importance of sector-specific security measures***. **Malaysia** highlighted the need to tailor protections for different industries, while **Mexico** advocated for harmonised cybersecurity standards and multistakeholder cooperation across the digital supply chain. **Mauritius** and **Malawi** reaffirmed the importance of upholding international cyber norms, with **Malawi** emphasising continued dialogue within the UN Open-Ended Working Group (OEWG).

Australia and **Canada** pushed for ***linking emerging threats to responsible state behaviour under international law***, with **Canada** calling for thematic groups to enable deeper discussions beyond general plenary meetings. **Switzerland** and **Germany** agreed, underscoring the need to first establish a shared understanding of threats before implementing coordinated responses. **France** called for shifting from merely identifying threats to actively developing solutions, proposing that expert briefings guide working group discussions.

AI security also emerged as a key concern. **Malaysia** stressed the role of AI developers in cybersecurity, while **Argentina** highlighted the private sector's responsibility in addressing AI-related threats. **Italy** pointed to the recent Joint High-Level Risk Analysis on AI, which provides recommendations for securing AI systems and supply chains.

Cybersecurity at the crossroads: Conflict, crime, and paths to cooperation

As discussed in July 2025[49]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[50] Discussions on emerging and existing threats reflected growing concern among states over the evolving complexity of the cyber threat landscape, with particular attention to ransomware, commercially available intrusion tools, and the misuse of AI and other emerging technologies. While there was broad recognition of new risks, debates emerged around how far the OEWG's mandate should extend—especially regarding cybercrime, disinformation, and data governance—and how to balance security concerns with development priorities and international legal frameworks.

Promoting peaceful use of ICTs – or acknowledging the reality of cyber conflict?

One of the key tensions in the final OEWG discussions on emerging cyber threats was the clash between *aspiration and reality*—specifically, ***whether the final report should promote the use of ICTs for exclusively peaceful purposes or instead focus on ensuring that their use, even in conflict, is constrained by international law.***

Several countries argued that the time for idealistic appeals is over. ICTs are already being used in conflicts and hybrid operations, often below the threshold of armed conflict, combining cyber activities with other non-conventional tools of influence. These states (including **the USA**, **Italy**, **El Salvador**, and **Brazil**) emphasised that acknowledging this reality is essential to advancing responsible behaviour. Malicious cyber operations, often attributed to state-sponsored actors, have targeted critical civilian infrastructure and democratic institutions (as noted by **Albania**).

Therefore, these countries pushed to remove or soften references to the exclusive peaceful use of ICTs. Their priority was to reassert that when ICTs *are* used, including in conflict contexts, their use must comply with international humanitarian law (IHL) and broader international law. In this context, there was also a call to reaffirm the obligation to protect civilians from harm during cyber operations in armed conflict—reflected in the *Resolution on protecting civilians and other protected persons and objects against potential human costs of ICT activities during armed conflict*, adopted by the 34th International Conference of the Red Cross and Red Crescent in October 2024 (referenced by **Switzerland** and **Brazil**).

On the other side, a group of states insisted on keeping strong language around the exclusive peaceful use of ICTs (such as **Iran**, **Pakistan**, **Indonesia**, **Cuba**, and **China**). ***They feared that weakening this reference could be interpreted as legitimising the use of force in cyberspace.*** While some of these countries acknowledged that ICTs have been used in conflict, they consider reaffirming the peaceful-use principle as a necessary political signal—a way to reinforce global norms and discourage militarisation of cyberspace. **China**,

---

[49] Andrijana Gavrilovic, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Vladimir Radunovic, and Jeanne-Louise Roellinger, 'UN OEWG concludes, paving way for permanent cybersecurity mechanism,' Digital Watch Observatory, 17 July 2025, https://dig.watch/updates/un-oewg-concludes-paving-way-for-permanent-cybersecurity-mechanism.
[50] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

for example, pointed out that the principle of 'exclusively peaceful purposes' has long been part of the OEWG consensus and should remain as a shared aspiration.

The outcome: The aspiration to promote ICTs for exclusively peaceful purposes was softened by removing 'exclusively,' while a new reference acknowledges the need to use ICTs in a manner consistent with international law. A previous reference stating that ICT use 'in a manner inconsistent with the framework … undermines international peace and security, trust and stability' was removed.

Cybercrime and international security: A growing intersection?

Another divisive debate was whether cybercrime belongs in a process focused on international peace and security. A broad group of delegations—including **the EU**, **the USA**, **Canada**, **the UK**, **Switzerland**, **Brazil**, **El Salvador**, and **Israel**—***argued that cybercrime has become part of this agenda too***. They emphasised the growing role of criminal actors operating in alignment with state interests or from state territories with impunity. According to this group, the cybercriminal ecosystem—offering tools, malware, and even full-spectrum capabilities—is increasingly exploited by state-backed actors, blurring the lines between criminal activity and state behavior. Ignoring this overlap, they warned, would be negligent.

In contrast, **Russia**, **China**, **Iran**, **Cuba**, **Belarus**, and **several others** opposed including cybercrime in the final report. They ***insisted that criminal acts in cyberspace are distinct from those that threaten international peace*** and should remain within specialised forums such as the Ad Hoc Committee on Cybercrime. Equating the two, they argued, risks expanding the OEWG's mandate beyond its intended scope.

A number of countries (**Canada**, **the USA**, **Japan**, **the UK**, **Australia**, **South Korea**, **Malaysia**, **Qatar**, and **Pakistan**) ***confirmed concerns about cryptocurrency theft and its role in financing malicious cyber operations,*** seeing this as a growing security issue. Others, notably **Russia** and **Iran**, ***pushed back, arguing that this—like cybercrime and other socioeconomic topics—falls outside the OEWG's mandate.***

The outcome: The final report noted that criminal activities 'could potentially' impact international peace and security.

Ransomware was one of the few specific threats that saw wide support for inclusion in the final report. Countries like **the USA**, **Canada**, **the UK**, **Germany**, **the Netherlands**, **Brazil**, **Malawi**, **Croatia**, **Fiji**, and **Qatar** stressed that ransomware poses a growing threat to national security and critical infrastructure, and requested that it be addressed with a dedicated paragraph in the final report. Several African states (including **Nigeria on behalf of the African Group**) noted its damaging impact on state institutions and regional bodies. **Costa Rica** pointed to the disruption of essential services, while **Germany** called for further discussion on applicable norms and legal frameworks, and **Cameroon** called for targeted capacity-building and cooperation—including through regional mechanisms like AFRIPOL. A human-centric approach was proposed by **Malawi**, **Colombia**, the **Netherlands**, and **Fiji**, while others (**Russia**, **China**) warned against overemphasising ransomware and argued it remains within the domain of cybercrime discussions.

The outcome: Ransomware remains mentioned in the final report, though a dedicated paragraph was not added.

Critical infrastructure: Shared concern, differing priorities

The protection of critical infrastructure (CI) and critical information infrastructure (CII) emerged as a shared concern in the OEWG discussions, especially for developing countries. Many states—particularly from Africa and the Pacific—highlighted how increased digitalisation and foreign investment in infrastructure have heightened their exposure to cyber threats. **Malawi** pointed to a breach in its passport issuance system in 2024, while **Costa Rica** recalled the crippling impact of cyberattacks on public services. For these states, safeguarding CI is not only a national security issue but essential for social and economic resilience.

Several delegations, including **Croatia** and **Thailand**, stressed the vulnerability of CI to criminal and advanced persistent threats (APTs). **Croatia** warned of non-state actors targeting weakly protected systems—the 'low-hanging fruit'—especially in countries with limited defences, calling for capacity building that avoids deepening the gap between developed and developing countries. **Thailand** emphasised that APTs can severely disrupt essential services, with potentially cascading effects on national stability. The importance of tailored assistance to protect CI, including cross-border infrastructure like undersea cables, was echoed by **the EU**, **the USA**, **the Pacific Islands Forum**, and **Malawi**—underscoring the global stakes involved. **Ghana** and **Fiji** underlined that each state must determine for itself what qualifies as critical. **Russia** opposed listing specific sectors—like healthcare, energy, or finance—in the final text, arguing such references could imply a one-size-fits-all approach. Meanwhile, **Israel** proposed adding the word 'malicious' before 'ICT attacks' in the final report—it was not explained, though, if there are non-malicious attacks, but an edit was ultimately accepted.

The EU and **the USA** also highlighted political risks, including threats to democratic institutions and electoral processes, while **the USA** raised concerns about pre-positioning of malware within CI by potential adversaries, though the lack of consensus kept this issue out of the final report. Still, the overall discussion reflected growing agreement that CI protection must be a core focus of future international cooperation, with stronger commitments and action-oriented measures.

The outcome: A specific list of critical infrastructure was removed from the final report, but protection of cross-border CI was newly emphasised, along with the inclusion of security-by-design in the context of vulnerabilities and supply chains.

Commercial intrusion tools: A market of growing concern

A particularly vivid discussion continued around the risks posed by the growing global market for commercial ICT intrusion capabilities, or spyware. Several delegations (**the EU**, **the UK**, **South Korea**) explicitly recognised this market as a growing threat to international security, but also to intellectual property (**the EU**). **Ghana** drew attention to the Pall Mall process—an initiative aimed at curbing irresponsible proliferation of such tools—as a complementary effort that should inform the OEWG's work. **Brazil** and others emphasised the risk of irresponsible use, while **Israel** raised the issue of the 'illegitimate dissemination' of such tools—implicitly suggesting that their spread can sometimes be legitimate, depending on context.

Debates intensified around conditions for lawful use of commercial intrusion tools. A range of countries (**South Africa**, **Iran**, **France**, **Australia**, **Fiji**, **the UK**) stressed that ***any***

use must be consistent with international law, legitimate and necessary, and—in some views—aligned with the UN framework on responsible state behaviour.

However, **Russia** and **Iran** ***resisted tying the use of intrusion capabilities to the framework of responsible state behaviour***, warning that this might make the framework seem legally binding and blur the line between voluntary norms and law. **Israel** further argued that when used in line with the UN framework, such tools should not be seen as threats to international peace. Some states (**South Africa**, **Australia**, **Pakistan**, **France**) ***supported the idea of safeguards and oversight mechanisms***, but others (**Iran**) noted these had not been fully discussed and could be addressed later. Meanwhile, **Russia** questioned whether the use of commercial intrusion tools for unauthorised access could ever truly align with international law, proposing to delete such references entirely.

The outcome: Concerns over commercially available intrusion tools were retained in the final report, calling for 'meaningful action' and use consistent with international law.

Emerging technologies: Risks vs opportunities

Debates around emerging technologies reflected a split between states advocating for proactive recognition of risks and those cautioning against overemphasis. Many countries—especially from the Global South (**Indonesia**, **Qatar**, **Singapore**, **Thailand**, **Colombia**, **Fiji**, **the African Group**)—***called for attention to the security implications of AI, IoT, cloud computing, and quantum technologies***. They highlighted the dual-use nature of these tools, particularly AI-generated malware, deepfakes, and synthetic content, and stressed that such technologies are already being misused in ways that could threaten international peace (as noted by **Indonesia** and **Mauritius**). ***In contrast, tech-leading states*** like **the USA** and **Israel** ***warned against placing disproportionate focus on risks, arguing it could overshadow opportunities***. **The EU**, meanwhile, urged caution to avoid duplicating work done in other forums, particularly on AI.

In practical terms, many states (**Canada**, **UK**, **El Salvador**, **Pakistan**) ***supported the deployment of post-quantum cryptographic solutions***, though ***others*** (**Russia**) ***considered such steps premature***. There was also strong support (**UK**, **Canada**, **Malaysia**, **Qatar**, **Fiji**) for ***naming specific emerging infrastructures—like 5G, IoT, VPNs, routers, and even data centres and managed service providers—as relevant to security discussions.***

Malaysia highlighted the need for ***changing the language related to technologies to terms that are also understandable to technical communities*** – a useful reminder that these processes shouldn't be left to diplomats alone. Still, some states (**Russia**, **the USA**, **Israel**) ***pushed to streamline or remove these references, citing concerns over technical detail and the need for broader consensus***.

The question of ***whether technologies are neutral sparked philosophical disagreement***—**Cuba** and **Nicaragua** said no; **Switzerland** reminded that the agreed language in the third APR from 2024 (paragraph 22) says yes.[51]

[51] Digital Watch Observatory, 'OEWG 2021–2025 Third Annual Progress Report (APR).'

The outcome: In the final report, risks from emerging technologies were underlined with adjusted specific terminology, while the paragraph on AI and quantum was shortened, though it still references LLMs and quantum cryptography.

New emphasis: Data, disinformation, and supply chain security

The growing strategic importance of data governance was emphasised by several states. **Türkiye** called for stronger protections around cross-border data flows, personal data, and mechanisms to prevent the misuse of sensitive information, highlighting the need to integrate data security into broader risk management frameworks. **Mauritius** linked data and responsible innovation, while **China** reiterated its long-standing proposal for a global data security initiative that could guide international cooperation in this domain.

Disinformation—particularly the use of deepfakes and manipulated content to destabilise institutions—was raised as an urgent and evolving threat. **The African Group**, represented by **Nigeria**, emphasised its damaging impact on post-conflict recovery and political transitions, especially in fragile states. **Egypt** echoed this concern, warning that misinformation campaigns disproportionately affect developing countries, increasing their risk of relapse into instability. **China** added concerns about the politicisation of disinformation, especially in the context of attributing cyber incidents.

On supply chain security, states agreed about the importance of adopting a security-by-design approach throughout the ICT lifecycle. The proponent, **Ghana** – supported by **Colombia**, **the UK**, and **Fiji** – stressed this as a baseline measure to address vulnerabilities. **Türkiye** added that global standards and best practices must be matched by practical implementation frameworks that consider varying national capacities and promote trust across jurisdictions.

Partnerships and cooperation: Making cybersecurity work in practice

The OEWG discussions underscored strong support for enhancing public-private partnerships (PPP) and the role of CERT-to-CERT cooperation as practical tools in addressing cyber threats. A wide range of states—the **EU**, **Canada**, **Indonesia**, **Ghana**, **Singapore**, **Malawi**, **Malaysia**, **Fiji**, and **Colombia**—welcomed explicit recognition of these mechanisms. Several countries (e.g. **Mauritius**, **Thailand**) stressed the growing importance of cross-regional cooperation, particularly as cyber threats increasingly affect privately owned infrastructure and cross-border systems. **The EU** called for greater multidisciplinary dialogue among technical, legal, and diplomatic experts.

Switzerland and **Colombia** ***emphasised the role of regional organisations as facilitators for implementing the global framework***. **Singapore** offered the newly established ASEAN regional CERT and information-sharing mechanism as a model.

While many acknowledged the expanding role of the private sector, **Türkiye** ***noted that its responsibilities remain insufficiently defined***, suggesting further dialogue is needed to clarify how private actors can contribute to addressing systemic vulnerabilities and managing major incidents. Türkiye also suggested the UN Technology Bank to support cybersecurity capacity building for least developed countries (LDCs) as part of broader digital transformation efforts and promoting secure digital development.

Norms, rules, and principles of responsible behaviour of states

The start of the debate on the implementation of existing norms and the elaboration of new norms

As discussed in December 2021[52]

The discussions on norms, rules, and principles of state behaviour in cyberspace and their applicability in cyberspace started out closely related to the nature of the 2015 and 2021 UN GGE reports and the 2021 OEWG reports.[53]

The majority of the states – **Australia, Colombia, Costa Rica, the EU** on behalf of its member states, the candidate countries **Montenegro**, the **Republic of North Macedonia**, and **Albania** the country of the stabilisation and association process, and potential candidate **Bosnia-Herzegovina** as well as **Ukraine, the Republic of Moldova and Georgia** (**EU**), **Egypt, Estonia, France, Fiji, Germany, India, Indonesia, Italy, Japan, Malaysia, Mexico, the Netherlands, Nigeria, Republic of Korea, Singapore, South Africa, Switzerland, Ukraine** (in national capacity)**,** and **the UK,** agreed that the ***previous UN GGE and OEWG reports, including corresponding UN GA resolutions*** adopted by consensus ***build an acquis for further discussions on the position, role, and implementation of the voluntary non-binding norms, rules and principles of state behaviour in cyberspace.***

Australia, **Colombia**, **the EU**, **Estonia**, **France**, **Germany**, **India**, **Indonesia**, **Italy**, **Japan**, **Malaysia**, **Mexico**, **the Netherlands**, **Nigeria**, **Republic of Korea**, **Singapore**, **Switzerland**, **Ukraine** and **the UK** wanted to build upon this acquis in the OEWG and perceived ***enhancing the understanding of, and implementing the existing norms as the best way forward***.

According to this group of states, norms are based in international law and do not replace states' binding obligations under international law. Norms play an essential role in introducing predictability and transparency in inter-state behaviour; Therefore, these states consider the implementation of norms a confidence-building measure. As expressed by the **Netherlands**, the order of priority should be first to implement the existing norms, clarify, and elaborate them, then, only when inevitable, create new norms. **The UK** pointed out that the starting point for any proposals for new norms must find consensus and not duplicate, rewrite, or undercut already agreed-upon norms. This group of states recognised the need for ***capacity building on national and regional levels for the norm implementation***.

---

[52] Digital Watch Observatory, *UN OEWG 2021–2025 – Rules, Norms, and Principles of Responsible State Behaviour in Cyberspace*, 15 December 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/rules-norms-and-principles-of-responsible-behaviour-of-states.

[53] UNGA, *Developments in the Field of Information and Telecommunications*, A/RES/70/174, UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/76/135), and UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/AC.290/2021/CRP.2).

Many states shared their national initiatives, policies, and regulatory measures already in place to implement the norms.

India expressed the need for the development of ***mechanisms for ensuring adherence to and implementation of the norms***. According to India, the acquis forms an excellent foundation to build upon the superstructure for the responsible behaviour of states.

Iran referred to its previous statement on the matter, stating that the norms are ambiguous, that there needs to be an agreement on terminology, and that the implementation of norms is premature.

Iraq and **Pakistan** voiced support for the ***OEWG's work to further elaborate norms***. **South Africa** wanted the ***states to exchange their views*** on the need for further development of norms through evaluating, updating, and refinement of the existing norms, while **Jordan** called for ***strengthening the capacity to be able to elaborate norms***.

Egypt called for elaboration, implementation of norms, and related capacity building. However, the result of the OEWG should be, according to Egypt, an agreement on recommendations where the ***existing norms may be codified into binding rules***.

China, **Cuba**, **Pakistan**, **Syria**, and **Russia** and are of the opinion that ***norms need to become legally binding regulations***. While **China**, **Cuba**, **Pakistan and Syria** see the current norms being transformed into binding ones, **Russia** wanted to undertake efforts to broaden the list of norms to create a foundation for a new universal legally binding instrument. **Cuba** does not see the 2015 UN GGE report as a basis for the work of OEWG, as it was not approved by all UN member states.

Two countries – **Costa Rica and Fiji** – spoke about ***the intersection of cybersecurity and cybercrime***. **Costa Rica** referred to ransomware attacks by private or non-state actors operating on foreign territory. As cybercrime and cybersecurity are connected, **Costa Rica** took note of the UNIDIR's Report on connections and engagement between the UN's First and Third Committee processes.[54] Fiji highlighted cybercrime regulation on the national and international level, specifically the Budapest Convention Against Cybercrime, as an approach to lend predictability and stability, and a tool for states to manage the use of ICTs and confront cybercrime. Fiji also took note of work by the Ad Hoc Committee on Cybercrime.

With respect to the upcoming work within the **OEWG**, states mentioned the following as the most pressing issues needing attention: ***attribution*** **(Pakistan, Switzerland, India**), ***due diligence*** (**France**, **Germany**, **Republic of Korea**), and ***respect for human rights*** (**France**, **the UK**, **the Netherlands**). **India** also specifically mentioned the need to ***protect the public core of the internet.***

Many delegates, such as **the EU**, **Estonia**, **Indonesia**, **Italy**, **Malaysia**, **Mexico**, **and South Africa, *supported the use of the national survey of implementation of norms as proposed by Australia and Mexico.***[55]

---

[54] Joyce Hakmeh and Kerstin Vignard, *ICTs, International Security, and Cybercrime: Understanding Their Intersections for Better Policymaking* (Geneva: UNIDIR, October 11, 2021), https://unidir.org/publication/ICTs-international-security-and-cybercrime.

[55] Australian Government, *Joint OEWG Proposal: Survey of National Implementation*, April 2020, https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf.

Norms: ‘Yes, but’

As discussed in April 2022

The norms of responsible state behaviour in cyberspace, outlined in the agreed framework, were reiterated by a number of countries. Yet, while some states, like **the EU**, **Australia** and **Japan**, wanted to ***focus on the implementation of the current norms***, others, like **Russia**, **Belarus**, and **Cuba,** find them insufficient. The countries called for the ***development of a new single international, legally binding instrument.*** Due diligence obligations, protection of critical infrastructure, and attribution were discussed in detail.[56]

Argentina, Austria, Australia, Brazil, Canada, Chile, Costa Rica, Estonia, France, Germany, Japan, Kenya, the Netherlands, Portugal, the Republic of Korea, Singapore, the UK, the USA, Uruguay, Vietnam, the EU and its member states, the candidate countries, **North Macedonia, Montenegro,** and **Albania**, the country of stabilisation and association process and potential candidate, **Bosnia and Herzegovina**, as well as **Ukraine**, **the Republic of Moldova**, **Georgia**, and **San Marino**, stated that the adoption of 2010, 2013, 2015, 2021 GGE and 2021 OEWG consensus reports provides an acquis, is the basis for the work of the OEWG 2021-2025, and has ***reaffirmed a set of foundational norms of responsible state behaviour in cyberspace***. These delegations voiced the opinion that ***discussions at the current OEWG should be focused on the implementation of the existing norms*** and the guidance on how to proceed with such implementation.

Based on 2015, 2021 GGE and 2021 OEWG reports, which guide UN member states to review the steps taken to implement the recommendations of the reports, identify barriers to implementation and specific capacity gaps that limit implementation, **Australia** collectively with **Argentina, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Islands Forum member states, Poland,** and **South Africa** ***presented an online national survey tool***.[57] This tool aimed to help states determine the implementation of norms, contribute to accountability, share best practices, and serve as a global points of contact (PoC) directory. **Australia** proposed that the OEWG recommend that states use the survey to voluntarily self-assess the implementation of norms and recommendations.

The Netherlands, the USA, Estonia, and **the UK** pointed out ***the importance of safeguarding the public core of the internet and internet freedom***, with an emphasis on the rights to access information, freedom of expression, peaceful assembly and association online.

Regarding ***specific norms that deserve the attention of the OEWG at the time of discussions***, the **EU, France, Germany, the Republic of Korea, Switzerland,** and **Vietnam** highlighted ***due diligence obligations in norm 13c of the 2015 UN GGE report*** (states should not knowingly allow their territory to be used for internationally wrongful acts using ICT).[58]

---

[56] Diplo Team, ‘What’s New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.’
[57] United Nations Institute for Disarmament Research (UNIDIR), *Cyber Policy Portal*, accessed July 27, 2025, https://cyberpolicyportal.org/en/.
[58] UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/70/174).

Haiti, the Netherlands, Kenya, Malaysia, Portugal, Switzerland, Ukraine, and **Uruguay** pointed out the importance of the ***protection of critical infrastructure (norm 13f)***. **Singapore** also stressed the importance of critical infrastructure in maintaining the integrity of political and electoral processes. **China** welcomed the discussion on defining and protecting critical infrastructure based on the principle of sovereignty.

Haiti and the **USA** recalled ***norm 13b on attribution***, with the **USA** emphasising its importance in the context of public attribution of state-sponsored malicious cyber activities. **China** stated that in the investigation of cyber incidents, any conclusion should be supported by complete and sufficient evidence. According to **China**, the publication of attribution conclusions will aggravate misunderstanding and miscalculation among states and even lead to confrontation.

Norm 13i on the integrity of supply chains was stated to be of utmost importance by **India, France, El Salvador, Switzerland,** and **Malaysia**. **China** called for the adoption of a consensus on the development and implementation of rules and standards for supply chain security.

Iraq and Nicaragua, on the other hand, pointed out that the ***norms in paragraph 13 of the 2015 UN GGE report and its recommendations are insufficient and should be revisited***.

Regarding the ***development of new norms***, **South Africa** and **Kenya** stated that the development of new norms should not detract from the implementation of the existing norms. Further development of norms, rules, and principles should be understood as a process of evaluating and updating where necessary and refining rather than seeking to develop a completely new set of norms.

India stated that the ***norms in the existing form need a complementary framework*** to outline the mechanisms of cooperation, information exchange, trust-building initiatives, and sharing of best practices. The OEWG should consider building an additional layer of understanding on the existing norms and may develop additional ones on an as-needed basis. **Egypt** suggested the ***development of a compilation document that would include the agreed norms and recommendations*** and relevant processes, with a focus on identifying gaps and overlaps and developing binding rules that reflect the ICT environment and differentiated capacities of member states.

On behalf of the Non-Aligned Movement, **Indonesia** pointed to the need for indicators and parameters to ***measure the level of effectiveness of the implementation of norms by using a voluntary national survey***.

Vietnam expected that the OEWG would ***discuss the development of an international framework of rules and norms*** in line with international law. Vietnam stated that in the meantime, all states should observe the widely acknowledged norms, including those developed within the GGE processes. **Pakistan** believes that adherence to the norms is contingent upon equipping member states with skills and technologies and clearly defining the modalities for the implementation, while ***the goal should be a new binding legal instrument.***

Belarus, China, Cuba, El Salvador, Iran, Nicaragua, and **Russia** stated that ***the current norms are not sufficient and need further discussion and development through the***

work of the OEWG. According to these states, the outcomes of the GGE reports and the 2021 OEWG Report (Chair's Summary) serve as guidance for clarifying and elaborating the norms.

China, Cuba, El Salvador, Iran, Pakistan, and **Russia** called for ***a new binding legal instrument to govern responsible state behaviour in cyberspace***. **Russia** suggested developing a UN convention on international information security. **China** pointed out their proposal on the Global Initiative on Data Security as a blueprint for possible global rules.

The ***proposed Programme of Action (PoA)*** as a permanent and inclusive platform for the implementation of current norms and capacity development was supported by **Argentina, Canada, Chile, Egypt, the EU, France, Germany, Japan, Jordan, Switzerland,** and **Ukraine.** Delegations reiterated the importance of regional engagement through a variety of forums, such as the Arab League, ASEAN, the OAS, the GFCE, and ITU.[59]

Clarifying the path ahead: Norms implementation vs elaboration

As discussed in July 2022[60]

In July 2022, states met at the third substantive session to adopt the group's first APR.[61] ***The discussion revolved around whether the OEWG should focus on the implementation of existing voluntary norms of responsible state behaviour, the development of new norms, or both.***

The majority of the states, such as **Germany**, **the USA**, **Canada**, and **Czechia**, have stated that ***focus should be given to the implementation of existing norms,*** with states working together to provide additional guidance to advance norm implementation, as well as elaborating on the conclusions and recommendations. **Kenya** proposed setting up ***OEWG work groups to share best practices***, especially on how the existing rules, norms and principles can be contextualised in translation to national policies.

Iran, however, was stridently ***against calling the proposals for implementation of existing norms 'action-oriented' proposals***. That would prioritise the sufficiency of implementing the norms and dismiss the necessity of negotiating a legally binding instrument, Iran noted. Adopting a concrete action-oriented approach would convert the OEWG into a proposed PoA structure to implement the framework of the GEE 2015 report, which is contrary to the mandate of the OEWG.

Iran and **Russia** remained ***adamant on the need for new norms***, with **Russia** ***suggesting new legally binding norms***, which were ***opposed*** by **Canada** and **Mauritius**.

Conversely, **South Africa**, **Botswana**, and **the Democratic Republic of Congo** stressed that ***developing additional norms can't be done at the same time as the***

---

[59] Digital Watch Observatory, *UN OEWG 2021–2025 – Rules, Norms, and Principles of Responsible State Behaviour in Cyberspace*, 30 March, 2022, https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-rules-norms-and-principles-of-responsible-state-behaviour-in-cyberspace.
[60] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.'
[61] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*.

implementation of existing ones. New norms will place a burden on small developing states.

Some countries, such as **Peru**, **Nicaragua**, **Indonesia**, **the Republic of Korea**, and **Singapore**, ***underscored the implementation of the existing norms but did not oppose the development of new ones***. **Singapore** noted that areas which could benefit from discussions on new norms or further implementation of the existing norms include the protection of electoral infrastructure and the general integrity and availability of the internet.

The outcomes: The first APR acknowledges that the states proposed that additional norms could continue to be developed over time. The term 'action-oriented' remained in the report as well.

Another strain of conversation around norms was ***developing common understandings on technical ICT terms***. **China**, **Iran**, **Cuba**, **Lao PDR**, and **Nicaragua** welcomed it. **Australia** was against it, while **the Netherlands** and **the USA** proposed that states could share national understandings of ICT terms for the purpose of transparency.

The outcome: Developing common understandings on technical ICT terms has not been included in the first APR.

Norms implementation: At the forefront of discussions

As discussed in March 2023[62]

The discussions surrounding the rules, norms, and principles of responsible behaviour of states in cyberspace centred on how to effectively implement those behaviours.

Some countries, like **Russia** and **Syria,** argued that the ***existing voluntary and non-binding rules of state behaviour don't effectively regulate the use of ICTs*** to prevent inter-state conflicts and promote the peaceful use of ICTs. They ***proposed a legally binding multilateral international treaty under the auspices of the UN***. **Egypt** stressed that the ***development of new principles and norms*** to close existing gaps at the international level ***does not conflict with the normative framework of responsible behaviour in the use of ICT.*** Other countries, including **Sri Lanka** and **Canada** (among others in the second session), ***critiqued Russia's proposal, stressing the importance of implementing the 11 norms of responsible behaviour before negotiating new legal frameworks***.

Due diligence implementation was emphasised as one of the key aspects of the framework for responsible state behaviour. **France**, for instance, noted that due diligence norms 13(C) and 13(H) are based on the principle of state sovereignty, which means that states are responsible for taking adequate and reasonable measures to respond to malicious activities that originate on their territory.

France proposed creating ***a practical guide that would help facilitate the implementation of norms 13C*** (states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs) ***and 13H*** (states should respond to appropriate

[62] Gavrilovic, Grottola, Ittelson, Kazakova, Petit-Siemens, Stadnik, 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session.'

requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty).

Emphasising due diligence, many representatives also discussed ***the need to protect critical infrastructure***. **Singapore** stressed the need to protect cross-border critical internet infrastructures (CIIs) as vital infrastructure to international trade, financial markets, global transport, communications, health, and humanitarian action. Disrupting or undermining the operations of these CIIs could impair the delivery of critical services to populations and have serious implications for international peace and security.

Persistent divergence: Existing norms vs calls for new norms

As discussed in May 2023[63]

The implementation of already agreed-upon norms was at the centre of discussions in May 2023, as a majority of countries continued to stress the implementation of the already established 11 voluntary, non-binding norms of responsible state behaviour in the 2015 GGE consensus report, unanimously endorsed by the UN General Assembly (UNGA).[64]

Several delegations emphasised ***the need for more focused discussions*** and highlighted ***the crucial role of capacity building*** in ensuring the practical implementation and realisation of norms beyond paper. Once again, a needs-based approach to capacity building for norms implementation was underlined.

The emphasis on practical implementation rather than mere endorsement of norms highlights nations' need for tangible actions to promote responsible state behaviour in cyberspace. Capacity building emerges as a crucial element in this regard, emphasising the importance of equipping nations with the necessary tools and knowledge to effectively implement these norms.

To offer more concrete guidance on norms implementation, **Singapore** announced that it started ***developing a preliminary norms implementation checklist*** with UNODA and ASEAN member states under the UN Singapore Cyber Programme. The checklist was envisaged as a simple guide for a set of actions that countries could take towards implementing the 11 norms. A preliminary checklist consisting of norms G, J, and K has been developed. Singapore believes it could serve as a guide and reference for all states and support them in their implementation of norms

Canada had also been working with stakeholders and states like **the USA** and the **Netherlands** to ***develop a paper with additional guidance on norms in general***, starting with the norms on critical infrastructure, and including the essential role that civil society would have to play in implementing them. They highlighted the work of the Cyber Peace Institute, Microsoft, the Royal United Services Institute, and the German think tank Stiftung

[63] Gavrilovic, Kazakova, and Petit-Siemens, 'What's new with cybersecurity negotiations? The informal OEWG consultations on capacity building.'
[64] UNGA, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/70/174).

Neue Verantwortung (SNV) in the drafting of the paper.

The EU and **Japan** suggested ***the PoA could guide national efforts to implement frameworks of responsible state behaviour***.

Some delegations questioned the existing norms and challenge their scope. They argued that the process of norm-setting in cyberspace should be continuous and adaptable to address emerging challenges in the digital domain. These countries were in favour of elaborating new norms. For instance, **China** proposed formulating new rules that effectively address global issues around data security, cross-border data flow and the protection of personal information. **Bangladesh** advocated for a flexible framework around norms creation in cyberspace, noting that developing additional norms should be seen as an ongoing exercise of evaluating, updating, and recalibrating the norms based on needs, rather than when a one-time event arises. In **Iran**'s view, any agreed-upon norms should be discussed within the OEWG forum, which should hold dedicated sessions and a thematic subgroup to draft a final set of norms prior to their operationalisation.

The discussion surrounding the formulation of new norms in cyberspace highlighted the evolving challenges in governing this domain. On the one hand, countries may encounter difficulties in operationalising these rules, due to the ever-changing cyber landscape. On the other hand, when faced with an ever-changing list of norms, operationalising rules on responsible state behaviour could be challenging.

An alternative perspective is that ***the operationalisation of the established 11 norms could serve as a foundation for the creation of new norms that reflect the ongoing challenges in cyberspace***. Their operationalisation would require a flexible and responsive framework to create norms around cyber-related issues as they emerge.

Iran argued that ***before taking steps towards the operationalisation of norms, the OEWG needs to agree on a final and comprehensive list of obligatory and universal norms***. The country emphasised that all norms, rules, and principles of responsible behaviour of the state must be discussed and adopted by consensus within the OEWG.

Existing fault lines resurface: Implementing or developing norms

As discussed in July 2023[65]

In July 2023, states met at the fifth substantive session to adopt the group's second APR.[66] The existing fault lines in opinions resurfaced. ***Most member states supported the implementation of the 11 existing voluntary norms before exploring the need for additional norms***. According to these member states, the development of new norms is premature.

On the other hand, **Russia, China, Cuba,** and others consider focusing on implementing existing norms to be outside of the mandate of the OEWG and think that ***the development***

[65] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's fifth substantive session'.
[66] Digital Watch Observatory, *OEWG 2021–2025 Second Annual Progress Report (APR)*.

of additional norms and new legally binding obligations should be the main agenda of the OEWG.

Some states were not satisfied with the level of emphasis put on implementation: for instance, **Australia** suggested that in the section on rules, norms and principles para 23 f) notes that states stressed the need for further focus discussions on *implementing* the rules, standards, and principles of responsible state behaviour in the use of ICTs, adding the word 'implementing' to the original phrasing.

The outcomes: The final wording of the second APR includes a focus on implementing norms to which the opposing states agreed in the spirit of goodwill and compromise. A mention of the possibility of future elaboration of new legally binding obligations within OEWG found its place in the section on international law.

Many states emphasised ***the importance of the private sector in the integrity, stability, and security of supply chains and cyberspace***. Other discussions related to ***critical infrastructure, critical information infrastructure, and the safety and integrity of supply chains***.

The outcome: These references were included in the second APR.

A group of states also resurrected the ***proposal to establish a voluntary glossary of national definitions of technical ICT terms***, which was declined by most states as they needed more consensus. Suggestions were made to include this glossary as part of CBMs.

This time, ***states disagreed over a new topic – a glossary of technical terms***. Some states (e.g. **Switzerland**, **the UK**, **New Zealand**, **South Africa**, etc.) did not support the proposal and asked to remove this from the second APR. They argued that states could more usefully continue to share national policies and their statement on international law and threat information. Some countries (e.g. **Kazakhstan** and **Iran**) ***disagreed with deleting this proposal.***

The outcome: The reference to the glossary of terms was removed from the final draft of the second APR.

A new proposal on substantiation of accusations was put forward by **Russia**, which suggested ***supplementing the section on norms with the provisions that accusations of wrongful acts with the use of ICTs brought against states must be substantiated***, and that computer incident response must not be politically motivated.

The outcome: The proposal was not included in the second APR.

From implementation guidance to supply chain security: Expanding the norms agenda

As discussed in December 2023[67]

Many delegations shared how they have already begun implementing national and regional norms through policies, laws and strategies. At the same time, some delegations shared the

[67] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Stadnik, 'OEWG's sixth substantive session.'

existing gaps and ongoing processes to introduce new laws, in particular, to protect critical infrastructure (CI) and implement CI-related norms.

Clarifying the norms and providing implementation guidance

Delegations also signalled that ***clarifying the norms and providing implementation guidance is necessary***. **Singapore**, for instance, ***supported the proposal to develop broader norm implementation guidance, such as a checklist***. **The Netherlands** argued that ***such guidance should not only consider the direct impact of malicious cyber activities but also consider the cascading effects*** that such activities may have, including their impact on citizens. **Canada** stressed that ***a checklist would be a complementary tool, formulating voluntary and non-binding guidelines***, while some delegations (e.g. **China** and **Syria**) called for ***translating norms as political commitments into legally binding elements***.

Australia suggested ***first focusing on developing norms implementation guidance for the three CI norms (F, G, and H)***. **China**, in particular, **among many other delegations**, ***expressed the same need to develop guidelines for the protection of CI***. **Portugal** ***proposed the focus on clarifying and implementing the due diligence, including by the private sector in protecting CI***, and **France** ***supported it***.

Norms related to ICT supply chain security and vulnerability reporting

In response to the Chair's query about the ***norms related to ICT supply chain security and vulnerability reporting***, **Switzerland** ***presented the Geneva Manual on Responsible Behaviour in Cyberspace***.[68] This inaugural edition offers comprehensive guidance for non-state stakeholders, emphasising norms related to supply chain security and responsible vulnerability reporting.

At the same time, **the UK** and **France** raised the issue of the ***use of commercially available intrusion capabilities***. **The UK** expressed its concerns about the growing market of software intrusion capabilities. It stressed that all actors, including the private sector, are responsible for ensuring that the development, facilitation and use of commercially available ICT capabilities do not undermine stability in cyberspace.

In addition, **France** highlighted ***the need to guarantee the integrity of the supply chain by ensuring users' trust in the safety of digital products*** and, in this context, cited the European Cyber Resilience Act proposal, which aims to impose cybersecurity requirements for digital products. **China argued that some states abuse these norms by developing their standards for supply chain security and undermining fair competition for businesses**.

China also said ***all states should explicitly commit themselves to not proliferating offensive cyber technologies*** and urged that the so-called term 'peacetime' had never been used in the context of the 11 norms in earlier consensus documents.

New norms vs existing norms

Delegations had divergent views on whether new norms should be developed or not. Some countries supported the idea of creating new norms till 2025 (the end of the OEWG

[68] Geneva Dialogue on Responsible Behaviour in Cyberspace, *Geneva Manual – Chapter 1: ICT Vulnerabilities and Supply Chain Security*, https://genevadialogue.ch/geneva-manual/chapter-1/.

mandate), and, in particular, **China** ***called for new norms on data security issues***. Other delegations (e.g. **Canada**, **Colombia**, **France**, **Israel**, **the Netherlands**, and **Switzerland**) ***opposed the development of new norms and instead called for implementing existing ones***.

South Africa emphasised ***the need to intensify implementation efforts to identify any gaps in the existing normative frameworks*** and whether there is a need for additional norms to close those gaps. **Brazil** stressed that ***the implementation of existing standards is not contradictory to discussing the possibility of adopting specifically legally binding norms*** and thus rejected the idea that 'there is any dichotomy opposing both perspectives'. Brazil expressed its openness to considering the adoption of both additional voluntary norms and legally binding ones to promote a peaceful cyberspace.

Still divided: Competing views on norms development and implementation

As discussed in March 2024[69]

Reflections of the several delegations in March 2024 highlighted the existing binary dilemma: ***should there be new norms or not****?*

Iran, **China and Russia** highlighted once again that ***new norms are needed***. Russia also ***suggested four new norms*** to strengthen the sovereignty, territorial integrity and independence of states; to suggest the inadmissibility of unsubstantiated accusations against states; and to promote the settlement of interstate conflicts through negotiations, mediation, reconciliation or other peaceful means. **Brazil** noted that additional norms will become necessary as technology evolves and stressed that any efforts to develop new norms must occur within the UN OEWG. South Africa expressed that it could support a new norm to protect against AI-powered cyber operations and attacks on AI systems. Vietnam strongly supported the development of technical standards regarding electronic evidence to help verify the origins of cybersecurity incidents.

However, some ***delegations insist that implementing already existing norms comes before elaborating new ones***. **Bangladesh** urged states to collaborate more to translate norms into concrete actions and focus on providing guidance on their interpretation and implementation. **The UK**, in particular, suggested four steps to improve the implementation of the norms by addressing the growing commercial market for intrusive ICT capabilities. The delegate called states to prevent commercially available cyber intrusion capabilities from being used irresponsibly, to ensure that governments take the appropriate regulatory steps within their domestic jurisdictions, to conduct procurement responsibly, and to use cyber capabilities responsibly and lawfully.

Several delegations mentioned the ***accountability and due diligence issues in implementing the agreed-upon norms***. **New Zealand**, in particular, shared that the OEWG could usefully examine what to do when agreed norms are willfully ignored. **France** mentioned that it had continued its work on the due diligence norm C with other countries.

[69] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's seventh substantive session.'

Italy called for dedicated efforts to set up accountability mechanisms to 'increase mutual responsibility among states' and proposed national measures to detect, defend and respond to and recover from ICT incidents, which may include the establishment at the national level of a centre or a responsible agency that leads on ICT matters.

The Chair issued a *draft of the norms implementation checklist* before the start of the session.[70] The document outlines a checklist comprising voluntary, practical measures for implementing responsible state behaviour using Information and Communication Technologies (ICTs). It suggests that states may use this checklist to support their implementation efforts, prioritise capacity building, and exchange best practices in ICT security. Primarily, the checklist serves as a starting point for states, providing actionable steps to bolster their implementation endeavours.

At the national level, implementation efforts include but are not limited to establishing robust national coordination structures like Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). Moreover, developing comprehensive national ICT laws, policies, and strategies is imperative.

Internationally, states are encouraged to actively participate in regional and global ICT processes, fostering the exchange of information and best practices. Furthermore, offering and seeking assistance where necessary strengthens collaborative efforts in upholding responsible state behaviour in ICT usage.

Capacity-building emerges as a central pillar in enabling states to undertake these practical actions effectively. Thus, investing in capacity-building initiatives is imperative for achieving widespread adherence to responsible ICT norms globally.

According to **Egypt**, this checklist must be simplified because it includes duplicate measures and detailed actions beyond states' capabilities. The checklist, Egypt continued, should acknowledge technological gaps among states and their diverse national legal systems, thus respecting regions' specifics. Many delegations have strongly supported the checklist and made recommendations. For example, the **Netherlands** suggested that the checklist include the consensus notion that state practices, such as mass arbitrary or unlawful mass surveillance, may negatively impact human rights, particularly the right to privacy.

Some delegations addressed the Chair's questions on implementing critical infrastructure protection (CIP) and supply chain security-related norms. The **EU** reminded us that it is necessary to look into existing cybersecurity best practices in this regard and gave an example of the Geneva Manual as a multistakeholder initiative to clarify the roles and responsibilities of non-state actors in implementing the norms.[71] **Italy** encouraged the adoption of specific frameworks for assessing the supply chain security of ICT products based on guidelines, best practices, and international standards. Practically, it could include establishing national evaluation and security certification centres for cyber certification schemes. The **Republic of Korea** suggested building institutional and normative foundations to provide security guidelines starting from the development stage of software

[70] Digital Watch Observatory, *UN OEWG Chair publishes discussion paper on norms implementation checklist*, 21 February 2024, https://dig.watch/updates/un-oewg-chair-publishes-discussion-paper-on-norms-implementation-checklist.
[71] Geneva Dialogue on Responsible Behaviour in Cyberspace, *Geneva Manual – Chapter 1: ICT Vulnerabilities and Supply Chain Security*.

products, which can be used in the public sector to protect public services or critical infrastructure from being targeted by cyberattacks. **Japan** suggested adopting the Software Bill of Materials (SBOM) and discussing how ICT manufacturers can achieve security by design.

No consensus yet: States split on norm implementation and development

As discussed in July 2024[72]

In July 2024, states met at the eighth substantive session to adopt the group's third APR.[73] ***Discussions on norms mainly centred around the need to develop new norms or implement existing ones.***

States shared different views: Some delegations, such as **Japan**, **Canada**, **Italy**, **South Korea**, **the Netherlands**, and **New Zealand** mentioned ***they did not support the idea of submitting working papers on proposals for the development of additional norms*** (the language which was proposed in the zero draft of the third APR).[74] **The USA** added that the proposals for new norms with a mere six months' working time remaining in the mandate of the current OEWG are unproductive. **The African Union** supported this view to exclude the language on the development of new norms, arguing that many African states are still in the early stages of understanding this process and don't have enough maturity to keep up with adopting new norms.

Italy added that ***the implementation of existing norms and the development of new ones cannot be considered at the same level***, as there are differences in the level of commitment required by states. This view wasn't supported by several other delegations (e.g. **El Salvador**, **Morocco**, **Russia**, **South Korea**, **Singapore**, **Bangladesh**, **Australia**, and others), who instead took the position that ***the implementation of norms can be complementary to the gradual development of additional norms***; these two processes are not mutually exclusive.

At the same time, ***some states called for stronger language in line with the OEWG's mandate, which is to develop new norms***. **The Dominican Republic** regretted that the development of new norms had been watered down in the text and that the third APR should be redrafted in a balanced manner to adhere to the OEWG's mandate. **Cuba** called for explicitly mentioning the option to develop new legally binding norms. **Syria**, **China**, and **Nicaragua** also disagreed with the view that new norms are not needed.

The outcomes: The final text of the third APR balances both sides. In paragraph 31(h), the APR highlights that 'States affirmed the importance of supporting and furthering efforts to implement norms' and, at the same time, in paragraph 31(j), it recalls the 'mandate of the OEWG […] to further develop the rules, norms and principles of

[72] Gavrilovic, Kazakova, Petit-Siemens, Roellinger, 'OEWG's eight substantive session.'
[73] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR)*.
[74] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Letter dated 29 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_29_May_2024.pdf

responsible behaviour of states and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour'.

Furthermore, the attempt to find a compromise between these different views is evident in paragraph 31(k), which mentions that 'States reaffirmed that additional norms could continue to be developed over time' and that 'the development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel,' which most delegations agreed with. In paragraph 31(l), the thrid APR highlights that 'States proposed that the current OEWG could continue its discussion on the possible development of additional norms.' This wording doesn't provide for commitments or obligations on this issue, but at the same time, leaves the discussion on the development of new norms open.

Chair's proposal for a norms implementation checklist

Most states welcomed the chair's proposal for a checklist to implement voluntary, non-binding norms of responsible state behaviour annexed to the APR, with the understanding that it should serve as a living, voluntary document adaptable to national contexts. ***Some states*** (e.g. **Pakistan**, **Russia**, and **Cuba**) mentioned that ***more time is required to study the checklist***. Therefore, the proposal could be postponed until next year's work cycle. Nevertheless, delegations agreed in discussing the checklist that there is no one-size-fits-all solution to implementing the norms.

The outcomes: **The third APR includes paragraph 33, which informs that 'States will continue efforts to implement norms and to discuss and update the Voluntary Checklist of Practical Actions (Annex A), which is a living document, with a view towards reaching a consensus recommendation on the Voluntary Checklist by July 2025.' Thus, the discussions will continue, and reaching a consensus on the Voluntary Checklist is expected next year.**

Protection of critical infrastructure (CI) and critical information infrastructure (CII)

The protection of CI and CII retook special attention. **The Netherlands** suggested ***putting the specific focus in the third APR on CI and CII***, and **South Africa**, **El Salvador**, **South Korea**, **Mauritius**, **Pakistan**, and **Chile** ***welcomed a special emphasis on CI and CII***. When discussing the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security norm 13(c), which says that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, **Russia** ***proposed to add a clarification that accusations against states for carrying out unlawful acts online should be justified*** and an indication that some of the activities using ICTs are originating from the territory of a named state is not sufficient to ascribe responsibility of a given state for this act. **France** said it would welcome further discussions to continue building a common understanding.

The outcomes: In paragraph 31(c), the third APR underlines the 'importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII)', and in paragraph (d), it emphasises 'the need to continue to strengthen measures to protect all CI and CII from ICT threats'. Russia's proposal for clarification wasn't included with regard to norm 13(c). Paragraph 31(b) includes the proposal of some countries, including France, to 'further discussions in order to continue building

common understandings through exchanges of national and regional experiences in this regard'.

Norms in dispute: Diverging views on implementation vs development

As discussed in December 2024[75]

The discussions on norms in December 2024 highlighted once again the ***division of states on binding vs voluntary and the implementation of existing norms vs the development of new norms.***

The chair invited all delegations to reflect on how states can bridge the divides if the discussion on new norms means that states are not prioritising implementation, and if states can do both. The chair reminded stakeholders that ideas for new norms have come from delegations, but also from stakeholders. He also added that some of the delegations have said it's too late to discuss new norms because the process is concluding (e.g. Canada); However, he reminded that when states began the process, some of the delegations also said it's too early to get into a discussion because it's important to focus on implementation. The chair concluded by noting that 'it's never a good time and it's always a good time'.

First of all, the main disagreement was over ***binding vs voluntary norms as well as implementation of existing norms vs development of new norms*****.** Some states, including **Zimbabwe, Russia, and Belarus**, ***advocated for the development of a legally binding international instrument to govern ICT security and state behaviour.*** They argue that existing voluntary norms are insufficient to address emerging threats.

However, the discussion also served as a platform for new proposals from delegations to achieve a safe and secure cyber environment. Some states also ***proposed specific new norms*** to address emerging challenges.

El Salvador suggested recognising the role of ethical hackers in cybersecurity.

Russia proposed several new norms, including: (a) The sovereign right of each state to ensure the security of its national information space as well as to establish norms and mechanisms for governance in its information space in accordance with national legislation, (b) Prevention of the use of ICTs to undermine and infringe upon the sovereignty, territorial integrity and independence of states as well as to interfere in their internal affairs, (c) Inadmissibility of unsubstantiated accusations brought against states of organising and committing wrongful acts with the use of ICTs, including computer attacks followed by imposing various restrictions such as unilateral economic measures and other response measures, (d) Settlement of interstate conflicts through negotiations, mediation, reconciliation or other peaceful means of the state's choice, including through consultations with the relevant national authorities of the states involved.

[75] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's ninth substantive session.''

Belarus suggested new norms which could include the norm of national sovereignty, the norm of non-interference in internal affairs, and the norm of exclusive jurisdiction of states over the ICT sphere within the bounds of their territory.

China noted that new norms could be developed for data security, supply chain security, and the protection of critical infrastructure, among others.

Additionally, ***some states proposed amending or enhancing the existing norms***:

The EU wanted to see greater emphasis on the protection of all critical infrastructures supporting essential public services, particularly medical and healthcare facilities, along with enhanced cooperation between states. The EU also wanted a priority focus on the critical infrastructure norms 13F, G and H.

El Salvador proposed strengthening privacy protections under Norm E, which **Malaysia**, **Singapore** and **Australia** supported.

UK suggested a new practical action recommending that states safeguard against the potential for the illegitimate and malicious use of commercially available ICT intrusion capabilities by ensuring that their development, dissemination, purchase, export or use is consistent with international law, including the protection of human rights and fundamental freedoms under Norm I, which **Canada**, **Switzerland**, **Malaysia**, **Australia**, and **France** supported.

Kazakhstan proposed: (a) adding a focus on strengthening personal data protection measures through the development and enforcement of comprehensive data protection laws to safeguard personal data from unauthorized access, misuse, or exploitation under the norm E, (b) emphasising the importance of conducting international scenario-based discussions that simulate ICT-related disruptions under Norm G, (c) establishing unified baseline cybersecurity standards will enable all states, respective of their technological development, to protect their critical infrastructure effectively under Norm G, (d) promoting ethical guidelines for the development and use of technologies such as AI under Norm K

Canada suggested adding text under norm G: ‘Cooperate and take measures to protect international and humanitarian organisations against malicious cyber activities which may disrupt the ability of these organisations to fulfil their respective mandates in a safe, secure and independent manner and undermine trust in their work’

In contrast, other states such as the **USA, Australia, the UK, Canada, Switzerland, Italy** and others ***opposed the creation of new binding norms*** and highlighted the necessity to prioritise the implementation of the existing voluntary framework.

In between these two polar opposites, there were states that favoured a parallel development, arguing that the ***implementation and the development of new norms can proceed simultaneously***. These states were **Singapore**, **China**, **Indonesia**, **Malaysia**, **Brazil**, and **South Africa**.

Egypt questioned ***whether states need to discuss enacting a mix of both binding and non-binding measures to deal with the increasing and rapid development of threats***, as well as suggested that states might consider developing a negative list of actions that states are required to refrain from.

Japan called for a priority to focus on the implementation of the norms in a more concrete way. **Russia** called for the same, and suggested that states present a review of their compliance with national legislation and doctrinal documents with the rules, norms, and principles of behaviour in the field of international information security (IIS), which has been approved by the UN. **Russia** submitted its review of national compliance with the agreed norms.[76]

Stalled talks: Little progress amid ongoing divides

As discussed in February 2025[77]

In February 2025, ***the divide persisted between states that prioritise implementing the agreed norms*** (e.g. **Japan**, **Switzerland**, **Australia**, **Canada**, **South Korea**, **Kazakhstan**) ***and those advocating for new, legally binding rules*** (e.g. **Russia**, **Pakistan**, **Cuba**). The former group argued that introducing new norms without fully implementing current ones could dilute efforts, while the latter believes that voluntary norms lack accountability, particularly in crises. **Italy** specifically called for the full implementation of existing cyber norms before introducing new ones.

Among the ***new norms proposed***, **Kazakhstan** proposed a 'norm-on-zero trust' approach, emphasising continuous verification and access controls, although it acknowledged the need to prioritise implementing agreed norms. **El Salvador** repeated its proposal to update norm E regarding privacy and personal data. **China** highlighted that existing norms do not cover data security, while **Vietnam** called for new norms to address emerging technologies and the digital divide.

Some states didn't propose new norms but sought fresh perspectives on existing ones. **The UK** suggested categorising the 11 norms into three themes: Cooperation (Norms A, D, H), Resilience (Norms G, J), and Stability (Norms B, C, E, F, I, K). **France** and **the UK** also reiterated the need for Norm I to address the non-proliferation of malicious tools. **Portugal** emphasised the importance of a common understanding of due diligence. **Italy** prioritised supply chain security, advocating for measures like ICT supply chain security assessments, Software Bills of Materials (SBOMs), national security evaluation centres, and cybersecurity certification schemes.

Some countries (e.g. **Malaysia** and **Brazil**) ***proposed a balanced approach, supporting both the implementation and development of norms***. **The EU** and **the USA** stressed that negotiations on binding agreements could be resource-intensive and counterproductive. **Iran** counter-argued that a uniform approach to norm implementation is impractical due to each nation's unique circumstances. **Nicaragua** and **Pakistan** contended that non-binding norms

[76] 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, unofficial translation (UNODA), 3 December 2024, 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

[77] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's tenth substantive session.'

fail to address emerging threats effectively, while **China** pointed out that the 2015 UN GGE report allows for developing additional norms over time.

Capacity-building as a critical component for cyber norms implementation

Many states, particularly **Singapore**, **Indonesia**, **Pakistan**, and **Mauritius**, ***emphasised that implementing cyber norms requires bridging the technical gap between developed and developing nations***. **Iran** and **Cuba** noted that resource constraints hinder developing countries. **Kenya** and **South Africa** advocated for integrating long-term capacity-building into the future UN cyber mechanism to improve norm implementation. **Kenya** highlighted the challenges posed by varying technical expertise among states. For example, Norm C, which prohibits allowing territory for wrongful acts, requires specific tools and skills that not all countries possess.

Singapore argued that each norm has policy, operational, technical, legal, and diplomatic aspects, and developing the capacity to implement these norms is essential for identifying gaps and determining the need for new norms. In this context, the ASEAN-Singapore Cybersecurity Centre of Excellence will launch a series of capacity-building workshops called 'Cyber Norms in Action.'

Voluntary checklists: Cyber norms implementation

The voluntary checklist was broadly supported as a tool for operationalising agreed cyber norms. Countries (e.g. **Colombia**, **Japan**, and **Malaysia**) view it as a 'living document' that should evolve with the evolving landscape of cyber threats. **Kazakhstan** suggested incorporating best practices for incident response and public-private collaboration.

An important aspect of the checklist is its potential to promote inclusive cybersecurity governance. **The UK**, **Brazil**, and **the Netherlands** stressed the need to integrate a gender perspective, ensuring that the implementation of cyber norms considers the disproportionate impact on women and vulnerable communities.

Despite this support, some countries remain sceptical. **Cuba** and **Iran** cautioned against using the checklist as a de facto assessment tool for evaluating states' cybersecurity performance. **China** insisted that the checklist remain within the UN information security framework to maintain neutrality. **Iran** proposed delaying negotiations on the checklist until a broader consensus is reached under a permanent UN cyber mechanism.

The norms implementation vs development debate continued into the last session

As discussed in July 2025[78]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[79] ***Many Western and like-minded states stressed the implementation of norms.*** In particular, **the Republic of Korea** underlined the importance of focusing on implementing

[78] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Radunovic, Roellinger, 'UN OEWG concludes.'
[79] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

and operationalising existing norms rather than creating new ones. **The USA**, **the Netherlands**, **Canada**, and others expressed concern about placing undue emphasis on developing additional norms and advocated for removing paragraphs 34R and 36 of Rev.1. **The EU** maintained that decisions on developing new norms should be left to the future permanent mechanism and called for more attention to norms implementation and capacity building.

Several developing countries supported this focus but noted capacity constraints. **Fiji**, speaking on behalf of **the Pacific Islands Forum**, noted the different stages of norms operationalisation among members and cautioned against moving forward with new norms without consensus or a clear gap analysis. **Ghana** welcomed a whole-of-government approach to the implementation, but also stressed the need to raise awareness of these norms at the national level.

The outcomes: In the final report, paragraph 34 and its subparagraphs were significantly condensed. Detailed proposals in Rev.1 were reduced to a shorter list (34a–h). Technical specifics, such as templates and gender considerations, were simplified or removed.

Work on new norms: A red line for some

In contrast, another group of states advocated for continued work on new norms. **Russia** argued there was a biassed reflection favouring norms implementation and insisted on language supporting the development of legally binding measures, highlighting the initially agreed mandate for the UN OEWG. **Iran** warned that removing subparagraphs in paragraph 34 as well as paragraph 36 would undermine the section's overall balance.

China called for a balance between norms and international law and proposed to delete paragraph 34H, arguing it was not balanced as it focused only on non-state actors and commercially available ICT intrusion capabilities while ignoring states as the major source of threat. China noted that countries that support the retention of paragraph 34H are countries that are opposing the creation of new norms, also commenting on perceived inconsistency among those opposing the creation of new norms while advocating for implementation. In the final report, the wording was adjusted (in paragraph 34F) to reference both state and non-state actors.

Walking the middle path on norms development

In the meantime, some countries attempted to take the middle ground. **Singapore** supported implementing existing norms while leaving space for new ones, noting that implementation is necessary to understand what new norms are needed. **Indonesia** expressed a similar view.

The outcome: While Rev.1 stated that developing new norms and implementing existing ones were not mutually exclusive and recommended compiling and circulating a non-exhaustive list of proposals in this context, the final report significantly softened this language. It retained the idea that additional norms could emerge in paragraph 36d, but excluded it from recommendations.

Voluntary Checklist of Practical Actions: Deferred

The Voluntary Checklist of Practical Actions received broad support with some exceptions. While **the UK** called it a valuable output of the **OEWG**, and **Ireland** described it

as an effective capacity-building tool, **Russia** and **Iran** ***opposed its adoption*** as it was formulated in paragraph 37 of Rev. 1, ***arguing it had not been fully discussed and should be deferred to the future mechanism***.[80]

At the same time, some additional proposals were shared, for example, **Cameroon** called for a working group on accountability for attacks on critical health infrastructure, while **China** reminded of the data security initiative and broader data security measures.

The outcome: The checklist, initially proposed for adoption, has been reworded and is now for continued discussion.

[80] Digital Watch Observatory, *OEWG Chair releases Zero Draft of the final report, setting stage for final talks*, 26 May 2025, https://dig.watch/updates/oewg-chair-releases-zero-draft-of-the-final-report

Application of international law to the use of ICTs

Applying international law to cyberspace: Competing state views

As discussed in December 2021[81]

The discussions on international law and on norms, rules, and principles of state behaviour in cyberspace and their applicability in cyberspace were closely related to the nature of the 2015 and 2021 UN GGE reports and the 2021 OEWG report.[82]

The majority of the states – **Argentina, Australia, Austria, Brazil, Colombia, Costa Rica, Czech Republic, the EU** on behalf of its member states, the candidate countries **Montenegro**, the **Republic of North Macedonia**, and **Albania,** the country of the stabilisation and association process, and potential candidate **Bosnia and Herzegovina,** as well as **Ukraine, the Republic of Moldova and Georgia** (**EU**), **Egypt, Estonia, France, Germany, Ireland, India, Indonesia, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, Ukraine** (in national capacity)**, UK, Philippines, Republic of Korea, Singapore, South Africa,** and **Switzerland**, agreed that the ***previous UN GGE and OEWG reports, including corresponding UN GA resolutions adopted by consensus, have confirmed that the existing international law, notably the UN Charter in its entirety, IHL, and international human rights law apply in cyberspace***.

These states recalled, in particular, ***the principle of state sovereignty, sovereign equality, the settlement of disputes by peaceful means, the provision of the use of force non-intervention in the internal affairs of other states, and the respect for human rights and fundamental freedoms as principles of international law that are applicable to states use of ICTs in cyberspace.***

As such, ***for these states, the previous reports by the UN GGE and OEWG, and related UN GA resolutions represent an acquis, and are the basis for negotiations at the 2021–2025 Open Ended Working Group (OEWG)***.

These states are now looking to discuss, within the OEWG, how to apply international law in cyberspace and build upon the previous acquis. **Colombia** suggested that, once the OEWG is able to identify the existence of gaps in the application of international law and ICTs, it can then make progress in developing new norms to fill those gaps. **Switzerland** and **Mexico** pointed out that the discussions need to clearly distinguish between the binding international law and non-binding norms.

Israel stated the opinion that, while international law is applicable to cyberspace, traditional rules of international law, which mainly evolved in a physical world and often in

---

[81] Digital Watch Observatory, *UN OEWG 2021–2025 – International law*, 14 December 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/international-law.
[82] UNGA, *Developments in the Field of Information and Telecommunications*, A/RES/70/174, UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/76/135), and UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/AC.290/2021/CRP.2).

domain-specific contexts, do not always lend themselves to application in the cyber domain, while its certain distinctive characteristics call for further studies. **Israel** also considers that the concepts of rules and principles of international law, which apply in principle to ICTs such as sovereignty, non-intervention, due diligence, state responsibility, attribution, and countermeasures, merit further study.

China and **Cuba** agreed that the general principle of international law based on the UN Charter applies to cyberspace. In the opinion of the **Islamic Republic of Iran (Iran)**, the behaviour in cyberspace differs from behaviour in the physical world, and the international law applicable to the use of ICTs may be different. However, **Iran** said that nothing prevents the application of general rules of the UN Charter in the ICT environment. **Iraq** stressed the importance of international law and the UN Charter as a point of reference towards creating a safe, open, and enabling environment for activities pertaining to ICTs, and towards eliminating the threats against society.

Need for a new legal instrument

Several states, namely **Cuba, China**, **Iran**, **Pakistan, and Russia**, ***have called for the creation of a new international legally binding instrument.*** The main reasons pointed out were the lack of agreement on terminology with respect to ICTs and rights and obligations of states, the existence of unregulated matters or gaps in international law, greater accountability of states, and enforcement. These countries see the UN as the most suitable forum to hold such discussions.

The Republic of Korea, Italy, EU and **France** have ***spoken against a new legally binding instrument at that point in time***. The **Republic of Korea** stated that, while the ultimate desirability of having a set of binding rules governing cyberspace can not be denied, seeking a new legally binding instrument at this stage is both impractical and potentially misleading, since the process itself might give the false impression that there is a legal vacuum in cyberspace. **Italy** and **France** pointed out that the focus now should be on the modalities of applying the existing international law.

Art. 51 of the UN Charter: Armed conflict and right of self-defence

The discussions further evolved to include specific principles and regulations of the UN Charter.

A number of countries spoke about how Art. 51 of the UN Charter[83], pertaining to the right of self-defence if an armed attack occurs, applies to cyberspace. **Singapore** pointed out that the right to self-defence applies in cyberspace and is of fundamental importance to small states, and should apply in cyberspace as in the physical world. The **Philippines** suggested that the OEWG should discuss the aspects of Art. 51 of the UN Charter, specifically the question of what constitutes an armed attack in cyber context and what are the thresholds for invoking the right to self-defence, or implementing countermeasures. **Egypt** stated that discussing the modalities of Art. 51 of the UN Charter should not divert attention from addressing cooperation to prevent such conflicts from occurring in the first place.

[83] United Nations, *Charter of the United Nations: Repertory of Practice—Article 51*, Codification Division, Office of Legal Affairs, accessed August 5, 2025, https://legal.un.org/repertory/art51.shtml.

Russia pointed out that the international community has no consensus on the question of qualification of malicious use of ICTs as an armed attack in the sense of Art. 51 of the UN Charter. Consequently, according to Russia, there is no basis for assessment of the legitimacy of the use of ICT, including from the standpoint of IHL.

Cuba stated that ***it is unacceptable to have a concept which seeks to equalise a cyberattack with an armed attack*** and tries to justify the presumed applicability of Art. 51 of the UN Charter. **Cuba *outright rejected the notion of the automatic application of Art. 51 of the UN Charter in cyberspace***.

Responding to Cuba's statement, **Australia *noted that there is consensus that the UN Charter in its entirety applies to cyberspace*** and therefore it follows that Art. 51 of the UN Charter applies to cyber activities which constitute an armed attack and in respect of acts of self-defense carried out by cyber means. Australia further noted that any reliance on Art. 51 of the UN Charter must be reported directly to the UN Security Council, which helps safeguard against the risk of armed escalation.

Attribution

Australia, **Germany**, **Ukraine**, **and Switzerland** spoke in detail about the attribution of cyberattacks.

Ukraine concurred with the previous UN GGE and OEWG reports that states must not use proxies to commit internationally wrongful acts using ICTs, and that states should take all actions to ensure that their territory is not used by non-state actors to commit such acts. It wishes to discuss the question of attribution at the UN.

Switzerland addressed the issue of legal attribution of cyberattacks, underlining that legal attribution is governed by the law of state responsibility and the International Law Commission's Draft Articles on State Responsibility.[84] Switzerland wanted the OEWG to further analyse legal constraints – preconditions and procedural requirements of countermeasures.

Australia also spoke about legal attribution, concurring with Switzerland that the customary law of state responsibility, reflected in the International Law Commission's Draft Articles on State Responsibility, provides the mechanism for the application of most of international law, including the UN Charter, and details strict rules on attribution, provides what measures state may take in response to unlawful acts, and determines the consequences of internationally wrongful acts, including reparations.

Germany agreed that a sufficient level of confidence is needed for attributing a wrongful act to a state. This applies equally to breaching international law in cyber context and in the physical world. Further, according to Germany, accusations of misconduct should be substantiated by results of extensive technical, contextual, and factual research.

Czech Republic and Switzerland addressed due diligence as a general principle of international law.

---

[84] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (Supplement No. 10, A/56/10), article 6 commentary; adopted 9 June 2001, UN Codification Division, *Responsibility of States for Internationally Wrongful Acts*, UNODA, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

International humanitarian law (IHL)

Australia, Brazil, Czech Republic, Estonia, EU, France, Germany, Ireland, Italy, Mexico, the Netherlands, Switzerland, Ukraine, and others specifically confirmed that ***the IHL, including the principles of proportionality, distinction, and precaution, applies to the use of ICTs by the states***, and should not be misinterpreted as encouraging the militarisation of, or legitimising the use of force in cyberspace. ***Calling for the OEWG to elaborate how IHL applies to the use of ICTs by states***, they pointed out that it would advance transparency and common understanding among states.

Italy pointed out that the OEWG mandate within the UN First Committee not only fully legitimises, but rather compels the OEWG to discuss how IHL applies in cyberspace. **Switzerland** and the **Netherlands** gave detailed statements on the applicability of the IHL, stating that the IHL addresses the realities of war without considering the legality of war, and reduces risks and potential harm to civilians, civilian objects, and combatants in the context of an armed conflict.

Colombia was of the opinion that further study on how the principles of IHL apply was needed.

Cuba stated that ***it does not consider the applicability of IHL relevant to the use of ICTs in the context of international security, since that would entail tacitly accepting the possibility of an armed conflict scenario***. According to Cuba, it would contribute to militarising cyberspace and it would be a first step in equalising cyberattack with a traditional armed attack.

International human rights law

Australia, Brazil, Czech Republic, Estonia, EU, France, Germany, Ireland, Italy, Mexico, the Netherlands, Switzerland, Ukraine, and others ***specifically confirmed that the international human rights law is also applicable in cyberspace***. **Iraq** stressed that human rights and other fundamental freedoms should be respected in the use of ICTs.

The Netherlands gave the most detailed statement on the human rights application in cyberspace. It pointed out that the current acquis states that human rights and fundamental freedoms apply online as well as offline, which means they should be respected, protected, and promoted in cyberspace. According to the **Netherlands**, the acquis needs operalisation through the work of the OEWG starting with recognition of interdependence and complementarity of human rights and cybersecurity. Full respect for international human rights law must also be given when designing, developing, and implementing cyber security laws and policies. The Netherlands also brought forward the right to privacy and freedom of expression, the role of the private sector, and risks of human rights violations in cyberspace related to women and vulnerable groups, including human rights defenders, journalists, LGBTQ, children, and ethnic minorities.

The way ahead

The majority of the states agreed that the discussions at the OEWG should explore how international law and its principles apply in cyberspace and build a common understanding of the matter.

Sharing national positions on how international law applies in cyberspace was perceived as the way forward in identifying convergences and points for discussion.

Several ways of sharing national positions and exploring how international law applies in cyberspace were discussed:

- The OEWG's repository of national positions (**Israel**)
- UNIDIR's Cyber Policy Portal (**UK**, **France**, **Italy**, **Germany**, **USA**, **Canada**, **Japan**, **Colombia**, **Estonia**, **Brazil**, and **Costa Rica**)[85]
- Australian and Mexico's proposal of a voluntary survey of national views and practices (**Austria**, **Argentina**)[86]
- Study on how international law applies to states' use of ICTs (**Switzerland**)
- Referring the question to the International Court of Justice and the International Law Commission to establish their views on the matter (**South Africa**)
- UN in general (**Singapore**)
- Cyber Law Toolkit and Tallinn Manual 3.0 (**Estonia**)[87]
- At the regional level, in addition to the international one (**Costa Rica**)

Throughout the session, ***the states emphasised the need of capacity building*** on the subject of international law.

International law: Yes, but

As discussed in April 2022[88]

Many countries, including Argentina, Australia, Brazil, Canada, Japan, Kenya, the Republic of Korea, the USA, and the EU member states, confirmed that ***the framework of responsible state behaviour adopted by the UN General Assembly in 2021 – based on 2010, 2013, 2015, 2021 GGE and 2021 OEWG consensus reports – is the basis for the work of the OEWG 2021-2025.*** **China** also stated that the framework is an important consensus of the UN information security process, and it should be fully, completely, and accurately implemented. **Russia** referred to the OEWG recommendations of 2021 (including

[85] United Nations Institute for Disarmament Research (UNIDIR), *Cyber Policy Portal*, accessed August 5, 2025, https://unidir.org/cpp/en/.
[86] Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member States, Poland, and South Africa, Joint Proposal for a National Survey of Implementation of UNGA Resolution 70/237, 16 April 2020, https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf
[87] NATO Cooperative Cyber Defence Centre of Excellence, Cyber Law Toolkit: An Interactive Resource for International Cyber Law, accessed August 5, 2025, https://cyberlaw.ccdcoe.org/wiki/Main_Page and NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual (2013) and Tallinn Manual 2.0 (2017), accessed August 5, 2025, https://ccdcoe.org/research/tallinn-manual/.
[88] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.'

the states' proposals in the Chair's Summary) in terms of the basis for the development of further rules; yet, it also stated that – in light of the extremely large number of unresolved issues related to the applicability of international law – **the *existing legal framework is practically useless*, and expressed the *need for an international legally binding instrument instead*.**

The ***need for a new legally binding instrument that would regulate the use of ICT by states*** remained an important question at the OEWG. Most countries did not see the need to develop a new legally binding instrument, with **Australia**, **Estonia**, **the EU**, **France**, **Ireland**, and **Switzerland** explicitly opposing such a proposal, saying it would mean a significant setback in the efforts to advance international security and stability that would lead to confusion and misunderstanding. On the other hand, **Belarus**, together with **Cuba**, **Iran**, **the Russian Federation**, and **Syria,** called for the ***development of a new single international legally binding instrument***. **China** would have liked to see the OEWG pursuing its ***global initiative on data security***, with a view to providing a blueprint for possible global rules.

Many states, including **India** and **Mexico**, confirmed that ***international law, including the UN Charter in its entirety, applies to the use of ICT by states***. **Belarus**, together with **Cuba**, **Iran**, **Russia**, and **Syria,** did not fully agree. **Cuba** specifically rejected the automatic application of IHL in cyberspace and any reinterpretation or application of Art. 51 of the UN Charter in the area of cybersecurity.

There were suggestions to move towards ***thematic discussions in dedicated groups on specific topics of how international law applies***, with experts involved, either within the regular OEWG or during the inter-sessional periods. Should these groups be put in place, we can expect that, in addition to the applicability of humanitarian law, the states would discuss the most pressing questions related to cybersecurity in the current geopolitical situation: what constitutes a breach of sovereignty, attribution of internationally wrongful acts, substantiation of such attribution, the difference between legal, technical, and political attribution, obligations of due diligence, and the protection of critical infrastructure, especially health facilities.

Acquis confirmed: Still, calls for a new binding instrument

As discussed in July 2022[89]

In July 2022, states met at the third substantive session to adopt the group's first APR.[90]

Three points were raised during the discussion on the introductory part of the APR: the acquis, the role of regional organisations, and gender parity.

The discussion on what constitutes the acquis, i.e. the legal framework which is already agreed upon and is the base for the work of the 2021-2025 OEWG (OEWG), has continued. The majority of the states consider previous UN GGE and UN OEWG reports as the base for the OEWG work to build on. **Nicaragua** and **Cuba**, however, find that ***the UN GGE report of 2021 is not a part of the acquis because of the restrictive nature***

[89] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.'
[90] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*.

of the Group of Governmental Experts (GGE). **Russia** similarly stated that ***the basis of the OEWG's work is the report of the previous OEWG.*** **Nicaragua** and **Cuba** ***also requested a reference to the UNGA Resolution 75/240 that created the current OEWG.***

The outcome: The first APR acknowledged the consensus report of the 2021 OEWG and the consensus reports of the 2010, 2013, 2015, and 2021 GGEs as the acquis.

The question that the OEWG has been debating over and over again: ***are voluntary norms enough, or are new legally binding obligations/a new legally binding instrument needed,*** was brought up again. **Pakistan**, **Democratic Republic of Congo**, **Russia**, **Iran**, **Nicaragua**, and **Egypt** highlighted the need to continue the discussion on a legally binding agreement. **Pakistan** stated that norms are effective in peacetime and lose efficacy in an event of a conflict. **Peru** and **the Netherlands** (on behalf of the informal international law group) did not exclude the necessity of adopting a legally binding instrument in the future.

This time, centre stage was taken by ***discussions on the application of the IHL to cyberspace.***

Switzerland, on behalf of the delegations of sixteen countries (**Argentina**, **Brazil**, **Canada**, **Chile**, **Colombia**, **the Czech Republic**, **Estonia**, **Germany**, **Indonesia**, **Japan**, **Jordan**, **Mexico**, **the Netherlands**, **Republic of Korea**, **Senegal**, **Sweden**) ***provided a statement saying that IHL applies in cyberspace and noting that it is a priority to clarify how it applies regarding cyber operations in armed conflicts***. These states see the adherence to the IHL of paramount importance as it offers fundamental protections and reduces the risks and potential harm to both civilians and civilian objects (IT infrastructure of hospitals or schools) and to combatants from cyber operations in the context of armed conflict. These countries also see the discussion on the IHL taking place under the auspices of OEWG 2021–2025 that includes briefings from experts, and encourage organising a focused discussion on the IHL during the next session of the OEWG.

The UK, **Congo**, **Ecuador**, **New Zealand**, **Ireland**, **Croatia**, **Canada**, **Peru**, **Romania**, **Brazil**, **Finland**, **Senegal**, **Costa Rica**, **Japan**, **El Salvador**, **Fiji** in their national capacity, **Mexico**, and **Czech Republic** ***supported this statement and its content***. **Austria**, **the Netherlands**, and **France** also ***suggested that the International Committee of the Red Cross (ICRC) is referenced in the first APR***. **Brazil** stated that the ICRC does not have to be explicitly mentioned, as the OEWG remains intergovernmental.

Nicaragua and **Cuba** stated that it is ***not relevant to even talk about the applicability of IHL to the use of ICTs in the context of international security since it would imply that the states tacitly accept the possibility of an armed conflict*** that would contribute to militarisation in cyberspace and would be the first step towards an armed cyberattack.

Cuba, **Russia**, and the **Islamic Republic of Iran** were ***against mentioning the IHL in the first APR***. **Pakistan** noted that ***IHL demands further politically neutral discussions among states for the development of common understanding***.

The outcomes: The possibility of developing a legally binding agreement and IHL in the situations of armed conflict were only mentioned as part of OEWG 2021 report recommendations. The ICRC was not mentioned in the first APR.

The Republic of Korea has ***welcomed the mention of the due diligence principle and the IHL***. **Iran**, on the other hand, ***prefered to delete any specific reference to due diligence and exchanges of best practices on international law***, believing them to be premature. **Portugal** suggested that ***some form of the due diligence norm applicable to the private sector could be devised***, with scholars being invited to make written contributions to this debate. A small group of member states should then write a food for thought non-paper to foster further debate on the viability of a due diligence code of conduct.

The outcome: Due diligence was listed in the first APR as one of the topics states proposed for further discussion.

Cyber attribution was brought forward by **Pakistan**, **Indonesia**, **Malaysia**, and **Germany**.

The outcome: Cyber attribution was not mentioned in the first APR.

Applying international law to cyberspace: Gaps and challenges

As discussed in December 2022[91]

While reaffirming that the existing international law applies to cyberspace, states discussed gaps in its applicability. **France** argued that the priority was to exchange views to build common understandings of how precisely international law applies, which may lead to identifying gaps and the need to develop binding norms if appropriate. As a particular gap, **Austria** identified the relationship between what has been defined as non-binding norms (like due diligence) and the well-established customary law.

Expectedly, **Russia, Iran, Cuba,** and **Pakistan** underlined that there are ***gaps caused by unique attributes and the transnational nature of ICTs which could only be filled by the development of legally binding instruments.*** **Russia** proposed that the OEWG discussions should focus on two dimensions: (a) how specific principles apply to the use of ICTs, and (b) which aspects of interstate relations remain unregulated by international law. In this view, Russia notably proposed that the OEWG could elaborate specific international legal mechanisms to decrease public unsubstantiated attribution of cyberattacks. In an unrelated contribution on norms, **Switzerland** proposed providing ***explanatory guidance on attribution***, as more states publicly attribute cyber incidents in recent times.

Another major thorny issue originated from a joint concept paper presented by **Canada** and **Switzerland** which proposed to ***prioritise the discussions on certain topics – namely the Charter of the UN, peaceful settlement of disputes, International Humanitarian Law, and state responsibility***.[92] The logic behind the suggestion was that details on how international law applies are needed in order to build tailored CBMs for different states' needs. Focusing on specific topics would notably be easier for delegations from smaller states as well as an opportunity for capacity building, **New Zealand** noted. ***While a vast***

[91] Gavrilovic, Ittelson, Petit-Siemens, Radunovic, Roellinger, Stadnik, 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs'.
[92] Canada and Switzerland, *A Practical Approach to International Law in the 2021–2025 Open-Ended Working Group*, 7 December 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20221207_Canadian_-_Swiss_Concept_Papier_on_International_law_PPT.pdf

majority of states welcomed and supported this proposal, **Russia, Iran,** and **Cuba** were against it. **Cuba** ***expressed concerns that if some items are prioritised, others will be left behind***, and **Iran** ***argued that such an approach could damage consensus.***

No progress was made in discussions on the applicability of International Humanitarian Law (IHL).

Past disagreements linger: States push forward on international law debates

As discussed in March 2023[93]

While the faultlines from the previous discussions remained, states have progressed in formulating and sharing their views, and delving deeper into international law issues.

The applicability of international law to cyberspace

The majority of states ***reaffirmed that international law, including the UN Charter in its entirety, applies to cyberspace***. ***Most states also reaffirmed the applicability of human rights law and IHL in cyberspace*****. Costa Rica** also stated that international criminal law applies in cyberspace.

Thailand pointed out the need to ensure that there are no gaps in the implementation of international law. **Israel** noted the need for further study into understanding whether adjustments and clarifications of the traditional international law are necessary to apply it in the cyber domain.

Some states acknowledged the applicability of principles of international law enshrined in the UN Charter – sovereign equality of states, non-use of force and threat of force, settlement of international disputes by peaceful means, and non-interference into internal affairs of states – ***but consider the automatic applicability of international law premature*** (**Cuba**, **India, Jordan, Nicaragua, Pakistan, Russia, Syria**). For **China,** the primary focus of discussions on the application of international law is to affirm the application of the UN Charter to cyberspace, especially that of its principles.

The need for a new legally binding instrument

The rift remained in the opinions on whether there is a need for a new legally binding instrument.

Cuba, Iran, Iraq, Russia and Syria ***supported a new legally binding instrument*****. Iran** was in favour a new legally binding treaty to define the terminology and principles of international law.

Russia, in line with its previous statements, sees the adoption of a new legally binding instrument as a priority and has submitted an updated concept (proposal) of the 'Convention of the UN on Ensuring International Information Security' with **Belarus and Nicaragua** as

[93] Gavrilovic, Grottola, Ittelson, Kazakova, Petit-Siemens, Stadnik, 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session.'

co-sponsors.[94] Previously, in 2011 and 2021, the Russian delegation prepared similar concepts for such a convention. However, the current updated concept has been shortened: parts on cybercrime and terrorism with the use of ICTs have been removed (which are, at the same time, on the table for the AHC negotiation process on a cybercrime convention). According to this updated concept, ***the Convention has three purposes such as to prevent and settle inter-state conflicts, build trust and develop cooperation among the UN member states in the field of international information security, and support the capacity building of states.*** For each of these purposes, the concept suggests several principles and proposals.

Australia, **Austria**, **Belgium**, **Canada**, **the Czech Republic**, **Estonia**, **Ireland**, **Israel**, **the Netherlands**, **Malawi**, **the Republic of Korea**, **the UK**, and **New Zealand** ***did not support a new legally binding instrument***.

Vietnam stated that if the idea of the new legally binding document is premature, the OEWG could clarify the rules of international law through (a) a request for an advisory opinion to the International Court of Justice; (b) a mandate for a study by the UN International Law Commission; or (c) through submitting a topic for discussion at the UN Sixth Committee.

The applicability of IHL

The discussion on the applicability of IHL in cyberspace, which dominated discussions at the previous session, ***continued***.

The majority of the states confirmed the applicability of IHL and its principles of necessity, humanity, proportionality, and distinction in cyberspace. The question, however, remained about what constitutes an attack and armed conflict for the purposes of IHL. **The EU and Switzerland** affirmed that the IHL applies in situations of armed conflict. **The EU** wants to further study how the IHL principles apply to the use of ICTs by states. **New Zealand** stated that a cyber activity might constitute an attack for the purposes of IHL where it results in death, injury, or physical damage, including loss of functionality equivalent to that caused by a kinetic attack. **South Africa** sees IHL as applicable to cyber operations, as it does to all operations with a nexus to an armed conflict, such as an attack on civilian infrastructure.

Russia ***refused the automatic application of IHL in cyberspace***. It stated that since there is no consensus on what constitutes an armed attack, there are no grounds for assessing the applicability of IHL. **Belarus** ***denied the applicability of the IHL, as it does not consider ICTs as weapons.***

The principles of the UN Charter

During this session, the discussions were more substantial on individual principles enshrined in the UN Charter: the principle of sovereignty and sovereign equality, the obligation of states to settle international disputes by peaceful means, the principle of non-intervention and the prohibition of the threat or use of force.

---

[94] Russian Federation, Updated concept of the convention of the United Nations on ensuring international information security, April 2023, 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.

- **Principle of sovereignty and sovereign equality (Art. 2.1. of UN Charter)**

The majority of states (**Austria, Canada, Croatia**, and **others**) stated that the principle of sovereignty and sovereign equality applies in cyberspace and shared opinions on what would constitute a breach of sovereignty in cyberspace.

Sweden, on behalf of Nordic states, said that a breach of sovereignty in cyberspace might amount to an internationally wrongful act. It may also give rise to state responsibility if attributable to a state. The assessments should be made on a case-by-case basis. **Singapore** considers the state's territorial sovereignty to extend over cyber infrastructure located in its territory and activities associated with such infrastructure. **The Netherlands** holds the view that states have exclusive authority over the physical, human and immaterial, which includes logistical or software-related aspects of cyberspace within their territory. **Switzerland** provided an example of state sovereignty in protecting ICT infrastructure on a state's territory against unauthorised intrusion or material damage. **Japan** sees a possible violation of sovereignty through an act which causes physical damage or loss of functionality through cyber operations against critical infrastructure.

Estonia, France, and Switzerland pointed out the limits of state sovereignty, such as the responsibility not to breach the sovereignty of other states and to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states.

Australia, Chile, Estonia, the Netherlands, Vietnam, the Republic of Korea, South Africa, and Switzerland recognised the principle of due diligence in cyberspace.

- **Obligation of states to settle international disputes by peaceful means (Art. 2.3, Art. 33 of UN Charter)**

Many states (**Australia, Austria, Belgium, Canada, Estonia, the Netherlands, Singapore, Switzerland, Sweden on behalf of Nordic countries, and the UK**) have reaffirmed the obligation of states to settle disputes by peaceful means by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

- **Principle of non-intervention (Art. 2.7 of UN Charter)**

The customary international law obligation not to intervene in the internal or external affairs of another state applies to cyberspace, just as it applies in the physical realm, according to **Australia, Singapore, Estonia, and others.** According to **Singapore**, a prohibited intervention in certain circumstances would be interference with the electoral processes of another state through cyber means. **Estonia** considers coercion as a key factor in assessing whether a cyber operation constitutes an unlawful intervention in cases, for example, the other nation's national democratic processes, such as elections or military security or critical infrastructure systems. **Austria,** citing the ICJ Nicaragua case and the definition of coercion, called for an in-depth discussion on how it translates to cyberspace.[95]

[95] Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). Judgment, International Court of Justice, 27 June 1986, I.C.J. Reports 1986, p. 14, General List No. 70, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

- **Prohibition of the threat or use of force (Art. 2.4 of the UN Charter)**

Canada, **Singapore**, **South Africa**, and **Romania** affirmed the obligation of all states to refrain from the threat or use of force against the territorial integrity or political independence of other states, which also applies in cyberspace.

The states also discussed the conditions for invoking Art. 51 of the UN Charter (right to self-defence in case of armed attack). **Austria** pointed out that the right of self-defence does not legitimise the use of armed force by any means but serves as a safeguard against unlawful armed attacks and is subject to certain conditions, such as necessity and proportionality. According to **New Zealand**, a cyber activity that amounts to the use of force will also constitute an armed attack for the purposes of Art. 51 of the UN Charter if it results in effects of a scale in nature equivalent to those caused by a kinetic armed attack. **South Africa** confirmed that a cyberattack can be an armed attack and invoke the right of self-defence, while **Cuba** firmly opposed this opinion. **Nicaragua** pointed out that there is no current consensus in the international community on how to qualify the misuse of ICTs, such as armed attacks, in accordance with Art. 51 of the UN Charter.

On the related issue of attribution of cyberattacks to states, **France** believes that the decision about attribution is a sovereign decision that falls under its exclusive purview, even if international coordination might be undertaken to attribute an information-based attack collectively. According to France, international law does not compel states to disclose the elements of evidence they have that form the basis for publicly attributing such a cyberattack. **Russia** stated that the current level of organisation of the global internet does not allow facts underpinning the attribution to be confirmed. **Thailand** saw it as essential to ensure that the process of attribution is objective, transparent, and based on solid evidence to avoid failed accusations and unjustified action, which is hard for countries with limited resources.

How to enforce the states' obligations

The discussions expanded – for the first time, we believe – into the question of enforcement of the obligations of states, citing the International Court of Justice (**Switzerland**) and the work of Liechtenstein within the International Criminal Court (ICC) on the application of the Rome Statute of the ICC to cyberwarfare, and in particular the provisions regarding the crime of aggression, war crimes, crimes against humanity, and genocide (**Belgium**, **Vietnam**).

What international law matter should the OEWG discuss next?

Most states supported the Canadian-Swiss proposal to include the topics of the UN Charter, peaceful settlement of disputes, IHL and state responsibility in the OEWG Programme of work for 2023.[96]

India suggested discussing convergence and gaps in member states' common understanding and interpretation of international law.

[96] Canada and Switzerland, *A Practical Approach to International Law in the 2021–2025 Open-Ended Working Group.*

States favouring a new legally binding instrument (**Russia, Iran, Cuba**) call for negotiating such a treaty, while **China** noted that the topics of intercession discussions must be balanced, not limited to a single topic.

Most of the states (**Australia, Austria, Canada, the Czech Republic, Estonia, the EU, Kenya, Netherlands, New Zealand, South Africa, Singapore, Sweden on behalf of Nordic countries, Switzerland, the UK, and others**) would welcome a dedicated session on international law in May or June in the form of virtual or hybrid inter-sessional meeting, ahead of the fifth substantive session in July.

No convergence in sight: Calls grow for continued talks on international law

As discussed in May 2023[97]

When summing up the discussions on international law for the OEWG's March 2023 session, we wrote that the faultlines from the previous discussions remain. The lack of progress towards convergence had prompted many calls for more discussions on international law within the OEWG.

The need for a new legally binding instrument: Are discussions premature?

China reiterated that additional new binding obligations are needed. According to **Iran** and **Russia**, a new legally binding instrument is not only needed, but urgently needed. **Bangladesh** also noted they recognise the merit of developing a dedicated international legal framework tailored to the distinct characteristics of the ICT environment.

However, the majority of states are not in favour of a new legally binding instrument. There has, in fact, been a shift in rhetoric: ***This camp is now calling negotiations on a new legally binding instrument 'premature and unnecessary', noting that states must first figure out how to apply the existing framework.*** It is worth noting, though, that this does not exclude such negotiations, as **the EU** and **the USA** put it: If gaps in common understanding are found, or it is found that existing law cannot address some aspect of conduct in cyberspace, then it can be considered whether additional legally binding obligations could be proposed.

The applicability of IHL: To be discussed

The discussions on the applicability of IHL to cyberspace continued to feature as a topic of friction. ***While a majority of countries agreed that IHL is applicable to cyber operations conducted in the context of armed conflict***, **Russia** is firm in insisting that the ***existing norms of IHL do not automatically apply to cyberspace – specific circumstances must be considered, and norms must be adapted accordingly***. Further study is needed on how and when IHL can be applied to the use of ICTs by states and codifying such an understanding in a legally binding instrument. **China** underlined the importance of handling the applicability of IHL with prudence and preventing turning cyberspace into a new battlefield.

[97] Gavrilovic, Kazakova, and Petit-Siemens, 'What's new with cybersecurity negotiations? The informal OEWG consultations on capacity building.'

The **USA**, **France**, **Czechia**, and **New Zealand** noted that ***recognising IHL applicability to cyberspace is not equal to promoting the militarisation of cyberspace***. **France**, **New Zealand** and **Czechia** underlined that such discussions are aimed at ensuring the protection of civilians and civilian infrastructures at all times, including in times of conflict. **Chile** noted that it helps build trust and predictability.

A common line of thought is, however, that the application of IHL should be discussed, and should be a topic of focussed discussion at the OEWG.

Principles of the UN Charter

- **How is sovereignty understood in the context of the use of ICTs by states?**

The general consensus is that states exercise sovereignty over their ICT infrastructure within their territories. **El Salvador** specifically clarified that this includes physical, digital, and cyber infrastructure, as well as the equipment facilitating data flow, applications, and interoperability standards, including submarine communication cables. **Iran** also noted that states exercise sovereignty over cyber equipment and added critical infrastructure (CI) and critical internet infrastructure (CII) to the list.

The issue of data sovereignty was highlighted by **China** and **Iran**, who emphasised that states have sovereignty over data. **Iran** defined this as 'data originated or ended in their territory or devices under its control or in the adjacent area'. **China** also noted that states exercise sovereignty over related resources. **El Salvador** and **China** underlined that states exercise sovereignty over ICT-related activities in their territories. **El Salvador** noted that states control interactions in cyberspace to prevent misuses and criminal activities, in line with states' due diligence obligations.

Austria noted that ***states exercise sovereignty over persons engaging in cyber actions on their territory***, while **El Salvador** stated states exercise sovereignty by understanding the legal status of cyberspace in three layers: 'a physical layer composed of the cyber infrastructure; a second layer of software logic; and, a third layer of cyber-persona, also representative of the social aspect of cyberspace linked to real people or to digital personas'.

- **When do cyber operations violate sovereignty?**

For the **Netherlands**, a violation of sovereignty occurs when a state's cyber activities infringe upon the territorial integrity of the target state.

The **Netherlands**, **Singapore**, and **New Zealand** share the view that ***violations of sovereignty occur when cyber activities disrupt another state's governmental functions***. For Singapore and New Zealand, that includes the state's right to freely choose its political, economic, social, or cultural system. **Singapore** also added the formulation of state foreign policy, while **New Zealand** highlighted national security and policing. Examples **Singapore** provided are interference with the electoral processes of another state or cyberattacking a state's infrastructure in an attempt to coerce its government to take a certain course of action on a matter ordinarily within its sovereign prerogative.

Japan and the **Nordic countries** noted that ***cyberattacks resulting in physical damage or loss of functionality are breaches of sovereignty***. The **Nordic countries** added ***cyber operations that alter or interfere with data without causing physical harm may, depending on the specific circumstances, also violate sovereignty***.

New Zealand ***noted the element of coerciveness*** (namely, that there is the intention to deprive the target state of control over its governmental functions). For **Iran**, any use of cyber coercion with physical or non-physical effects that threaten national security or may lead to political, economic, societal, and cultural destabilisation, constitutes a threat to sovereignty. However, for **Austria**, intrusive or disruptive cyber operations, even when not amounting to coercive interference, might still violate sovereignty.

South Africa and **Ireland** underlined that ***a breach of sovereignty in cyberspace might amount to an internationally wrongful act***. For **Ireland**, this is true regardless of whether the cyber activity falls short of the threshold of non-intervention or the use of force. **El Salvador**, on the other hand, notes that while cyber operations that limit another state's sovereignty are prohibited under international law, there are exceptions that should be analysed case by case.

- **How should states settle their international disputes by peaceful means in the context of the use of ICTs by states?**

States must endeavour to settle such disputes in line with the peaceful means set out in Article 33 of the UN Charter, the majority of states agreed. **Austria** also noted that the article offers states flexibility regarding the means that they can use to resolve their disputes peacefully.

Japan, **South Korea**, **New Zealand**, and **France** noted that the powers of the UN Security Council, based on Chapters 6 and 7 of the UN Charter, should be used in disputes stemming from cyber operations. The latter two underscore that states can bring any dispute, or any situation likely to endanger international peace and security, to the attention of the UN Security Council, under Art 35. of the UN Charter. **Japan** noted that the functions of the other UN organs, including the International Court of Justice (ICJ), based on Chapter 14 of the UN Charter, and the Statute of the International Court of Justice, should be used in disputes stemming from cyber operations.

The **Netherlands, Switzerland** and **Japan** noted that the Points of Contact (PoC) directory could also contribute to the peaceful settlement of disputes, as it stimulates contacts and the exchange of information between states.

- **When does a cyber operation constitute a threat or use of force under Article 2.4 of the UN Charter?**

Cyber operations may constitute a threat or use of force and a violation of the UN Charter if the scale and effects of the operations are comparable to ones using kinetic means, according to **Austria**, **Switzerland**, the **UK**, **France**, and **New Zealand**. For **Ireland**, if the cyber operations scale and effects correspond to those of a physical use of force, it may constitute a threat or use of force. For the **Netherlands**, a cyber operation with a very serious financial or economic impact may potentially qualify as the use of force. **Estonia** also underlined the impact of the cyber operation, **South Africa** noted it depends on the operation’s effect and scale of the operation, the **Nordic countries** that it depends on its gravity, while **Japan** noted it depends on certain circumstances but did not go into detail. **Singapore** listed the following: the prevailing circumstances at the time of the cyber operation, the origins of the cyber operation, the effects caused or sought by the cyber operation, the degree of intrusion of the cyber operation, and the nature of the target.

The states also discussed the conditions for invoking Art. 51 of the UN Charter (right to self-defence in case of armed attack). **Ireland** noted that cyber operations could only reach the threshold of armed attack in exceptional circumstances. In **Singapore**'s view, 'malicious cyber activity attributable to a state that causes death, injury, physical damage or destruction equivalent to a traditional non-cyber armed attack, or presenting an imminent threat thereof' would constitute an armed attack. However, Singapore also noted that malicious cyber activity may amount to an armed attack based on its skill and effects, such as sustained infrastructure outages or a series of coordinated cyber attacks.

What role can other UN bodies play in advancing the understanding of the implementation of international law?

South Africa reiterated that ***the International Law Commission (ILC) could contribute to the discussions***, which **Iran**, **El Salvador**, **Malaysia**, and **Colombia** supported. **South Africa** also suggested ***using the expertise of other UN bodies that deal with cyberspace, state behaviour and international law, such as UNIDIR***. **Colombia** noted that ***the UN Office of Legal Affairs could contribute thematically to the discussions on international law.***

On the other hand, **Australia** noted that ***the application of international law to peace and security in cyberspace is firmly within the OEWG's remit*** and that, should other UN bodies start discussing the same, states' understanding of how international law applies to cyberspace could fragment.

Debates on scenarios selected by UN bodies

Germany proposed that further focused discussions be based on concrete and potentially real scenarios which would be chosen by UN bodies. The real conditions would lead to an increased level of credibility, and ultimately tackle the question of whether the existing legal framework can address these issues. Germany suggested that these case studies can cover election interference or cyberattacks on critical cyber infrastructure. The **Netherlands** supported the proposal.

The second APR: Standoffs on a legally binding instrument and human rights

As discussed in July 2023[98]

In July 2023, states met at the fifth substantive session to adopt the group's second APR.[99] The statements at the session clearly reflected that over the previous year, the ***member states have advanced in explaining their positions and clarifying their points of disagreement on both norms and international law,*** thus making drafting the APR language more challenging.

Discussion on international law has built upon the intersessional meeting in May 2023. There were two key opinions present.

[98] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's fifth substantive session'.
[99] Digital Watch Observatory, *OEWG 2021–2025 Second Annual Progress Report (APR)*.

Most states reaffirm that international law, including the UN Charter, applies in cyberspace. This group proposed to deepen the discussion on how international law applies (Art. 30 of APR) and focus on sovereignty and sovereign equality, due diligence, respect and protection of human rights. The proposals within this group of states also included a direct reference to Art. 2(3), Art. 2(4) and Art. 33 of the UN Charter (Art. 30 a)-c) APR) and IHL's applicability (Art. 29 b) ii APR).

Another group of states insists on discussing a new legally binding instrument to regulate the state's behaviour in cyberspace (Art. 29 b) i APR). The proposal by **Argentina** and **South Africa** to involve the International Law Commission in the discussions on the applicability of international law to cyberspace did not find support.

There were, however, proposals that have found support from all across the board – on the need to hold dedicated inter-sessional meetings on how international law applies to cyberspace (Art. 35 APR) and on capacity building in international law (Art. 36 APR).

References to formulating a legally binding instrument in the second APR

Russia and **Iran** noted that the second APR needs more references to the possibility of formulating a legally binding instrument, with **Iran** stating that para 32 contains a weak reference, which they found insufficient. **China** requested that para 32 be deleted, or that additional wording be added under the section on Norms accordingly. **Estonia**, on behalf of **Australia**, **Colombia**, **El Salvador** and **Uruguay**, proposed an alternative language to article 32 of Rev 2: States discuss the need to consider whether any gaps exist in how existing international law applies in the use of ICTs and whether further to consider the possible development of additional legally binding obligations if appropriate. **The USA**, **New Zealand**, and **Switzerland** supported this edit.

The outcome: Paragraph 32 of the second APR notes the possibility of future elaboration of additional binding obligations, if appropriate, states discussed the need to consider whether any gaps exist in how existing international law applies in the use of ICTs and further consider the development of additional legally-binding obligations.

Australia suggested changing the word 'norms' to 'obligations' in paragraph 30 because the word 'norms' in the original text is used in the context of this OEWG, slightly differently from how it is often used in international law. Many delegations, such as **South Korea**, **Switzerland**, **Japan**, and **Austria**, supported this edit. **The USA** called new references to norms in the international law section 'muddying of waters.'

Inclusion of human rights in the second APR

States shared disagreements on human rights in the second APR: **Germany** first ***proposed adding the reference to human rights, and several countries*** (e.g. **Switzerland**, **the EU** and **its member states**, **New Zealand**, etc.) **supported this proposal.** Another group of like-minded States (**Russia**, **Iran**, **China**, **Cuba**, etc.) shared that they were disappointed by the inclusion of language on human rights in the final text. These countries argued that ***IHL and the overemphasis on gender issues should not have been incorporated without achieving consensus***.

Concrete proposals made during the session

States discussed the proposal for conducting an intersessional on international law, and the **Netherlands** and **Mexico** ***proposed to broaden the list of relevant briefers*** (in para 33 of the APR) ***so the OEWG can benefit from the expertise of stakeholders***, including from regional and sub-regional organisations, businesses, NGOs, and academia. Some countries (e.g. **the UK**, **Switzerland**, **Croatia**) strongly supported this proposal.

Concerning the same para 33, **South Africa** proposed amending the language and replacing 'developing a common understanding of the applicability of international law' with 'better inform the OEWG's deliberations', arguing that states should not be forced and ***the OEWG should let the conversation about the applicability of the international law develop in a bottom-up manner***.

Australia stressed that ***it does not support reference to the UN Secretariat compiling national views***, noting this would be a duplication of existing efforts, such as those undertaken by UNIDIR.

The outcomes: Both formulations 'norms' and 'objectives' have been removed from paragraph 30 of Rev 2 of the second APR.

Mapping convergences: Legal gaps and capacity needs

As discussed in December 2023[100]

The discussion on international law in the use of ICTs by states was guided by four questions: whether states see convergences in perspectives on how international law applies in the use of ICTs, whether there are possible unique features of cyber domain as compared to other domains that would require distinction in application of international law, whether there are gaps in applicability, and on capacity-building needs. While some delegations had statements prepared by legal departments or had legal counsel input, others, especially developing countries, needed support in formulating their interventions.

Convergences in perspectives on how international law applies in the use of ICTs

The overwhelming majority of delegations stated that there agreement that international law, in particular, the UN Charter, is applicable in cyberspace (**Thailand**, **Denmark**, **Iceland**, **Norway**, **Sweden**, **Finland**, **Brazil**, **Estonia**, **El Salvador**, **Austria**, **Canada**, **the EU**, **Republic of Korea**, **Netherlands**, **Israel**, **Pakistan**, **UK**, **Bangladesh**, **India**, **France**, **Japan**, **Singapore**, **South Africa**, **Australia**, **Chile**, **Ukraine**, and others). These states see the need to deepen a common understanding of how existing international law applies in cyberspace, alongside its possible implications and legal consequences. Most delegations also stated that cyberspace is not unique and would require a distinction in how international law applies. **Kenya** pointed out the role of regional organisations in clarifying how international law applies to cyberspace, the African Union in particular, and their contributions to this debate, which was supported by many.

[100] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Stadnik, 'OEWG's sixth substantive session.'

India stated that, in their view, ***the dynamic nature of cyberspace creates ambiguity in the application of international law*** since a state, as a subject of international law, can exercise its rights and obligations through its organs or other natural and legal persons.

Another group of states (**Cuba**, **Nicaragua**, **Vietnam**, and **Syria**) ***maintained that cyberspace is unique and can not be addressed by applying existing international law***. ***They call for a legally binding instrument in the UN framework***. **Russia** and **Bangladesh** see gaps in international law that require new legally binding regulations. According to **China** and **Syria**, the draft of the International Convention on International Information Security proposed by Russia would be a good starting point for such negotiations.

The delegations also discussed general international law principles enshrined in the UN Charter. ***There is an overarching agreement that the principles of sovereignty and sovereign equality, non-intervention, peaceful settlement of disputes, and prohibition of the use of force apply in cyberspace*** (**Malaysia**, **Australia**, **Russian Federation**, **Italy**, **the USA**, **India**, **Canada**, **Switzerland**, **Czech Republic**, **Estonia**, **Ireland**, others).

The states concluded that ***the principles of due diligence, attribution, invoking the right of self-defence, and assessing whether an internationally wrongful act has been committed requires additional work to understand how they apply in cyberspace.***

Many delegations (**Australia**, **Canada**, **the EU**, **New Zealand**, **Germany**, **Switzerland**, **Estonia**, **El Salvador**, **the USA**, **Singapore**, **Ireland**, and others) stated that ***the discussions need to clarify how international law addresses violations, what rights and obligations arise in such case, and how international law of state responsibility applies in cyberspace***. **Mexico**, **Italy**, and **Bangladesh** see value in the contributions of the UN International Law Commission to this debate.

The majority of delegations see convergence in understanding that IHL applies in cyberspace in cases of armed conflict and that the states must adhere to international legal principles of humanity, necessity, proportionality and distinction (**Kiribati**, **UK**, **Germany**, **the USA**, **Netherlands**, **El Salvador**, **Ukraine**, **Denmark**, **Czech Republic**, **Australia**, others). Deeper discussions on this matter were deemed necessary. **Cuba**, in line with its previous statements, ***disagreed with the concept of applying IHL in cyberspace.***

Addressing capacity building in international law, **Uganda** stated that it is extremely difficult for developing countries to be equal partners and effectively participate globally due to a lack of expertise and capacity. The majority of countries have supported continuous capacity building efforts in international law (**Thailand**, **Mexico**, **Nordic countries**; **Estonia**, **Ireland**, **Kenya**, **the EU**, **Spain**, **Italy**, **Republic of Korea**, **Netherlands**, **Malaysia**, **Bangladesh**, **India**, **France**, **Japan**, **Singapore**, **Australia**, **Switzerland**), with **Canada** mentioning two priority areas: national expertise to enable meaningful participation in substantive legal discussions in multilateral processes such as our OEWG and expertise to develop national or regional positions. Almost all delegations have found the UNIDIR workshop to be a valuable contribution to understanding international law's applicability in

cyberspace.[101] Several delegations have underscored the value of sharing national positions (**Thailand**, **Brazil**, **Austria**, **the EU**, **Israel**, **the UK**, **India**, **Nigeria**, **Nordic countries**, and **Mexico**) in capacity-building and confidence-building measures.

Going forward, most speakers (**Estonia**, **the EU**, **Austria**, **Spain**, **Italy**, **El Salvador**, **the Republic of Korea**, **the UK**, **Malaysia**, **Japan**, **Chile**, and others) supported the proposal to hold a two-day inter-sessional meeting dedicated to international law.

At a standstill: IHL debates deepen amid ICT law uncertainty

As discussed in March 2024[102]

The member states have held their previous positions on the applicability of international law. Most states have confirmed the applicability of international law to cyberspace, including the UN Charter, international human rights law and IHL. However, **Russia** and **Iran** stated that ***existing international law does not apply to cyberspace***, while **Syria** noted that how international law applies in cyberspace is unclear. However, **China and Russia** pointed out that the principles of international law apply. These states, as well as **Pakistan, Burkina Faso, and Belarus**, support the development of a new legally binding treaty.

Of note was the contribution by Colombia on behalf of Australia, El Salvador, Estonia, and Uruguay that reflected on the continued engagement of a cross-regional group of 13 states based on a working paper from July 2023.[103] The contribution highlighted the emerging convergence of views that:

- States must respect and protect human rights and fundamental freedoms, both online and offline, by their respective obligations.
- States must meet their international obligations regarding internationally wrongful acts attributable to them under international law, which includes reparation for the injury caused.

---

[101] United Nations Institute for Disarmament Research, *Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations* (Conference Report, UNIDIR Security & Technology Programme, July 24, 2023), accessed August 5, 2025, https://unidir.org/wp-content/uploads/2023/09/UNIDIR_CS_2023-Conference_Report_Use_of_ICTs_by_States_Roles_Responsibilities_under_UN_Charter.pdf

[102] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's seventh substantive session.'

[103] Australia, Colombia, El Salvador, Estonia, and Uruguay. *Joint Statement on International Law*. Delivered at the seventh session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG7_-_Legal_Grouping_-_Joint_Statement_-_Final.pdf. and Australia, Colombia, El Salvador, Estonia, and Uruguay. *Applicability of International Law, in Particular the United Nations Charter, in the Use of ICTs: Areas of Convergence*. 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.

- International humanitarian law applies to cyber activities in situations of armed conflict, including, where applicable, the established international legal principles of humanity, necessity, proportionality and distinction.

Many states echoed the Colombian statement, including **Germany, Australia, Czechia, Switzerland, Italy, Canada, the USA, the UK, Spain** and others.

New discussion point: Reparation for the injury caused

The contribution by Colombia on behalf of Australia, El Salvador, Estonia, and Uruguay highlighted that ***states must meet their international obligations regarding internationally wrongful acts attributable to them under international law, which includes reparation for the injury caused***, a new element in the discussions within the OEWG substantive sessions. **Thailand, Uganda, and the Netherlands** have also specifically addressed the **need for reparation for the injury caused**.

Applicability of IHL

The discussions have also progressed on the applicability of IHL to the use of ICT in situations of armed conflicts.

Senegal presented a working paper on the application of IHL on behalf of **Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Sweden, and Switzerland.**[104] This working paper shows convergence on the applicability of IHL in situations of armed conflict. It delves deeper into the principles and rules of IHL governing the use of ICTs, notably military necessity, humanity, distinction, and proportionality. Other states welcomed with working paper, including **Italy, Australia, South Africa, Austria, the United Kingdom, the USA, France, Spain, Uruguay** and others.

On the other hand, **Sri Lanka, Pakistan, and China** have ***called for additional efforts to develop an understanding of the applicability of IHL and its gaps***.

In its statement on IHL, the **ICRC** has pointed out the differences between the definitions of armed attack under the UN Charter and under IHL, the need to discuss how IHL limits cyber operations, and the need to interpret the existing rules of IHL as not to undermine the protective function of IHL in the ICT environment.

The discussion on international law greatly benefited from the recent submission to the OEWG by the Peace and Security Council of the **African Union** on the Application of international law in the use of ICTs in cyberspace (**Common African Position**).[105] Reflecting the views of 55 states, it represents a significant contribution to the work of the OEWG and an example of valuable input by regional forums. This comprehensive position paper addresses issues of applicability of international law in cyberspace, including human rights and IHL, principles of sovereignty, due diligence, prohibition of intervention in the affairs of

[104] Brazil et al., *Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts*, 1 March 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations.pdf.
[105] African Union Peace and Security Council, CAP Communiqués FULL, adopted at the 1196th meeting on 29 January 2024, African Union, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/CAP_Communiques_FULL_0e34eb5799.pdf.

states in cyberspace, peaceful settlement of disputes, prohibition of the threat or use of force in cyberspace, rules of attribution, and capacity building and international cooperation. The majority of the delegations welcomed the Common African Position.

The Chair has also pointed out that, at that point in time, 23 states shared their national positions, and many others were preparing their positions on the applicability of international law in cyberspace.

Most states supported scenario-based exercises to enhance the understanding between states on the applicability of international law. They wanted to have the opportunity to conduct such exercises and have a more in-depth discussion on international law in the May intersessional meeting. **China *firmly opposed this.***

Several states, such as **Japan, Canada, Czechia, the EU, Ireland** and others, ***wished to see future discussions on international law embedded in the Programme of Action (PoA).***

From dispute settlement to IHL: Views on applicability of international law

As discussed in July 2024[106]

In July 2024, states met at the eighth substantive session to adopt the group's third APR.[107]

The Point of Contact (PoC) directory as a mechanism for peaceful dispute settlement

Switzerland expressed surprise at the mention of the Point of Contact (PoC) directory in paragraph 36B as a potential avenue for facilitating dialogue between states for peaceful dispute settlement. They pointed out that the PoC was not discussed as a potential instrument for dispute resolution within the OEWG and requested the deletion of this sentence. **The USA** echoed this sentiment, acknowledging the PoC directory's role in facilitating communication for various cyber purposes but arguing that it is not appropriate for dispute settlement, which involves diplomatic engagement methods outlined in Article 33 of the UN Charter, such as negotiation, mediation, and arbitration. **The Netherlands** agreed, stating that the PoC directory did not feature prominently in discussions on international law and supporting the inclusion of Chapter 6 of the UN Charter, which provides for the peaceful settlement of disputes instead.

The outcome: The mention of the PoC directory as a facilitator for peaceful dispute resolution was deleted altogether from the third APR.

The applicability of IHL in the context of ICTs

The debate over the inclusion and specificity of IHL in the context of ICTs revealed once again a significant divide among states. On the one hand, countries like **Nicaragua**, **Russia**, **Belarus**, **Syria**, **China**, and **Venezuela** argued that the ***current references to IHL***

[106] Gavrilovic, Kazakova, Petit-Siemens, Roellinger, 'OEWG's eight substantive session.'
[107] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR)*.

in the proposed texts, specifically paragraphs 36(f) and 36(g), as they apply to civilian objects and critical infrastructure, went far beyond the consensus that had been reached within the OEWG. **Venezuela** emphasised that existing international laws and non-binding norms are inadequate for the complex virtual environment of cyberspace, which differs significantly from the traditional contexts these laws were designed to address. Consequently, **Venezuela**, along with other states, supported the creation of a legally binding convention under the UN to address international security in the use of ICTs. Similarly, **Nicaragua** criticised the section on international law for capturing progress on certain aspects while ignoring the specific proposal for a UN Convention on International Information Security, as proposed by **Russia** and supported by several delegations.[108] **Russia** insisted that, given the absence of consensus on the applicability of IHL to the digital sphere, the unique nature of cyberspace necessitates new legally binding conventions to ensure stability and security, free from the subjective interpretations of traditional IHL that might lead to politically motivated abuses.

Conversely, countries such as **Germany**, **Canada**, **Switzerland**, and **the USA**, among others, ***pointed to the substantial body of existing norms and rules regarding state behaviour in cyberspace, as endorsed by previous UN working groups and the General Assembly.*** **Germany** urged Nicaragua and others to consider these achievements and the wealth of agreed norms already in place. **Brazil**, for instance, reminded delegations that the applicability of IHL in situations of armed conflict was recognised by the last GGE in a report that was endorsed by consensus by the General Assembly in Resolution 7619. Delegations like those of **Switzerland**, **the EU** and **the USA** proposed clarifications in paragraphs 36(f) and 36(g) to ensure precision and avoid ambiguity by inserting references to obligations under IHL in situations of armed conflict.

The outcome: Ultimately, the outcome disappointed many delegations advocating for the explicit inclusion of IHL, as the third APR did not reflect these discussions. This omission, was seen by delegations including Switzerland, the EU, and Senegal, among others, as a significant concession by the chair, failing to capture the comprehensive legal framework necessary to address the challenges posed by the use of ICTs in modern conflicts. This divide highlighted the need for ongoing dialogue and negotiation to reconcile these differing perspectives and ensure a robust, transparent, and universally applicable legal framework for cyberspace.

Sharing national and regional views on the applicability of international law

Delegations from **Japan**, **France**, and **Australia** supported the call for sharing national and regional views on how international law applies in cyberspace, believing such efforts would deepen discussions in both the current OEWG and future mechanisms. In contrast, **Russia** saw no added value in exchanging regional positions on this topic. **China** further argued that submitting country-specific or regional positions contradicts the goal of promoting a unified international law stance globally, as individual interpretations could increase differences and weaken trust among states.

---

[108] Russian Federation and like-minded states, *Concept of a UN Convention on Ensuring International Information Security*, submitted to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, April 2023, 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.

The outcome: The third APR does not mention sharing regional views on the applicability of international law.

Delegations such as **Mexico**, **New Zealand**, **Switzerland**, and **Argentina** were also disappointed by the removal of references to scenario-based exercises in the APR, given how many delegations had commended their value and usefulness to deepen discussion on the application of international law to cyberspace.

Growing momentum on sharing views; Consensus remains elusive

As discussed in December 2024[109]

More than fifty member states delivered their statements in the discussions on international law, which included several small and developing states that have previously not done so.

The discussions highlighted the diverse national and regional perspectives on the application of international law, especially the Common African Position on the application of international law in cyberspace, and **the EU's** Declaration on a Common Understanding of International Law in Cyberspace.[110] **Tonga**, on behalf of the 14 Pacific Island Forum member states, presented a position on international law affirming that international law, including the UN Charter in its entirety, is applicable in cyberspace.[111] **Fiji**, on behalf of a cross-regional group of states that includes **Australia**, **Colombia**, **El Salvador**, **Estonia**, **Kiribati**, **Thailand**, and **Uruguay** recalled a working paper that reflected additional areas of convergence on the application of international law in the use of ICTs.[112]

As mentioned by Canada, Ireland, France, Switzerland, Australia, and others, ***these statements build momentum at the OEWG in building common understandings on international law***, as over a hundred states have individually or collectively published their positions.

Applicability of international law to cyberspace

---

[109] Gavrilovic, Kazakova, Ittelson, Stadnik, Petit-Siemens, 'OEWG's ninth substantive session'.
[110] African Union (AU), *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, adopted by the Peace and Security Council at its 1196th meeting, 29 January 2024, https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y. and European Union (EU), *Declaration on a Common Understanding of the Application of International Law to Cyberspace*, approved by the Council on 18 November 2024, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.
[111] Pacific Islands Forum countries (Australia, Fiji, Kiribati, Federated States of Micronesia, Marshall Islands, Nauru, New Zealand, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu), *Statement on the Application of International Law to the Use of ICTs*, delivered at the Ninth Session of the Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025, 4 December 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PIF_Statement_OEWG_ICTS_Int_Law.
[112] Australia, Colombia, El Salvador, Estonia, Uruguay, 'Working Paper: Application of international law in the use of ICTs: areas of convergence,' 30 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/240530_-_Cyber_OEWG_-_Working_paper_on_the_application_of_international_law_in_the_use_of_ICTs_-_submitted_by_a_group_of_States.pdf

Despite the many published statements and intensified discussions, the main major rift between the states persists. On the one hand, ***the vast majority of the member states call for discussions on how international law applies in cyberspace*** and do not see the reason to negotiate new legally binding regulations. On the other hand, ***some states want to see the development of new legally binding regulations*** (**Iran**, also recalling requests by the countries of the Non-Aligned Movement, **Cuba** on behalf of the delegations of the **Bolivarian Republic of Venezuela**, **Nicaragua**, as well as **Russia**, **China**, **Pakistan**).

The majority of the states emphasised the applicability of IHL in the cyber context (**the EU**, **Lebanon**, **the USA**, **Australia**, **Poland**, **Finland**, **Republic of Korea**, **Japan**, **Malawi**, **Egypt**, **Sri Lanka**, **Brazil**, **South Africa**, **the Philippines**, **Ghana**, and others) recalling the Resolution on protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict adopted by consensus at the 34th International Conference of the Red Cross and Red Crescent as a major step forward in international armed conflicts.[113]

The EU, **Colombia**, **El Salvador**, **Uruguay**, **Australia**, **Estonia**, and others expressed regret that the APR3 did not include a reference to the IHL and called for it to be included in the final OEWG report.

Other topics

The states also shared what topics in international law shall be discussed in more detail. ***State responsibility, sovereignty and sovereign equality, attribution and accountability*** were the most mentioned topics. The member states differed in their opinions on whether the topic of international law and norms should be discussed in the future mechanism within one thematic track or not.

On capacity building in international law, ***scenario-based exercises received overwhelming support***, with **Ghana** and **Sierra Leone** recalling the importance of South-South cooperation and regional capacity-building efforts.

One of the main deciding factors for the future of discussions on international law will certainly be the future permanent mechanism, if the states decide to establish under said mechanism a dedicated group which will discuss international law. That would allow states to keep a status quo until the end of the OEWG's mandate and defer the issue to the next mechanism.

Penultimate session concluded; Progress remained limited

As discussed in February 2025[114]

The discussions on international law have shown little progress in drawing closer between the positions. The states have made suggestions on how to capture the progress of the

[113] International Conference of the Red Cross and Red Crescent, 'Resolution: Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict,' 34th International Conference of the Red Cross and Red Crescent, October 2024, https://rcrcconference.org/app/uploads/2024/11/34IC_R2-ICT-EN.pdf.
[114] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's tenth substantive session.'

OEWG 2021-2025 in its final report and shared opinions on the structure and content of discussions on international law within the future permanent mechanism.

The persistent rift: The need for a new legally binding framework

In the substantive positions of the states on international law, the rift remained between the states that **do not see a need for a new legally binding framework and those that do**.

The majority of states (**Sweden, the EU**, **the Republic of Korea, the UK and others**) ***do not see the need for a new legally binding framework*** and emphasise the need to discuss the application of existing international law in cyberspace. In rushing to discuss new legally binding obligations, the **UK** sees the risk of undermining the application of core, foundational rules of international law, including the UN Charter.

Cuba, China, Russia, Pakistan, and the Islamic Republic of Iran reiterated their positions, stating that ***the new legally binding mechanism is necessary to prevent interstate conflicts in cyberspace and to contribute to strengthening cooperation in this area***. **China** has supported the Russian Draft Convention on International Information Security as a good basis for discussions.[115] At the same time, **Pakistan and Iran** stated that there are gaps in international law that need to be addressed by binding rules.

Despite the Chairs' call to states to find flexibility in their statements in December 2024 and time pressure, the statements on both sides are repeats of the positions voiced in the past substantive sessions.

These differences directly translate to the language that the states were proposing to be included in the 2021-2025 OEWG final report, as well as positions on how to structure the Future Permanent Mechanism.

Final report: How to best reflect progress

States have discussed the proposals on how to best reflect the progress in the 2021-2025 OEWG on international law in its final report, as it will serve as a summary of the efforts, positions, and basis for the negotiations within the future permanent mechanism.

The states predominantly concluded that the OEWG was a successful process and contributed to a greater understanding of international law in cyberspace. Specifically, states (**Austria, Sweden, Brazil, Senegal, Canada, Thailand, Czechia, EU, Vanuatu, Switzerland, Australia, Germany and others**) ***saw progress in a number of published national and regional positions on the applicability of international law in cyberspace*** in the course of the 2021-2025 OEWG.

There were also specific wording suggestions for inclusion in the final report. The Joint Statement on International Law (**Australia, Chile, Colombia, the Dominican Republic, El Salvador, Estonia, Fiji, Kiribati, Moldova, the Netherlands, Papua New Guinea, Thailand, Uruguay and Vietnam**) gained support from **Czechia, Canada, Switzerland, United Kingdom, Republic of Moldova**, **Ireland**, and others. The

[115] Russian Federation and like-minded States, *Concept of a UN Convention on Ensuring International Information Security*, April 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

re-published paper, now with more co-sponsors, offers a convergence language for the final report that includes peaceful settlement of disputes, respect for international human rights obligations, the principle of state responsibility, and application of IHL to ICT activities during armed conflicts.[116]

Another wave of proposals was focused on including a clear reference to the applicability of IHL and the fundamental legal principles of humanity, neutrality, necessity, proportionality, and distinction in the final report, supported by **Sweden, the USA, the Republic of Korea, Malawi, Senegal, the EU, Tonga on behalf of the Pacific Island Forum, Australia, Germany, Republic of Moldova, Ireland, Ghana, Austria,** and others. Just like in the 9th OEWG substantive session in December 2024, the Resolution on protection for the civilian population against the humanitarian consequences of the misuse of digital technologies in armed conflict within the framework of the 34th International Red Cross and Red Crescent Conference resonated with the states.[117]

Brazil has referred explicitly to the Operative Paragraph 4 of that Resolution ('*states recalled that in situations of armed conflict, IHL rules and principles serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities*') to be included in the final report. **Canada, France, Netherlands, Czechia, and others** supported this proposal.

Switzerland, which sees the inclusion of the applicability of IHL as a priority, has also proposed a specific wording for the final report that builds on the 34th ICRC resolution and includes medical and humanitarian facilities.

States also called for stronger wording on the applicability of human rights law **(Australia, Albania, Malawi, Mexico, Mozambique, Moldova, North Macedonia, Senegal, Switzerland, Thailand, and Germany)** in the final report.

Cuba and Iran stressed that ***the final report should include references on setting up a legally binding instrument***, and definitions of terms and technical mechanisms.

The future permanent mechanism: How to tackle international law

States further discussed ways that the discussions on international law would be incorporated and framed within the Future Permanent Mechanism.

States reflected on Annex C of the Chair's Discussion Paper on Draft Elements on Stakeholder Modalities and Dedicated Thematic Groups of the Future Permanent Mechanism, ***which proposed a dedicated thematic group on rules, norms and***

[116] Cross-Regional Group of States, Joint Statement on International Law, July 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG10_-_Joint_statement_on_international_law_-_cross-regional_group_-_final.pdf

[117] International Committee of the Red Cross (ICRC), *Protecting Civilians and Other Protected Persons and Objects against Cyber and Information Operations during Armed Conflict*, draft zero resolution adopted at the 34th International Conference of the Red Cross and Red Crescent, October 2024, https://rcrcconference.org/app/uploads/2024/04/34IC-Draft-0-Cyber-EN.pdf

principles of responsible state behaviour and on international law.[118] **Mexico, Colombia, Indonesia,** and **Algeria *endorsed the thematic group dedicated both to norms and international law***, as they see these as complementary and contributing to safety and security.

Others, such as **Sweden, the EU, Czechia, Brazil, and the USA, *did not support the Chairs' proposal to create one thematic group for norms and international law due to the voluntary nature of norms and binding nature of international law and combining these discussions posing a risk conflating distinct legal and policy concepts,*** that could hinder progress in both areas.

Canada proposed integrating ***international law into each of the first three thematic working groups set out in the Chairs' discussion paper*** (building resilience, enhancing cooperation in the management of ICT-related incidents, including through CBMs, and preventing conflict and increasing stability in the ICT sphere) to build common understandings on how international law applies to practical policy challenges. Thematic group meetings could include expert briefings on technical and legal topics and scenario-based discussions.

The states have deepened discussions on the Program of Action proposed by France, which seeks to incorporate discussions on international law in a cross-cutting manner in three action-oriented thematic groups: on building resilience, cooperation in the management of ICT-related incidents, and prevention of conflict and increasing stability in cyberspace.[119] This approach was supported by **Sweden, Portugal, Czechia, the UK, the EU, Albania, Australia**, **Germany, Ireland** and others. The PoA also foresees the inclusion of non-state experts in cybersecurity, to which the **EU and North Macedonia** specifically expressed their support.

In addition to the two proposals above, several states have voiced additional proposals regarding a thematic group on international law.

Switzerland generally supported the thematic and cross-cutting working groups as proposed by France but voiced concern that it might not be sufficient for in-depth discussions on international law. Switzerland considers it better if the discussion on the implementation of norms would occur in the cross-cutting working groups. In contrast, ***the discussion on the application of international law would benefit from a specific forum***.

The **USA** believes that the states are ready to integrate discussion into practical, thematic working groups oriented toward addressing specific, real-world concerns to international peace and stability and focusing on practical tools.

---

[118] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Letter dated 27 January 2025 (A/AC.292/2025/3), 27 January 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_27_January_2025.pdf.

[119] Cross-Regional Group of States, 'Proposal on Thematic Groups for the Regular Institutional Dialogue (RID)', 6 December 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/FR_Statement_on_RID_(proposal_on_groups)_ENG.pdf

Senegal recalled the equal importance and relevance of the five pillars of the OEWG mandate and would be willing to discuss adding a pillar on the application of international law.

Ireland ***does not consider a thematic group on international law necessary or desirable***. Their concern would be that such a group could be stifled by being overly outcome-focused and that it would duplicate efforts and divert resources and attention from more dynamic engagement on legal issues within the other thematic groups.

Conversely, **Egypt** ***sees the need for a dedicated platform on international law in the future permanent mechanism*** and is sure that the modalities, mandate, structure, and types of discussions can be agreed on by consensus. Egypt sees the discussion as reshaping the content of international law and underscores the need to have a place within the UN to have a multilateral conversation with the participation of stakeholders. **Iran**, **China** and **Russia** ***see as a priority within the future permanent mechanism to initiate a substantive discussion on developing legally binding obligations in the ICT field and have a dedicated thematic group on international law***. These states do not support the participation of non-state experts in the discussions.

The role of capacity building in fostering a better understanding of states on how international law applies to cyberspace and contributes to promoting peace, security, and stability in cyberspace was underscored by **Tonga on behalf of the Pacific Island Forum, Viet Nam, Kenya, Ghana, Canada, Thailand, UK, France, Colombia, and many others.**

Deep divisions: Limited consensus emerged

As discussed in July 2025[120]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[121] The international law section of the final report reflects the prevailing splits between the states on the need for new binding norms, the applicability of international human rights law and humanitarian law, resulting in a consensus text that fails to reflect the depth and richness of discussions on international law in the past five years.

The UN Charter: Applicability reaffirmed

States reaffirmed that international law, in particular the UN Charter applies is applicable and essential to maintaining peace, security and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Building on the previous work captured in the APRs, ***the states reaffirmed principles of state sovereignty and sovereign equality*** (based on the territorial principle), ***as well as Art. 2(3) and Art. 33(1) of the UN Charter on the pacific settlement of disputes. The reference to Art. 33 (1) has been included in the text despite the request of*** **Iran** ***to remove it, as in their opinion, it lacks consensus and reflects divergence between states.***

Further, the states ***reaffirmed the Art 2 (4) of the UN Charter on the prohibition of the threat or use of force and the principle of non-intervention.***

---

[120] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Radunovic, Roellinger, 'UN OEWG concludes.'
[121] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

The definition of what may constitute the use of force from Zero Draft ('An ICT operation may constitute a use of force when its scale and effects are comparable to non-ICT operations rising to the level of a use of force') was ***supported by*** **the EU**, **Finland**, **Italy**, **Netherlands**, **Korea**, **United Kingdom**, **Australia**, and ***was contested by*** **Russia**, **Cuba**, **Iran**, and others.

IHRL and IL: Contentious and omitted

While the final report states that the discussions on international law deepened, ***two topics have not found their place in the text – IHRL and IHL.*** Despite the strong push by **the EU**, **Australia**, **Switzerland**, **France**, **Chile**, **Colombia**, **the Dominican Republic**, **Ecuador**, **Egypt**, **El Salvador**, **Estonia**, **Fiji**, **Kiribati**, **Moldova**, **the Netherlands**, **Papua New Guinea**, **Thailand**, **Vanuatu**, **Uruguay**, **Vietnam**, **Japan**, **Nigeria** on behalf of the **African Group** and many others who supported the inclusion of references to the applicability of IHRL and IHL as part of the consensus in the final report. **Brazil**, **Canada**, **Chile**, **Colombia**, **the Czech Republic**, **Estonia**, **Germany**, **the Netherlands**, **Mexico**, **the Republic of Korea**, **Senegal**, **Sweden**, and **Switzerland** provided a statement that referred explicitly to the applicability of IHL and its principles to be included in the final report.[122] Many have mentioned the depth of work in this area, as well as the Resolution on Protection of Civilians of the 34th Conference of the Red Cross and Red Crescent Movement, a consensus document.[123] On the other hand, **Russia** considered that the work on the protection of civilians was not consensus-based, and **Belarus**, **Venezuela**, **Burkina Faso**, **the Democratic People's Republic of Korea**, **Iran**, **China**, **Cuba**, **Nicaragua**, **Russia**, and **Eritrea** considered the applicability of IHL a contentious topic on which there is a clear disagreement.

Additional binding obligations: The door is open

The final report keeps the door open for discussions on the possibility of future elaboration of additional binding obligations, if appropriate, and the development of additional legally-binding obligations. In its statement on the final report, **Russia** has already pushed for the Global Mechanism to focus, among other issues, on developing new legally binding norms in the field of digital security.[124]

What's missing?

The final report does not include references to a variety of resources that could have been the basis for discussions in the future process, from the above mentioned ICRC report, to the Common African Position, the Declaration by the European Union and its member states on a Common Understanding of the Application of International Law to Cyberspace, Updated concept for a convention of the UN on ensuring international

---

[122] India, *Working Paper on the Application of International Humanitarian Law to the Use of ICT Operations: Update 2025*, 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

[123] International Committee of the Red Cross (ICRC), 'Resolutions of the 34th International Conference of the Red Cross and Red Crescent,' *International Review of the Red Cross* 106, no. 927 (March 2025): pp. 1303–34, https://doi.org/10.1017/S1816383124000729

[124] Russian Federation, *Statement by the Russian Interagency Delegation on the Adoption of the Final OEWG Report*, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/Russia_-_OEWG_-_Adoption_of_the_final_report_-_ENG.pdf

information security (by **Belarus**, **the Democratic People's Republic of Korea**, **Nicaragua**, **Russia**, and **Syria**), as well as Working Paper on the Application of IHL to the use of information and communication technologies in situations of armed conflicts by **Brazil**, **Canada**, **Chile**, **Colombia**, **the Czech Republic**, **Estonia**, **Germany**, **the Netherlands**, **Mexico**, **the Republic of Korea**, **Senegal**, **Sweden**, and **Switzerland** and the Working Paper on the application of international law in the use of ICTs: areas of convergence outlining proposed text for inclusion in the final report international law section by **Australia**, **Chile**, **Colombia**, **the Dominican Republic**, **Ecuador**, **Egypt**, **El Salvador**, **Estonia**, **Fiji**, **Germany**, **Kiribati**, **Moldova**, **the Netherlands**, **Papua New Guinea**, **Romania**, **Thailand**, **Uruguay**, **Vanuatu**, and **Vietnam.**

The outcomes: The recommendations for the Global Mechanism in relation to the subject matter of international law reiterate further discussions on how international law applies, pushing the divides in this area into the future. The main achievement in the international law section, according to the final report, is the voluntary exchanges of national positions and the commitment to increased capacity building in this area, which was highlighted by the small and developing countries. The definition of what may constitute the use of force was omitted. IHRL and IHL were not referenced in the final report.

Confidence building measures (CBMs)

CBMs: Their importance and the way forward for the OEWG

As discussed in December 2021[125]

There was a broad consensus that CBMs are an important and integral part of the previously agreed-upon framework for responsible state behaviour, though states placed different emphasis on them. **The Netherlands**, for instance, considered CBMs as a key pillar of the OEWG work, while **China** reminded that CBMs cannot replace the international norms setting, and **Cuba** stated that CBMs are supplementary to the international legal instrument for cyberspace.

Cuba noted that, for CBMs, it is important that states refrain from turning to unilateral coercive measures which restrict universal access to technologies. While inviting for an agreement on fundamental universal principles for CBMs, **Russia** added, in a similar tone, that such principles should not provide states with instruments for military or political advantage, such as for interference in domestic affairs or punishment in the form of sanctions. **China** underlined that CBMs should not become an excuse to use weapons in cyberspace. **Iran** went further, noting that the ICT environment is a peaceful space which should be kept aside from the disarmament context, and thus the CBMs, which have military history and connotation, should not be applied in cyberspace.

Iran also warned that the reference to the UN Resolution 43/78 (H) of 1988, which provides guidelines for CBMs adopted by the Disarmament Commission, may leave a false impression that cyberspace is recognised as a battlefield. **Egypt**, on the contrary, suggested that states to take into consideration these guidelines and the UN Resolution 43/78.

Regional experiences and cross-regional exchange

A number of countries, including **Argentina**, **Indonesia**, **Chile**, **Cuba**, and **Thailand,** clearly recognised the OEWG itself as an important CBM. The work of regional organisations in defining and implementing CBMs was reiterated over and over again. **Indonesia**, **Japan**, **Malaysia**, and **Thailand**, among others, showcased the good practices by the ASEAN and the ASEAN Regional Forum (ARF); **Estonia**, **Germany**, **Serbia**, and **Switzerland**, among others, have elaborated on 16 OSCE CBMs and practical follow-ups; **Chile and other OAS members** have reflected on the 6 OAS CBMs. Most countries agreed about the value of cross-regional exchange of experiences out of and within the OEWG.

There were differences, however, in observing the role of regional experiences within the OEWG. Switzerland reminded that the OEWG and GGE reports underscore the relevance of regional and subregional efforts, while **Korea** and **Serbia** underlined that regional efforts are an important contribution to the OEWG and the development and advancement of CBMs. **The EU, together with North Macedonia, Montenegro, Bosnia, Ukraine, Georgia, and**

[125] Digital Watch Observatory, *UN OEWG 2021–2025 – Confidence building measures (CBMs)*, 16 December 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/confidence-building-measures-cbms.

Moldova, suggested that the OEWG should continue to provide space for regional fora to share practical tools, best practices, and examples to further advance the development and implementation of CBMs, which helps their improvement and engages other interested stakeholders in implementation. **Estonia** suggested that the OEWG to enhance cross-regional information and identification of synergies through regional road maps or toolboxes. **The Netherlands** went further to suggest that the OEWG to facilitate adherence of states to CBMs developed by regional organisations and multistakeholder initiatives, by providing practical measures to disseminate and exercise CBMs, and providing guidance to universalise those already existing CBMs that are based on the GGE consensus. In this direction, **Malaysia** called for the OEWG to adopt the existing practical measures implemented by the regional and subregional organisations. **Indonesia** called for expanding regional efforts into global ones, but taking into account regional differences.

Cuba was particularly cautious about regional experiences in the global context, noting that every region or subregion has its own specificities and therefore CBMs implemented at that level cannot be considered as global models; in addition, their implementation should be voluntary, and not allow interference in the internal affairs of a state. **India** noted that CBMs of global relevance could be propagated and implemented on regional levels, but agreed that frameworks developed at the bilateral and regional levels may have their own limitations – at least as an action point for the first substantive session of the OEWG. **Indonesia** and **Thailand** supported the cross-regional exchange, but emphasised that the UN maintains the lead role in CBM development and implementation.

Proposals for actions

A number of concrete proposals for ways forward for the OEWG were also brought up. Following the OSCE example of states and group of states voluntarily spearheading particular CBMs to further explore their implementation, as presented by **Estonia** and **Serbia**; **Germany** suggested that the OEWG can embrace similar approach and engage states in groups to advance particular CBMs with involvement of the industry, academia, and others; **Germany**, **Serbia**, **and Switzerland** offered to elaborate this proposal to other delegations. **Germany** also proposed that the list of national terminology on ICT, compiled by the OSCE as part of its CBMs, be offered to all the UN member states.

India noted that harmonisation of regional CBMs is the key to developing a common action by the international community, and invited the OEWG to create an indicative list of agreed CBMs to be implemented voluntarily. **The Netherlands** invited the OEWG to advise states to make declaratory statements reaffirming that they subscribe to and adhere to the CBMs within the existing Framework adopted by the UN GA.

Egypt invited states to address requests to mitigate concerns emanating from their own territories, while taking into account the limited capacities that certain states might have in this regard. **Russia** invited states to conduct consultations on their activities in cyberspace that could cause concern, and proposed establishing a practice of exchanging national lists of spheres involving critical information infrastructure. **Iran** went a step further to invite states with offensive cyber capabilities to unilaterally declare to refrain from offensive use of it.

India invited states to recognise critical transnational networks, respect the designation of critical infrastructure and transnational infrastructures by other states, and organise joint drills and tabletop exercises (TTX) for national CERTs. **Cuba** suggested that states to

standardise the methodology of cyber incidents and incident response, and provide CERTs with tools to capture and process evidence related to published or hidden vulnerabilities. **Mexico** suggested the creation of a global cyber incident repository, which can be used by member states to voluntarily share their experiences on the technical characteristics and variables of attacks or incidents reported.

Columbia invited states to translate CBMs into tangible action with the support of the multiple stakeholders; **Estonia** and **Switzerland** underlined the important role of the private sector in particular. **Korea** confirmed that a multistakeholder approach is essential to CBMs, and called for utilising available technical instruments like FIRST, the global network of CERTs, for communication. Israel focused on public-private partnerships to develop skilled cyber professionals and bridge the existing global gap in demand. It shared its experiences with engaging the private sector for 'out of the box' solutions, running education programmes for girls and women and the wider population, and developing cybersecurity research centres that assist regulators and policy makers to get a holistic view of progress.

Points of Contact

Points of Contact (PoC) were of particular relevance for many countries. **Germany** presented PoC as the basis for other CBMs and information exchange. **Russia** saw PoC as an immediate follow-up on the invitation by the previous OEWG to share information, though it noted that the amount of information should be determined by states themselves. **Cuba** also noted that information sharing should not reveal state's capacities.

Chile and **Singapore** both invited states to establish a global PoC list in the context of the UN, on the basis of existing regional PoC networks, and **the Netherlands** suggested that the OEWG enhance the existing directories. **Thailand** and **the Netherlands** have suggested this list to contain contacts on technical and diplomatic levels, **Costa Rica** and **Indonesia** listed policy level as well, while **Malaysia** and **Singapore** also listed law enforcement level, based on the experiences of the ARF. **Japan** suggested identifying a coordinator country in each region to simplify managing PoCs and updating the lists.

The Netherlands invited states to shape the framework for the PoC interaction, while **India** proposed to create a robust mechanism for sharing PoC and information, and suggested that the Secretariat collect PoCs. **Costa Rica** invited the OEWG to develop a template for communication among PoC, including conducting communications checks to keep the directory up-to-date, and scenario exercises to test their work. **Estonia** and **Singapore** also invited a demonstration of the value of such PoC networks through training and TTX, based on the experiences of OSCE and ASEAN, respectively. Singapore added that such tests could develop a common understanding about the minimum thresholds for cyber incidents, and offered to work with the UN on such exercises with PoCs of all states in tthe echnical and operational domains at the Singapore Cyber Week in 2022.

A central repository of information

India proposed to create a related repository of PoC and shared information, while **Argentina** added the legislative repository and a glossary of common definitions. Many countries shared the view that the UNIDIR Cyber Policy Portal is a convenient platform for information sharing. **Japan** invited governments to submit new lessons learned at the OEWG meetings, as well as to the Cyber Policy portal. **The Netherlands**, which invited OEWG to encourage states to share the information about their national policies and

positions, and how they advance implementation of norms and CBMs, saw Cyber Policy Portal as useful also for publishing state positions on the interpretation of how international law applies to cyberspace.

Korea, Egypt, Indonesia, Estonia, and Costa Rica also expressed support for the role of the Cyber Policy Portal for the exchange of information, as well as indexing and disseminating accumulated experiences of states and regional organisations, and a central place for states to report their progress on CBMs. In addition, **Costa Rica** suggested forming templates for reporting on CBMs, possibly following the example of the biological weapons convention, and invited the OEWG to standardise the information which states should include in their reports.

Broader issues

A number of delegations reflected on issues not directly included in the OEWG mandate. **India** warned about the proliferation of misinformation, smear campaigns, and terror propaganda, and outlined the obligation of the states to cooperate on counterterrorism as CBM (include removing harmful content). **India** also invited the OEWG to develop an effective mechanism for sharing information and digital evidence between law enforcement agencies, to counter terrorism and crime in order to build confidence. **Malaysia** also shared the ARF experiences with sharing on preventing criminal and terrorist use.

Cuba expressed belief that internet governance with the participation of states on equal footing is required to close the digital gap and build confidence. In the same vein, **Iran** called the OEWG to address the main source of mistrust in the ICT environment: the monopoly in the internet governance, coupled with challenges of anonymity, offensive cyber strategies, hostile image building, and xenophobia, which is leading to unilateral coercive measures and a lack of responsibilities. Therefore, Iran continued, CBMs should be extended to areas such as national security and limiting coercive policies and measures against other states, but also to cryptocurrencies, ICT products, services, and content.

Early areas of convergence: A national survey of implementation and a PoC Directory

As discussed in March 2022[126]

A national survey of implementation

CBMs showed themselves to be one field where possible progress in talks was spotted early. An old proposal was tabled by **Mexico** to establish a national survey of implementation of the UN framework as a practical mechanism for countries to map their own actions that contribute to building confidence and share best practices with others. This led to the establishment of a repository – introduced by **Australia,** hosted by UNIDIR at its Cyber Policy Portal – of national policies and strategies, positions on the applicability of international law in cyberspace, contact points, etc.

[126] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.'

On one hand, a repository could increase the transparency about how countries approach cybersecurity, which in turn would reduce chances for misunderstanding among diplomats, as well as states' technical experts. On the other hand, the repository could play an important role in capacity building: developing countries may learn from others about practical ways to uphold the agreed framework through the work on national policies and strategies, capacities of CERTs, and shaping positions about international law, and proudly showcase their progress in future OEWG statements and submissions.

Establishing points of contact (PoCs)

An even more important achievement may be anticipated in the long run. The severity and impact of various global cyber incidents in the past years have nudged experts to question if an operational body of diplomats could be created to address crises as they emerge, much like how CERTs already function well in networks like FIRST. The shapes of such a formation seem to be emerging from a CBM agreed upon in the OEWG and GGE in 2021: that ***states should consider nominating a national Point of Contact (PoC) at the technical, policy, and diplomatic levels (if not also law enforcement or other), and work on establishing a PoC directory at the global level.***

There seemed to be a general agreement at the second substantive session – including by states with typically opposing views, such as **the USA** and **Russia** – that ***this directory should further be turned into an active, operational, and regularly tested network***.

There is still a diversity of views on what such a network would do: from running regular table-top exercises and exchanging information about incidents, reacting to requests from other states in relation to malicious activities, to becoming an international coordination mechanism for detecting, preventing, and responding to attacks, with a 24/7 system and hotlines for crisis management.

Protocols and procedures for communications among PoC, especially during crises, were then expected to be discussed at the next OEWG meetings. But – first things first: states had to nominate their PoCs, so that the directory – then expected to be hosted through the UNIDIR Cyber Policy Portal – could be formed.

Laying the groundwork: First steps toward the PoC Directory

As discussed in August 2022[127]

In July 2022, states met at the third substantive session to adopt the group's first APR.[128] ***The idea of a global PoC directory had been enjoying support during the OEWG***, with many countries using this session to underline that a recommendation for this directory should be included in the annual progress report. **Singapore suggested** that this directory can be coordinated by UNODA, while **Malaysia** and **the Netherlands** suggested leveraging the existing PoCs within regional and sub-regional platforms.

[127] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted'.
[128] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*.

The informal 'confidence builder' group, which included **Australia**, **Brazil**, **Canada**, **Germany**, **Israel**, **Mexico**, **the Netherlands**, **the Republic of Korea**, and **Singapore,** also noted that the PoC directory should build upon the existing regional efforts and should be complementary to the existing regional efforts. Modalities of the PoC can be discussed in further sessions, this group noted.

Russia noted that the creation of a registry of PoCs is a 'strategically urgent task' as it would establish direct ties and cooperation between relevant agencies. It would also ease threats and tensions as regards to conflicts and misunderstandings, and incidents in the ICT realm. Russia submitted its proposal to this effect.

It was then expected that more countries would share their views on the topic over the subsequent substantive sessions. The UN Secretariat was requested to seek those views and produce a background information paper on them by the end of January 2023, which would feed into discussions during the fourth and fifth substantive sessions of the OEWG.

The outcomes: Creating a global directory of ICT PoCs was among the recommended further steps listed in the first APR, to be discussed at the fourth and fifth substantive sessions of the OEWG. The significant work done by regional organisations on the CBMs was also recognised in the section on the CBMs.

Diverging views on the PoC Directory and the introduction of the GCSCP proposal

As discussed in December 2022[129]

Delegations focused on establishing a directory of national Points of Contact (PoC), and which types of PoC should be listed in the directory. There were a number of other proposals related to CBMs and capacity building. The UN allocating more resources for capacity building programmes, a cyber fellowship programme being established under the OEWG, and a global cybersecurity cooperation portal being created were among the proposals that stood out.

The global PoC directory

As the PoC directory was discussed by the **OEWG**, the disarmament arms of the UN, ***UNODA and UNIDIR presented an overview of then-current positions.***[130] The two presentations indicated general agreement about the importance of creating a PoC directory

[129] Gavrilovic, Ittelson, Petit-Siemens, Radunovic, Roellinger, Stadnik, 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs'.
[130] United Nations Office for Disarmament Affairs, *Preliminary overview of State inputs on PoC directory: OEWG intersessional, December 2022*, UNODA, 5 December 2022, accessed 23 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Preliminary_overview_of_State_inputs_on_PoC_directory_OEWG_intersessional_Dec_2022.pdf and United Nations Institute for Disarmament Research (UNIDIR), *UNIDIR PoC preliminary results v3, December 2022*, UNIDIR, accessed 23 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNIDIR_POC_preliminary_results_v3_dec2022_0.pdf

(figure 1), suggested the role of UNODA Secretariat in its maintenance and emphasised the online format available in all UN official languages (figure 2).

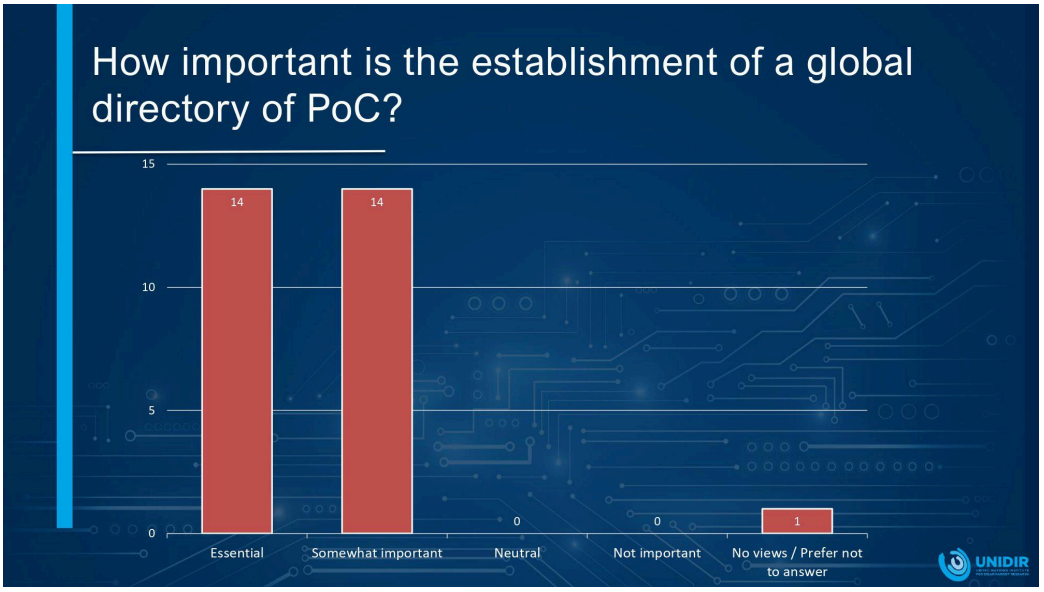


Figure 1: The majority of states agreed that the establishment of a PoC directory is important. *Source*: UNIDIR.

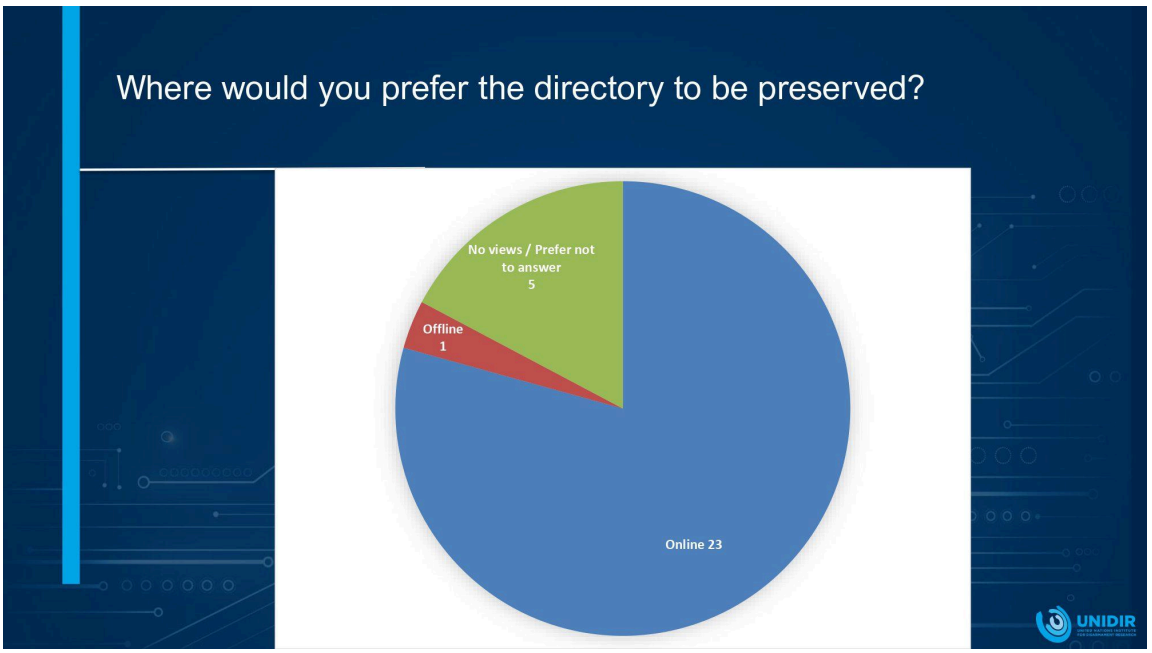


Figure 2: The majority of states expressed a preference for an online PoC directory. *Source*: UNIDIR.

Building on this summary, ***delegations shared the view that CBMs should be implemented gradually and that the PoC directory constitutes a good starting point***. A vast majority of states ***emphasised the need to build on existing PoC infrastructures from regional organisations and integrate them so that efforts and information aren't duplicated.***

What kind of activities could be pursued by the PoCs, and how the directory could be used, were questions that remained open. **Italy** and **Germany**, for instance, supported the

low-hanging fruit perspective, explaining that the higher the level of details the PoC directory ambitions to collect, the more difficult it will be to agree on its format. **France** suggested that the PoC should start with very simple tasks, while **South Korea** suggested that the PoC should stay flexible when it comes to details, modalities, and timelines. **Tanzania** suggested that PoC could assess the capacity-building needs and requirements of each region or each nation. **Iran** stated that capacity building was a prerequisite for developing countries to implement such a CBM. **The UK**, however, expressed concerns that the PoC directory could become a channel for capacity-building requests, such as visits and best practice exchange in CERTs.

The type of PoC that should be added to the directory was also a point of contention. According to the UNODA and UNIDIR summary of previous positions, ***the majority of states were in favour of having two PoCs – a diplomatic and a technical one with distinct functions. Yet, some states were reluctant to have PoCs at different levels*** (figure 3). Some states argued for starting with either a diplomatic or technical PoC, depending on the state's capacity to nominate one. Others, like **Estonia**, proposed to have a single PoC for efficiency.

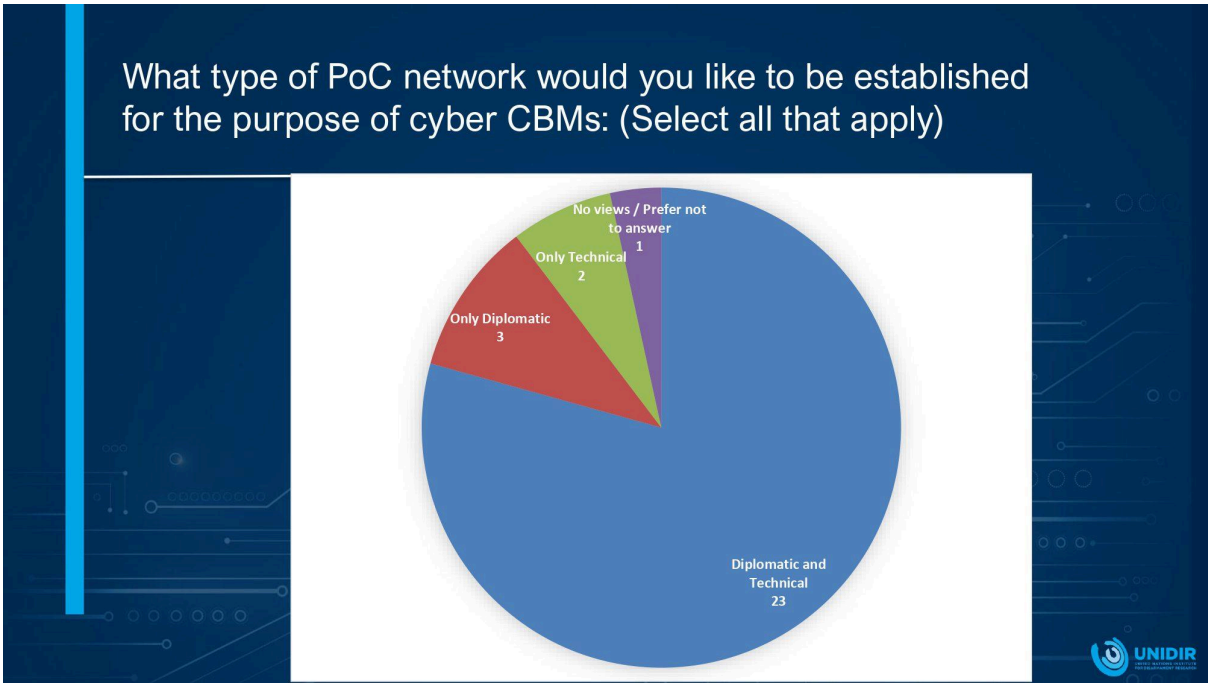


Figure 3: The majority of states expressed a preference for diplomatic and technical PoC directories. *Source*: UNIDIR.

Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, the Netherlands, Singapore, and **Uruguay** gathered around the informal working group on implementing CBMs globally, and ***presented an outline of recommended PoC tasks and a timeline of next steps.***[131] They also proposed an agreement on modalities of the UN PoC

[131] Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, Republic of Korea, Mexico, Netherlands, Singapore, and Uruguay, *Implementing CBMs Globally: Towards the UN Point of Contact Directory*, 5 December 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PoC_Directory_Next_Steps_CBM_joint_group.pdf.

directory to be included in the July 2023 Annual Progress Report and endorsed with a resolution by the First Committee subsequently.

Open stakeholder consultations on CBMs

The open stakeholder consultations on CBMs provided time for inputs from all interested stakeholders. For the first time in the OEWG process, there were official interventions from regional and sub-regional organisations sharing their experience with CBMs, cooperation between their member states, current PoC structures, and best practices related to CBMs. All speakers supported the UN role in creating a global PoC structure and underscored the importance of building upon the existing PoC networks and CBMs. The majority of speakers called for the inclusion of non-state stakeholders in the process of establishing PoC directories and CBMs.

India *proposed creating an online and centralised 'Global Cybersecurity Cooperation Portal' (GCSCP) for global cooperation in ICT security*.[132] It would aim to reduce multiple sites with the same purpose. The portal would be set under UN auspices, and the cost should be borne by the UN Secretariat. India also suggested that the GCSCP should be modular and incrementally built to respond to evolving needs, and allow ideas to mature. With both public and private interfaces, the portal would allow delegations to modulate which information is public. The GCSCP would contain:

- A repository of important documents generated during intergovernmental discussions on ICT security, of particular relevance for small delegations who will engage in the OEWG in the upcoming years
- Mapping of available assistance providers and resources, that allow countries to match their needs and request particular assistance
- PoC directory
- Conferences and events calendar
- Incident reporting tool

The proposal was well-received by delegations who expressed interest in discussing the project further. **Egypt** expressed concerns about the security of such a platform, the **Philippines** asked the secretariat to report on the feasibility and cost of the portal, while the **Netherlands** proposed to merge platforms that have already been established.

[132] India, *Working Paper on Global Cyber Security Cooperation Portal (GCSCP)*, Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG) 2021–2025, July 2022, https://documents.unoda.org/wp-content/uploads/2022/07/Global-Cyber-Security-Cooperation-Portal_.pdf

Regional organisations, additional CBMs, and key elements of the PoC Directory

As discussed in March 2023[133]

Many states highlighted the important role of regional organisations in operationalising regional CBMs. In particular, states have mentioned the value of the OSCE, the OAS and ASEAN in enhancing information sharing between states. Therefore, some delegations, e.g. the EU, have also called for more active participation of regional organisations to share their experiences in the OEWG.

Another topic in states' interventions was whether additional CBMs are needed. Some have suggested that the states should implement what has been already agreed on, while others suggested that new CBMs could be considered. **Russia** suggested agreeing on the basic universal principles of CBMs (e.g. to ensure that CBMs are not used as a tool to interfere in the internal affairs of states). **Iran** proposed developing ICT-related terminology. **Canada**, **Australia,** and the **Netherlands** have stressed the importance of exercising transparency by sharing cybersecurity agency missions and functions, national views and practices on cybersecurity incidents and related threats, and, as suggested specifically by **Canada**, what sectors each country considers as critical infrastructure. **The EU**, **Spain**, **Chile**, **Mauritius**, **South Korea**, **India**, and **Canada** stressed that active exchange with the private sector, academia, and NGOs could contribute to strengthening CBMs. Finally, **Chile**, the **Czech Republic**, **Switzerland**, **Malaysia,** and **the Netherlands** have highlighted the importance of sharing vulnerability information and coordinated vulnerability disclosure (CVD) as other concrete areas where states can further advance operationalisation efforts.

A broad agreement existed to establish a Points of Contact (PoC) Directory. However, states have shared diverging views on nuances, e.g. who should be nominated as a PoC (agencies or particular persons), who would be considered as 'technical PoCs and which functions should be assigned for both technical and diplomatic PoCs', if participation should be voluntary, and if the development and use of standardised templates should be a part of the work.

Delegations have also separately commented on capacity building elements in the context of the PoC Directory (and referring to the Chair's revised non-paper).[134] During the hybrid informal inter-sessional meeting on this topic (held on 2 March 2023), several delegations (e.g. **Australia, Austria, Canada, and China**) expressed their concerns about proposed capacity building elements. Delegations stressed that the proposed measures seem overambitious, as well as that capacity building should not end with the PoC Directory only.

As co-sponsors, **Russia**, **Belarus**, and **Nicaragua** ***have submitted a proposal for establishing a PoC directory.*** Its tasks would include: (a) defining and keeping updated a list of PoCs; (b) establishing practical interaction between authorised national organisations

[133] Gavrilovic, Grottola, Ittelson, Kazakova, Petit-Siemens, Stadnik, 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session.'
[134] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 28 February 2025*, 28 February 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_28_February_2023.pdf

in the field of computer incident response; (c) reducing tensions and the threat of conflicts resulting from misunderstanding and misperception of computer incidents. States would designate PoCs at the diplomatic and technical levels.

Iran ***proposed seven principles***, including but not limited to the principles of non-intervention in the internal affairs of other states, along with sovereign equality for the work of the PoC Directory; the principle allowing the PoCs and their resources not to be subject to restrictive and blocking measures, including unilateral coercive measures (UCMs).

Iran ***suggested that the UN Secretariat seek views from states on the capacities required for effective participation of PoCs in the Directory*** and on suitable mechanisms and actions for building such capacities. As a result, the background paper could be produced by the end of June 2023 for consideration at the 5th session of the OEWG.

The Chair shared his hope that by July 2023, states will be able to agree on modalities and adopt them within the next APR. Under such a timeline, the implementation of the PoC Directory was expected to happen only in early 2024.

The next step regarding the PoC was that the Chair will convene an informal virtual meeting at the end of April, where he plans to invite regional PoC Directories to share their experiences. After that, the Chair was expected to prepare a second revision of the PoC elements non-paper.

Advancing CBMs: Concrete proposals on operationalisation and new measures

As discussed in May 2023[135]

During the session on confidence-building measures (CBMs), delegations discussed concrete proposals to approach the operationalisation of CBMs, and also made some proposals regarding the possibility of new CBMs.

Operationalisation of CBMs

Some delegations (e.g., Canada, Chile, the EU, the Netherlands, Singapore, and the USA) ***reiterated the role of regional organisations and supported mentioning this in the second OEWG APR***. ***New proposals were also made for the operationalisation of CBMs.***

Other delegations echoed the proposals to enhance transparency. For example, **Switzerland** stressed that the operationalisation should start with the CBMs that are easier to implement, for example, those which lead to better cooperation and dialogue, as well as transparency. **Canada** also supported enhancing transparency and, in particular, acknowledging that a state has an offensive cyber capability that will be used in accordance with international norms and laws. Canada also proposed providing more transparency about what states classify as critical infrastructure, while supporting **Singapore's** suggestion to organise a workshop. **Australia** also emphasised the need for greater transparency regarding ICT security agency missions and functions, as well as their legal and oversight

[135] Gavrilovic, Kazakova, and Petit-Siemens, 'Informal OEWG consultations on capacity building.'

regimes.

Germany, on behalf of the Confidence Builders Group (Argentina, Australia, Brazil, Canada, Chile, the Czech Republic, Fiji, Israel, the Republic of Korea, Mexico, the Netherlands, Singapore, Uruguay, and Germany), ***presented the joint working paper to set incentives for the operationalisation of a PoC directory***.[136]

The possibility of new CBMs

Mexico argued that the development of new CBMs should remain on a voluntary basis. **Pakistan** proposed to focus on new CBMs in areas such as capacity building, research in cybersecurity, exchange of best practices and addressing disinformation and fake news. **Russia** added that the voluntary and non-binding nature of CBMs limits their efficiency. In developing new CBMs, **Russia** proposed agreement on basic universal principles and, in particular, stressed that it is important to observe the principle 'do no harm – i.e. new CBMs should not cause harm to the security of other states, provide advantages to any state or group of states in the military, political, economic or other spheres, should not be used as a tool for interference in the internal affairs of states, or as an instrument or pretext for sanctions or other unilateral measures.

Critical infrastructure protection

Singapore proposed an informal workshop with technical experts, policymakers, and diplomats on considerations and challenges to **protect critical information infrastructure**, and thus to identify capacity-building needs and map them into actionable implementation of the CBMs.

Germany proposed two measures based on Organization for Security and Co-operation in Europe (OSCE) regional practices to enhance the protection of critical infrastructure and to promote cooperative activities to reduce risks.

Enhancing transparency by using UNIDIR's Cyber Policy Portal

Singapore proposed ***enhancing transparency by using existing resources such as the voluntary UNIDIR Cyber Policy Portal***, and added that the portal could be further developed to include a points of contact (PoC) with relevant excerpts of the organisational charts and contact details that would be kept up-to-date annually.

Informal virtual meetings to share info on PoC directory

The Confidence Builders Group suggests that, in particular, **regular informal virtual meetings could be held by UNODA to share practical information regarding a PoC directory**, such as agenda activities and exercises, among others.

[136] Argentina et al., *Joint Working Paper on Confidence-Building Measures and Capacity Building*, 23 April 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Working_Paper_CBMs_&_Capacity_Building.pdf

Unresolved nuances: Defining PoC nature and directory function

As discussed in July 2023[137]

An unsolved issue was the nature of PoCs which will be nominated for the directory. **India** noted that states should remain flexible on having multiple technical or operational PoCs. India suggested the integration of the PoC Directory Module with the Global Cyber Security Cooperation Portal – a mechanism proposed earlier by the Indian delegation. Ghana recommended that this nomination be made at a technical, policy, and diplomatic level due to the differences in capacities.

Regarding the function of the directory itself, **Russia** expressed the view that the global intergovernmental PoCs directory should become the 'centrepiece in organising interaction of countries in response to computer attacks/incidents'. In this regard, Russia considered it inappropriate to limit cooperation between PoCs to incidents with possible implications for international peace and security. Instead, the interaction between PoCs should be built on an ongoing basis, regardless of the significance of a computer incident. On the other hand, **Switzerland** noted that the PoCs network will complement the work of CERTs and CSIRTs in cases of ICT incidents with possible implications for international peace and security.

Operationalising the Global PoC Directory: Regional organisations' role and expanding CBMs

As discussed in December 2023[138]

Many states supported the operationalisation of the agreements to establish a global PoC Directory. **Australia** stressed that those states already positioned to nominate their diplomatic and technical PoCs should do so promptly. **Switzerland**, however, reiterated that the PoC Directory should not duplicate the work of CERT and CSIRT teams. **The Netherlands** stressed the need to regularly evaluate the performance of the PoC Directory once it is established. **Ghana** supported this proposal to develop a feedback mechanism to collect input from states on the Directory's functionality and user experience. At the end of this agenda item, the Chair also addressed the participation of stakeholders and shared that a dedicated intersessional meeting in May will be convened to discuss stakeholders' role in the PoC directory.

Some delegations (e.g. the USA, the EU, Singapore, etc.) ***highlighted the role of regional organisations in operationalising the PoC directory and CBMs. However, several delegations expressed their concerns*** – e.g. **Cuba** and **the EU** noted that not all states are members of regional organisations. **The EU** added that the UN should develop global recommendation service practices on cyber CBMs and encourage regional dialogue and exchanges.

Delegations discussed potentially adding additional CBMs. **Iran** highlighted the need for universal terminology in ICT security to reduce the risk of misunderstanding between states.

---

[137] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's fifth substantive session'.
[138] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Stadnik, 'OEWG's sixth substantive session.'

India reiterated the proposal for a global cybersecurity cooperation portal to address cooperation channels for incident response. India also called for differentiating between cyberterrorism and other cyber incidents in this context. India also suggested that the OEWG may focus on building mechanisms for states to cooperate in investigating cyber crimes and sharing digital forensic evidence. **The Chair**, at the end of this agenda item, ***highlighted that the OEWG must continue discussions on potentially adding new CBMs and the importance of identifying if there are any additional things to do.***

PoC Directory launched: Focus turns to operationalisation

As discussed in March 2023[139]

The official launch of the Points of Contact (PoC) directory was scheduled for 9 May 2024, which ***led to the discussion revolving around the operationalisation of the PoC directory.*** At the time of the session, 25 countries had appointed their PoCs. Most delegations reiterated their support for the directory and either confirmed their appointments or that the process was ongoing.

Some states nevertheless suggested adjustments to the PoC directory. **Ghana**, **Canada**, and **Colombia** commented that communication protocols may be helpful, while **Czechia** and **Switzerland** recommended that the PoC shouldn't be overburdened with these procedures yet. Argentina also brought up the potential participation of non-state actors in the PoC directory.

To further facilitate communication, ***several states advanced the usefulness of building a common terminology*** (**Kazakhstan**, **Mauritius**, **Iran**, **Pakistan**), while **Brazil** mentioned that Mercosur was effectively working on this kind of taxonomy.

While **Czechia**, **Switzerland** and **Japan** ***underlined the necessity to focus first on the implementation and consolidation of existing CBMs***, ***many states nevertheless were in favour of additional CBMs:***

- On the protection of critical infrastructure (**Switzerland**, **Colombia**, **Malaysia**, **Pakistan**, **Fiji**, *the* **Netherlands**, **Singapore**, and **Czechia**)
- On coordinated vulnerability disclosure (**Singapore**, **Netherlands**, **Switzerland**, **Mauritius**, **Colombia**, **Malaysia**, and **Czechia**)
- On public-private partnerships as a CBM (**Kazakhstan, Qatar, Switzerland, South Africa, Mauritius, Colombia, Malaysia, Pakistan, South Korea, Netherlands,** and **Singapore**)
- On capacity building (**Argentina, Iran, Pakistan, Djibouti, Botswana, Fiji, Chile, Thailand, Ethiopia, Mauritius, and Colombia**)

All states recalled and praised the significance of regional and subregional cooperation in the implementation of CBMs and how it can contribute to the development of CBMs globally. In that respect, most states highlighted enriching initiatives at a

[139] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's seventh substantive session.'

cross-regional level**,** such as a recent side event at the German House. Work within the OAS, the OSCE, the ASEAN, the Pacific region, and the African Union was underlined. Interventions were enriched explicitly by sharing national experiences, most notably **Kazakhstan's and France's** most recent use of the OSCE community portal for PoC.

Contrasting priorities: Operationalising the PoC Directory vs proposing new CBMs

As discussed in July 2024[140]

In July 2023, states met at the eighth substantive session to adopt the group's third APR.[141] ***The launch of the Global PoC Directory and its online portal in May 2024 marked the concretisation of CBMs and a key achievement for the OEWG process.***[142] Only a few countries have not appointed their national PoCs at this point in time. Most countries have again reiterated their support for this flagship achievement of the OEWG, especially in light of the future permanent mechanism, which should be established after the end of the OEWG mandate in July 2025.

This session's discussion of CBMs mainly focused on an old dispute: the step-by-step approach to the operationalisation of the PoC directory vs its potential overburdening. The Netherlands, the EU, Australia, Germany, Switzerland and Canada argued that the focus should be on the existing CBMs and directly operationalising the PoC. **Ghana** underlined the need to elaborate clear guidelines concerning the circumstances under which member states could and should reach out to their counterparts through the PoC. **Fiji** and **the UK** further argued that lessons about the PoC Directory should be learned before developing it further.

The elaboration of standardised templates for communication through the PoC, aimed at enhancing transparency and understanding between states, ***was supported by*** **Czechia**, **New Zealand**, **Indonesia**, and **Ghana**. **The EU**, **Germany**, and **South Korea** ***argued that the development of such templates may hinder practical progress and overload the PoC directory system***, while others underlined that ***such a discussion is a lengthy process and that more time is needed*** (**the Netherlands**, **Canada**, **Czechia**, and **Malaysia**). Regional organisations and their experiences remained an important reference in that regard.

The outcome: The development of a standardised template was included in the third APR as one of the recommended steps. The UN Secretariat was requested to present an example of such a template by April 2025.

The sharing of technical ICT terms and terminologies

Support for the national sharing of technical ICT terms and terminologies as a recommended next step was given by **Mauritius** and **Congo**. ***Others had opposing***

---

[140] Gavrilovic, Kazakova, Petit-Siemens, Roellinger, 'OEWG's eight substantive session.'
[141] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR).*
[142] Digital Watch Observatory, *The significance of the OEWG POC directory*, Digital Watch newsletter – Issue 90 – June 2024, https://dig.watch/newsletters/dw-monthly/digital-watch-newsletter-issue-90-june-2024#PoC

views. **South Korea** opposed a fixating discussions on establishing unified terminology definitions, as these would also hinder the discussions of more practical CBMs. **The EU** held the same view, while **Germany** and **Canada** saw little or unclear value in sharing national views on terminology.

The outcome: The sharing of national technical ICT terms and terminologies, already appearing in the second APR, was eventually kept as such in the third APR.

From commitment to practice: Implementing CBMs and operationalising the PoC Directory

As discussed in December 2024[143]

This session was marked by noticeable activity in the CBM domain – from both developed and developing states – with the organisation of substantial side events and dedicated conferences as well as cross-regional meetings throughout the year. The letter sent by the chair in mid-November channelled pragmatic discussions and the session was marked by numerous practical recommendations pertaining to CBM implementation, the sharing of best practices and the operationalisation of the PoC directory.[144]

A new dynamic concerning CBMs emerged. It was then expected that the further implementation of CBMs will rely on capillarity. First, from the general CBM implementation point of view, capillarity was expected through the sustained commitment from states to share best practices in a cross-regional way, as shown in the inter-regional conference on cybersecurity organized by the **Republic of Korea** and **North Macedonia**, bringing together the OSCE, OAS, ECOWAS and African Union. Second, new levels of participation in the PoC directory have been specifically linked to such initiatives and to more general capacity-building to which states are highly recommended to contribute.

CBMs implementation and sharing of best practices

Whereas the guiding questions provided by the chair were oriented towards the implementation of existing CBMs, ***few new CBMs and measures were nevertheless proposed and not extensively picked up nor discussed by most delegations***. The well-worn question of shared technical terminology was brought back to the table solely by **Paraguay**, and **Thailand** mentioned an additional measure about CERT-to-CERT cooperation. Finally, **Iran** proposed a 9th CBM considering the facilitation of access to the ICT security market with the view to mitigate potential risks in the supply chain. **El Salvador** and **Malaysia** recommended the inclusion of voluntary identification of critical infrastructure and critical information infrastructure to the CBM 7 current phrasing.

---

[143] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's ninth substantive session.'
[144] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 12 November 2024* (A/AC.292/2024/5), 12 November 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_12_November_2024.pdf

Focusing on CBMs implementation, **Switzerland** shared an OSCE practice called 'Adopt-a-CBM' in which individual or several states adopt a CBM and are committed to its implementation and recommended that CBMs 2, 5, 7 and 8 would be suitable for this approach.[145] Kazakhstan also advised something similar in focusing on specific CBMs and engaging with individual states to promote them. Indonesia and El Salvador displayed numerous ways to foster the implementation of CBMs, among which the importance of shared practices that could fuel guidelines as practical reference for member states.

A substantive engagement by various states was noted, especially about the sharing of specific practices pertaining to each CBM. Whereas most of these practices are usually confined to regional frameworks, it is noticeable that numerous states have densely exchanged best practices at an ever more global level through the application of ***CBM 6*** about the organisation of workshops, seminars and training programs with inclusive representation of states (**Germany, Korea, Peru, Fiji** and **the UK**) and **CBM 2** about the exchanging of views and dialogue from bilateral to cross-regional and multilateral levels (**Germany, Peru,** and **Moldova**). Consequently, some states also shared their application of **CBM 5** about the promotion of information exchange on cooperation and partnership between states to strengthen capacity-building (**Korea, Peru**). More specific best practice exchange on the protection of CI and CII (***CBM 7***) was also noted to be undertaken by several states **(Malaysia, Fiji,** and **the UK**). Finally, ***CBM 8*** on the strengthening of public-private sector partnership and cooperation was also fostered by several states (**Korea, Albania,** and **the UK**).

PoC directory operationalisation

At the time of the 9th substantive meeting, **111 countries had joined the PoC directory**. Most states sharing insights on ways to increase participation suggested raising awareness through workshops, webinars and side events (for instance, **Albania** and **Kazakhstan**). At this level of participation, it was reasonable to think that any increase in participating states should be considered a matter of capacity-building (**South Africa**).

Some states shared their experience with the use of the PoC and the feedback could not be more contrasted. On the one hand, **Russia** stated that it already had problems when cooperating on incident response through the PoC directory given that some contacts did not work and some technical PoCs had too limited powers which left them unable to respond to notifications. Consequently, it recommended that the determination of the scope of competence of each of the PoC should be the first priority task, only supported by **Slovakia**. On the other hand, **France** shared that it had received several demands of communications since the creation of the PoC and that it answered positively to all of them. **Russia** and **China** urged other states to actively use the PoC directory; **France** nevertheless advocated not to exploit and overuse the tool at the risk of making it inoperable.

Lines of division nevertheless sometimes fade and the one about the template question was definitely less stark than last session, considering that few states expressed their reluctance to build such a template (**Switzerland** and **Israel**). Contributions nevertheless ranged from general opinion about the format of the template to the very detail of its content. ***Most delegates advocated for flexible and voluntary***

[145] Organization for Security and Co-operation in Europe (OSCE), *10 Years of OSCE Cyber/ICT Security Confidence-Building Measures* (Vienna: OSCE Secretariat, October 2023), https://www.osce.org/files/f/documents/f/7/555999_1.pdf.

templates (**Indonesia, Malaysia, Singapore, Thailand, the Netherlands** and **Paraguay**). This framing was justified as enabling a better accommodation of different institutional frameworks as well as local and regional concerns (**Brazil, Thailand, the Netherlands,** and **Singapore**). ***All states nevertheless reasserted the necessity for the template to be as simple as possible*** for either capacity-building and resource constraints (**Kiribati** and **Russia**) or emergency reasons (**Brazil, Paraguay,** and **Thailand**). **South Africa**, supported by **Brazil**, proposed that the template should at a minimum provide a brief description of the nature of assistance sought, details of the cyber incident, acknowledgement of receipt by the requested state and provide indicative response timeframes. **Indonesia** added to this list the response actions taken, the requests for technical assistance or additional information and the emergency contacts options. Finally, **Kazakhstan** notably suggested numerous examples of templates each dedicated to various scenarios such as incident escalation, threat intelligence, CBM reporting, PoC verification, capacity-building, cross-border incident coordination, annual reporting and lessons learned. The Secretariat was still expected to produce such a template by April 2025 and the chair expressed its intention to have standardised templates as an outcome of the final report.

CBM dialogue in waiting? Anticipation builds around a permanent mechanism

As discussed in February 2025[146]

A more subdued CBMs discussion at this session seemed to suggest that states now anticipate the future permanent mechanism to serve as the forum for detailed CBMs discussions. **Kazakhstan** suggested that addressing subtopics, such as standardised incident response procedures, would be more effective within thematic groups engaged in detailed discussions rather than plenary sessions. Some states voiced a cross-cutting approach to discussing CBMs more efficiently in the permanent mechanism, such as **Germany** proposing to address CBM 3, 5 and 6 under the single umbrella of the resilience of critical infrastructures.

While the previous session had already seen a decline in the discussion of additional CBMs, only **Iran** ***circulated a working paper proposing a new CBM to ensure unhindered access to a secure ICT market for all***, aiming to foster global trust and confidence. No other state engaged with this proposal; **Germany** merely remarked that it might be more appropriately framed as a norm, given its reference to expectations or obligations.

The deliberations on standardised templates further exemplified the subdued nature of this session's CBM discussions. **South Africa**, with **Brazil**'s support, reiterated its proposal for a template encompassing a brief description of the assistance required, details of the cyber incident, acknowledgement of receipt by the requested state, and indicative response timeframes. **Thailand** emphasised the necessity for a flexible template, while **Korea** underscored that it should serve as a communication reference without imposing constraints on interactions. Finally, **Kazakhstan** reiterated its proposal to have specific templates for different scenarios, such as incident escalation, threat intelligence sharing and

[146] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's tenth substantive session.'

cyber capacity-building requests. The Secretariat is anticipated to produce such a standardised template by April 2025. In related matters, **Mauritius** proposed the development of secure communication platforms for exchanging information on cyber incidents.

This contrasts with the dynamic CBM landscape at the regional level, where numerous states shared their CBM implementations (the **United Kingdom**, **Albania**, **Korea**, **Canada**, **Ethiopia**, **North Macedonia**, **Kenya**, and the **OSCE**) often linked to regional initiatives and best practices (**Tonga**, **Bosnia and Herzegovina**, **Thailand**, **Ghana**, **Brazil**, **Dominican Republic**, **Philippines**). This further illustrates states' eagerness to advance the operationalisation of CBMs.

The PoC: Finally ripe for the picking?

As of the 10th session, **116 states have joined the Points of Contact (PoC) Directory**—an increase of 5 since December 2024—registering nearly 300 diplomatic and technical PoCs. The Secretariat shared conclusions from the December ping test and provided a detailed overview of the then-upcoming scenario-based exercise scheduled for March 10–11 and March 17–18, 2025. **Russia** actively encouraged remaining member states to participate in the PoC Directory, promoting its guidelines on designating UN technical PoCs and supporting a UNIDIR seminar aimed at achieving universal participation in the directory.

While most states remained silent regarding the ping test outcomes and their experiences with the PoC Directory, three nations expressed dissatisfaction. **Russia** reiterated concerns about the inactivity of certain PoCs and the insufficient authority of some technical PoCs, which hampers their ability to respond to Russian notifications—echoing points raised during the 9th session's CBM discussions. **Germany** and **France** jointly addressed issues with a specific state's use of the PoC Directory, noting that their technical PoCs received notifications about malicious cyber activities linked to IP addresses in their respective countries. They recommended redirecting these requests to appropriate national authorities; however, identical requests continued to be sent to their technical PoCs. This behaviour, they argued, contradicts the principle that the PoC Directory should complement existing CERT-to-CERT channels designed for such requests.

Without directly referencing these situations, **China** observed that, ***given the voluntary nature of the PoC Directory, member states are free to determine the functions of their PoCs, as well as the types and channels of messages they handle. This scenario highlights a broader lack of common understanding regarding the PoC Directory's intended use.*** **Mauritius** emphasised the need to define clear thresholds for reportable incidents, while **Cuba** stressed the importance of detailing circumstances under which information exchange should occur. On a side note, **the EU** proposed that the private sector could participate in the PoC directory.

Towards a more integrated approach: CBMs and capacity-building

Most states reaffirmed that capacity-building is a prerequisite to CBM implementation (**Kazakhstan**, **Tonga**, **Russia**, **Thailand**, **Malawi**, **Laos**, **Ghana**). **Cuba** and **India** voiced their interest in gathering the PoC Directory in the global portal for capacity-building as a central access point and a core knowledge hub for resources. **Pakistan** argued that the PoC Directory goes beyond crisis management but is a foundation for broader collaboration, including capacity-building.

Muted exchanges: A quieter round of deliberations in the last session

As discussed in July 2025[147]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[148] While CBMs have been one of the main areas of progress in recent years within the OEWG process, the discussions during the last substantive session were notably subdued.

New CBMs: Overcommitting or not?

A few new proposals were tabled. Indeed, a clear and long-standing had emerged among several delegations, including **the EU, Canada, the Netherlands, Ukraine, New Zealand, Australia,** and **the USA**, that ***the OEWG's final report should avoid overcommitting to new CBMs.***

This position was the principal counterpoint to **Iran's *longstanding proposal for a new CBM aimed at ensuring unhindered access to a secure ICT market for all states***. Although this proposal did not gain significant traction in earlier discussions, ***it became a central point of contention during the latest round of negotiations***. States such as **Brazil** and **El Salvado**r expressed support for retaining this reference, but others—including the **Netherlands, the USA, New Zealand, Australia,** and **Switzerland**—***firmly rejected its inclusion***, citing both the absence of consensus and the need to prioritise the implementation of the eight CBMs agreed under the OEWG framework. **Switzerland *proposed relocating this reference to the capacity-building section, where states could voluntarily provide others with ICT tools to strengthen capacity.***

The standardised template for communication: First time discussed in the plenary

First circulated in April 2025, the standardised template developed by the Secretariat had not yet been discussed in plenary. Some delegations—notably **Qatar** and the **Republic of Korea**—expressed their preference to keep the template flexible and voluntary. **Thailand** proposed enhancing the template by incorporating elements such as urgency and confidentiality to help states identify operational needs in sensitive contexts. Nevertheless, the proposal received a lukewarm reception from **the EU** and **the Netherlands**, with the latter calling for its removal from the final report.

Responsible reporting of ICT vulnerabilities, norm J)

A final point of contention concerned the inclusion of norm J), which pertains to the responsible reporting of ICT vulnerabilities, under the CBM section of the final report. While **El Salvador *supported its inclusion***, **the Netherlands**, **the EU**, and **Israel *strongly opposed it***. **The Netherlands** questioned the logic of singling out this particular norm over others, while **Israel** argued that this issue had not been substantively deliberated and therefore should not appear under the CBM heading.

The outcomes: While Iran's proposal did not make it onto the formal list of CBMs, it remains referenced in the final report for potential consideration within the future

---

[147] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Radunovic, Roellinger, 'UN OEWG concludes.'
[148] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

permanent mechanism. Although it was initially the Chair's ambition to include the standardised template of communication, it ultimately was not retained. Norm J) was not included in the CBMs section.

Capacity building

Strengthening capacity: Capacity building principles, experiences, and the role of UN processes

As discussed in December 2021[149]

Many countries reiterated the basic principles of capacity-building, agreed upon by the previous OEWG and outlined in paragraph 56 of its 2021 report. In addition, **Singapore** and **Thailand** stressed the demand-driven approach, focused rather on outcomes than on outputs. **Brazil** and the **Czech Republic** reminded that capacity-building is a two-way street. **Switzerland** underlined that capacity-building should be considered a holistic effort. **Iran** suggested that non-discriminatory access to ICT security-related science, technology, and products and services should be included as a principle. **China** connected to this by calling for the basic internet resources to be distributed fairly, while ensuring that relevant international internet governance processes are inclusive and on equal footing.

A number of states emphasised the importance of a multistakeholder approach and public-private partnerships to capacity-building – notably **Australia**, **Chile**, **India**, **Indonesia**, **Korea**, **Switzerland**, **Thailand**. **Russia** ***called for establishing an exchange of best practices and experience in building public-private partnerships in the area of using ICT at the national level***, and argued that it is important to develop mutually acceptable ways of providing assistance and cooperation between states and private entities – at the request of each recipient state, and taking into account the state's specific needs and characteristics.

Capacity-building efforts on national and regional levels

A number of states shared examples of capacity-building efforts on national and regional levels. For instance, the Dominican Republic worked with Germany, Estonia, and Luxembourg to utilise the EU's CyberNet project knowledge and establish a cyber training centre for public and private sector and law enforcement authorities for Latin America and the Caribbean. The Philippines partnered with Australia and Israel on particular national activities, and participated in regional training with the support of Japan. Korea and the Netherlands organised a webinar for the exchange of national views among 14 Asian countries.

Japan stated its intent to conduct activities in the Indo-Pacific region, involving industry, governments, and academia. **The Lao PDR** benefited from the national and regional training and workshops organised by ICT for Peace, an NGO. **Thailand** recognised Japan's support in building a regional centre in Bangkok to strengthen regional capacity-building. **Singapore** had been conducting programs throughout ASEAN and partnering with the industry, academic institutions, and the Global Forum on Cyber Expertise (GFCE). The **Indian** CERT had undertaken joint training and workshops to train government officials. **Greece**, hosting the EU's Network Information Security Agency (ENISA), announced support programmes for

[149] Digital Watch Observatory. *UN OEWG 2021–2025 – Capacity-building*, 16 December 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/capacity-building.

the Western Balkans and offered further assistance to various regions. The International Security in Cyberspace Fellowship by Canada was praised by several participants, as being instrumental in bringing more women on board, the first substantive session of the OEWG included.

Several countries warned about certain challenges which impact capacity-building. **Cuba** underlined that it is vital for states to refrain from adopting any unilateral, coercive measure which restricts universal access. **Syria** also warned that unilateral coercive sanctions are impeding capacity-building in developing countries. **Iran** followed in the same vein, outlining the restrictive measures against other states as the problem, including unilateral digital sanctions that have been intensifying against some countries.

Speaking about the priorities of capacity-building, **the EU**, **together with Republic of North Macedonia**, **Montenegro**, **Albania**, **Bosnia and Herzegovina**, **Ukraine**, **Republic of Moldova**, **and Georgia**, stressed that capacity-building is fundamental for implementing the framework of responsible behaviour, through developing and implementing national strategies, establishing CERTs, setting up crisis management structures, and enhancing capacities to tackle cybercrime. **Indonesia** emphasised capacity-building as important for the implementation of international law and voluntary cyber norms, but also reminded of the need to ensure the physical infrastructure of ICT. **India** outlined the necessary focus on crisis management, while **Brazil** and **the Czech Republic** added the resilience of critical infrastructure. **The UK** saw the development of national strategies as an urgent step which would allow international cooperation, underlining the importance of the models that assess cybersecurity status in countries and help them understand their needs, such as their Cybersecurity Capacity Maturity Model for Nations (CMM).[150] **Columbia** invited for actions which close the digital divide, focus on training of trainers, and involve more women in the process. **Iran** suggested that non-discriminatory access to ICT security-related science, technology, and products and services should be prioritised for early action by the OEWG.

What role for the OEWG?

The majority of countries that took the floor also brought forward certain concrete proposals. **The Philippines** suggested that the OEWG assign facilitators for consultations with members for sharing best practices for each priority area, which would then, periodically, report the outcome of such informal consultations to the chair. **South Africa** called for the OEWG to discuss appropriate institutional arrangements and special programmes for capacity-building. **Russia** invited states to continue negotiating universal principles for providing capacity-building assistance and discussing optimal ways to create a targeted program or fund for capacity-building, which could involve other stakeholders. **Malaysia** suggested that the OEWG should map out and develop a baseline or a framework for capacity-building.

The Czech Republic called for dedicated OEWG thematic sessions in the following years as an opportunity to exchange best practices. It also invited the OEWG to recommend mainstreaming of cybersecurity into the UN digital development agenda across the UN system, to tap into development funds and ensure safe digital transformation. **India** called for the OEWG work to comprise of practical cooperation initiatives and regular activities between member states, and suggested: training of cybersecurity professionals through

[150] Global Cyber Security Capacity Centre (GCSCC), 'The Cybersecurity Capacity Maturity Model for Nations (CMM),' accessed 1 August, 2025, https://gcscc.ox.ac.uk/the-cmm.

short and long term courses through collaboration with reputable international institutions, the establishment of centres of excellence in different countries, and setting up infrastructure for testing of the ICT products and systems in order for a comprehensive understanding of the security challenge to be developed.

Indonesia called for a drawing of a framework for assessing the impact of capacity-building, and the OEWG to play a role in creating an inventory of lessons learned related to the execution of capacity-building. Similarly, **Singapore** suggested a framework for assessment of needs that guides capacity building, and the establishment of the metrics and measures for success. Several states, including **the UK** and **France**, underlined the relevance of the self-evaluation Survey of National Implementation, proposed by **Mexico** and **Australia** in the previous OEWG, for mapping capacity-building needs and progress.[151]

Singapore also called for the establishment of a UN cyber fellowship program for small states that would support the training in cyber issues for mid-to senior-level officials from smaller developing countries. It offered that this fellowship programme be organised under the auspices of the existing UN-Singapore cyber program, and focus on cyber and digital security governance, including best practices. **The Netherlands** called the OEWG to adopt a gender sensitive approach to capacity-building, to mainstream the gender and the position of women and girls. **The Lao PDR** supported enhancing women's participation, such as through a cyber fellowship programme. **Columbia** emphasised the inclusion of marginalised groups, particularly women, girls, older people, people with disabilities, and indigenous communities, in the ICT discussions. **Brazil** saw the OEWG as a platform for regional dialogue and the establishment of capacity-building coordination mechanisms with the involvement of other stakeholders, to help match the needs and available resources.

The UN role and avoiding duplication

Columbia considered that the UN should maintain a repository of capacity-building initiatives. **The Lao PDR** reminded of the important role of UNODC with capacity-building, and suggested that the UNIDIR Cyber Policy Portal could also serve for collecting needs and actions in support of capacity-building. **Cuba** argued that the UN, and particularly the ITU, should assume a central role as a standing forum for dialogue and capacity-building, while regional and other efforts should only complement multilateral ones.

The Netherlands confirmed the merits of the UN's role as coordinator in the area of capacity-building, as long as it reinforces and supports the work of regional organisations and other existing multistakeholder endeavours, like the GFCE. **Switzerland** warned about possible duplication of efforts – for instance, the UN efforts to create a database overlaped with GFCE work, which already bridged demand with offer, such as through the GFCE-AU programme, and invited for the improvement of coordination of international partnerships among states and stakeholders, providers, as well as recipients of capacities. **The UK** also suggested promoting the existing routes by which states can access support, including funding, such as the GFCE.

The role of POA in capacity building

[151] Australia et al., *Joint Proposal for a National Survey of Implementation of UNGA Resolution 70/237*, 16 April, 2020, https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf.

Several countries reflected on the role that the Programme of Action (PoA), proposed by **France**, **Egypt**, and over 50 other countries, could play in capacity-building.

The Netherlands stressed that the GGE and OEWG consensus reports are ready to be implemented, and that the PoA could contribute to this through capacity-building. **Switzerland** reminded that the PoA was mentioned in the OEWG 2021 report as important for building capacities of states to implement the framework, and compared the PoA, as a place for implementation, against the OEWG as the place for negotiations. **Korea** presented that PoA would establish a permanent, open, and inclusive instrument focused on capacity building. **Japan** added that PoA is seen as an action-oriented form of institutional dialogue that would also deal with capacity-building, regularly share actual efforts, and provide periodical reviews.

The EU and several aligned states suggested that the PoA can advance cooperation on national, regional and global levels, and foster meaningful multistakeholder initiatives. The PoA could also explore dedicated funding mechanisms and enhance coordination between existing instruments such as the World Bank, in line with principles as set out in paragraph 56 of the OEWG 2021 report. **France** added that the PoA should have the necessary financial and human resources, including a dedicated secretariat, for seeking new financing for capacity-building. **Egypt** suggested that the PoA could also discuss establishing a UN fellowship program – possibly following the model of the PoA on small arms and light weapons, which provides specialised courses and training for cyber experts on the technical and political levels.

Capacity building landscape: Principles and key international organisations

As discussed in March 2022[152]

The principles of capacity building, and matching needs with solutions

Malawi stressed that 'being one of the developing countries, we recognise that we also have a significant role to play in identifying our needs'. There was a general consensus among states that, in order for capacity-building initiatives to have the greatest possible impact, capacity-building efforts must be nationally-owned, sustainable, non-discriminatory and politically neutral, and guided by the principles contained in paragraph 56 of the final substantive report of the 2019–2021 OEWG. **Brazil**, **Malawi, Fiji and Pacific Islands Forum countries, and South Africa** further emphasised the importance of political neutrality. **Nicaragua, Cuba, Venezuela, Indonesia, and Syria** strongly reject the imposition of any unilateral coercive measures that could undermine the development plans. In addition, **Bangladesh, Iran, and Sri Lanka** stressed the principle of sovereignty. **Portugal** underlined that cybersecurity capacity building must be complemented by a proportional effort to combat crime.

[152] Digital Watch Observatory, *UN OEWG 2021–2025 – Capacity building*, 31 March, 2022, https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-capacity-building.

Addressing the question of the universal principle of capacity building, **the Russian Federation** stressed that the list of principles should include:

1. The inadmissibility of using ICT by states as a tool for taking economic, political, or other coercive measures, including measures of a restrictive or blocking nature against particular states, which hamper universal access to the benefits from the use of ICT
2. The requirement for states to prevent the use of harmful hidden functions in ICT supply chains developed under their control and jurisdiction to create or facilitate the creation of vulnerabilities in products, goods, and services that prejudice the sovereignty and security of recipient states
3. The inadmissibility of taking measures that entail unreasonable restrictions on the use of ICTs for peaceful purposes, international cooperation in this area, or the transfer of technology

Singapore highlighted that capacity building would enable countries to contribute meaningfully to international cyber discussions. In light of this, the establishment of the UN Singapore Cyber Fellowship Program, which should target senior-level officials, particularly those from developing countries holding decision-making responsibilities in the areas of social security and cyber governance, was mentioned. **Fiji, Brazil, Iran, South Africa, Malaysia,** and **Egypt** expressed their support by saying that these initiatives constitute a good basis for a more focused discussion in the next session.

A number of developing countries expressed the necessity to enhance financial support. **Iran, Nicaragua, Cuba,** and **Pakistan** proposed to establish a mechanism for financial assistance to developing countries, especially in projects which promote safe and peaceful use of the ICTs, as well as through the promotion of scholarships, workshops, seminars, and other initiatives for the exchange of experience.

Providing technical assistance to developing countries was highlighted by **Sri Lanka**, **Nicaragua, Lao PDR, Cuba, Venezuela, Côte d'Ivoire, Ghana, and Pakistan**. **Ghana** suggested that it should be anchored in the normative framework, in order to ensure that there are clear guidelines through which it can be carried out. In addition, **Colombia** suggested to carry out technical studies like 'gaps research', in order to allow us to understand the needs of a country, in order to present and offer adapted assistance. **Pakistan** proposed that developing states should be provided with necessary financial and technical support, and resources required for the establishment of the CSIRT, securing critical infrastructure and training for crisis management. In light of this, **India** suggested developing an 'international counter task force' by involving experts from the member states to provide technical assistance to developing countries in cases of cyberattacks targeting their critical infrastructure. Such a task force could also provide support in guiding these countries with necessary infrastructure to protect their assets against cyberattacks. **Germany** would welcome further elaboration of the task force development.

Development of specific capacity-building programs

Developing countries put forward a number of capacity-building programs. **Cuba** proposed the creation of a scholarship program to train experts in developing countries on all aspects of cybersecurity, while taking into consideration current debates within the UN. Additionally,

Pakistan suggested diverse fellowships and training for cybersecurity professionals from developing states in the areas of critical infrastructure security, cyber policy making, and the application of international law. **Kenya** advocated for the development of exchange programs, including south to south triangular cooperation through which states can learn from each other's experience. Furthermore, centres of cyber excellence could reinforce capacity-building efforts.

The Cybersecurity Capacity Maturity Model (CMM)

Both developed and developing countries expressed support for the Cybersecurity Capacity Maturity Model (CMM), developed by the Oxford Centre, which would allow developing countries to better set priorities for capacity development.[153] A number of concrete proposals for capacity building were put forward by delegations. **The UK** proposed the Oxford Centre Cybersecurity Capacity Maturity model, CMM, co-sponsored by Australia, Botswana, Chile,Colombia, the Dominican Republic, Fiji, Georgia, Germany, Iceland, Japan, Malawi, Mauritius, the Netherlands, Norway, Peru, Switzerland, Tanzania, Uganda, the United Kingdom, and Global Cyber Security Capacity Centre (GCSCC), the Cybersecurity Capacity Centre for Southern Africa, the Commonwealth Telecommunications Organization, the OAS, and the GFCE, to review cybersecurity capacity maturity; CMM would enable nations to self-assess, benchmark and better plan investments and national cybersecurity strategies, as well as set priorities for capacity development.

The UK called on the OEWG to promote the routes by which states can access support including funding to conduct the CMM and invited UNIDR to track global progress and assess states priority needs, perhaps through voluntary reporting using the survey of national implementation. **Malawi,** the country that has conducted the CMM, attested that its first assessment provided a baseline of where the country stood when it came to cybersecurity, and helped formulate a strategy that targeted its needs. **Fiji, Colombia, Malaysia, the Philippines** supported the UK's intervention, and underscored the importance of the assessment of capacities of each state.

The role of the OEWG in capacity building

According to a number of member states, most notably **Lao PDR, Nicaragua, Malawi, Iraq, Indonesia on behalf of Non-Aligned Movement, Philippines, France, the Russian Federation, Republic of Korea, Finland, India, and Poland, *the OEWG can significantly promote capacity building at a global level*,** while regional bodies and other organisations continue to play a vital role. In order to enhance capacity building at the global level, **the EU on behalf of the Turkey, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Ukraine, the Republic of Moldova, Georgia, and San Marino** underlined the need to increase our international coordination using organisations such as the GFCE to bring states together, facilitate the exchange of information on ongoing and planned efforts, best practices and lessons learned. **Malawi**, **Côte d'Ivoire** and **Ghana** expressed the necessity to encourage the **sharing of information** and to establish a **platform and a database that states can use to identify the available capacity-building opportunities** and programs. In a similar vein, **Singapore, India, and Kenya** invited the UN to compile a comprehensive calendar of capacity-building programs that would allow us to have greater

[153] GCSCC, 'The Cybersecurity Capacity Maturity Model for Nations (CMM).'

visibility of existing needs or gaps to better tailor our programs and focus our resources. **Cuba** proposed to develop a database of best practices and techniques available.

Malaysia suggested that the OEWG could facilitate the states' effort by aligning capacity-building requirements and assistance based on the cybersecurity baselines once these are developed. **Germany** echoed the remarks made by **Finland** and **Costa Rica** on the importance of the OEWG to closely involve the private sector actors at the conceptual and practical level in preparing its recommendations with respect to capacity building. Other member states, most notably **Sri Lanka, Nicaragua, Germany, Japan, Colombia, Côte d'Ivoire, Venezuela, Indonesia, Bangladesh, El Salvador, Haiti, Republic of Korea, Finland, Dominican Republic, Costa Rica, India, the EU, Poland,** and **Kenya** also emphasised the role of **public-private partnerships in facilitating knowledge and skill transfer and in overall capacity building efforts.** According to **Chile**, the OEWG, through the UN system, could contribute to developing a global map for capacity-building opportunities, while working with regional and other bodies and acting on focal points through a specialised unit in the area, responsible for coordinating these capacity-building opportunities. **Iran** suggested that the OEWG should focus on the components of the global architecture for capacity building, including cybersecurity training and education under the auspices of the UN. **The Philippines** maintains that the OEWG can address significant concerns, such as insufficient coordination and complementarity in the identification and delivery of capacity-building efforts. **El Salvador** believes that the OEWG could, within its report, highlight the current efforts generating progress in cyberspace and incentivise such initiatives through information exchange. **Haiti** highlighted the extreme importance of strengthening international cooperation to prevent and combat the use of the ICTs for criminal purposes and to establish the necessary follow-up mechanisms. **The Netherlands** supported the creation of a permanent platform, as suggested by Izumi Nakamitsu (High Representative for Disarmament Affairs), to enhance capacity building by complementing the OEWG work to further develop a common understanding and elaborate the consensus framework for responsible state behaviour in cyberspace. **France** suggested that such a platform could be part of the Programme of Action (PoA).

The role of PoA in capacity building

Many delegations – most notably **Germany, Finland, Dominican Republic, Republic of Korea, Chile, Japan, Colombia,** and **the Netherlands** pointed to the unique role of Programme of Action (PoA) in operationalisation of the principles to conduct capacity-building activities set in paragraph 56 in the final report of the OEWG 2019-2021.

Egypt explained that the PoA could play a crucial role in the capacity-building efforts as well, allowing a bottom-up mechanism to support implementation efforts at the national level, particularly through a tailored and coordinated fashion, while fully respecting state sovereignty.

In addition, **France** explained how the PoA would materialise in practice – e.g. PoA could encourage the development of capacity-building efforts to assist states in the establishment of a national cybersecurity strategy, to help them to build capacity on incident response or in outlining policies that would improve the protection of critical infrastructure.

Switzerland highlighted the uniquely universal role of the UN, where the PoA would facilitate capacity building at the global level – e.g. the PoA could support the development and

appropriate update of the UNIDIR survey of national implementation. It could also encourage the use of the survey to regularly assess states' needs and to identify further actions required for the development of capacity building. The PoA would also have a dedicated trust fund for capacity-building projects.

The role of the Global Forum on Cyber Expertise (GFCE) in capacity building

There were multiple calls to increase international coordination using existing organisations such as the Global Forum on Cyber Expertise (GFCE) . **Chile** maintained that the UN could evaluate these kinds of initiatives to move forward with viable cooperation, assistance, capacity-building plans and strategies. **The Netherlands** and **Portugal** highlighted the work of the GFCE, which helps match capacity-building needs with expertise and resources.

Singapore advised the OEWG to consult with UNIDIR, the member states, regional organisations and stakeholders in organisations, such as the GFCE to better identify synergies for a more collaborative and sustainable approach to cyber capacity building, e.g. the Cybil Portal of the GFCE has enabled participating member states to tap into the rich exchanges of cyber capacity-building initiatives. Similarly, **the Philippines** suggested that the OEWG can build on the work of the GFCE or look into replicating the GFCE working groups to organise sub-working groups which would focus on thematic priorities of capacity building, *inter alia*, the implementation and establishment of norms and of national strategies, the applicability of international law, incident response emergency management and protection of critical infrastructure, which would offer concrete deliverables. **Canada** and the **Dominican Republic** highlighted the work and significant progress of the GFCE since its establishment in increasing participation and providing all participants with the tools, knowledge, and expertise required to coordinate global efforts in cyber capacity building.

The role of UNIDIR in capacity building

Further consultations on a new 'mechanism' that would allow compiling lessons learned, and publishing comparative studies on different regional organisations that offer capacity building programmes in the form of a calendar, were to be expected. Such a mechanism would make it easier for countries to find suitable capacity-building initiatives. Given the fact that different countries have raised the role of UNIDIR and the potential of its Cyber Policy Portal, it seemed likely that UNIDIR would take this up and elaborate on some of these initiatives.[154]

UNIDIR has been brought up in the discussion in many instances. **Germany** reminded that it is an independent institute funded by UN member states on a voluntary basis and cannot work per se – the OEWG can suggest areas for further research or work to UNIDIR, which would require additional resources to be provided by the member states. **Japan** recommended that the UNIDIR portal could be used to post information concerning cyber-related events around the world. Furthermore, countries that provide capacity-building initiatives could provide a summary of their programs to be included in the APRs of the OEWG or on the UNIDIR's portal to share information related to capacity building. In addition, **Indonesia** proposed that UNIDIR could play a role in compiling lessons learnt on capacity building and ICT security. Furthermore, **the Philippines** suggested that UNIDIR can support a more coordinated role in capacity building by conducting a comparative analysis on different international and regional organisations that offer programs and assessment

[154] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.'

tools, cyber capacity building, while determining best practices and creating a list of recommendations for the OEWG's consideration on how the UN can improve the existing initiatives.

Gender

Several countries highlighted gender parity in cybersecurity discussions and capacity building as imperative. **Malawi, Sri Lanka,** and **Colombia** stressed that any capacity building efforts should consider gender issues. **Canada** and **Netherlands** stressed that the OEWG should further promote a gender sensitive approach to cyber capacity building. This also applies to the area of cyber diplomacy where we should seek to increase the representation of women in discussions.

Debating the future: Coordination of cyber capacity building

As discussed in July 2022[155]

In July 2022, states met at the third substantive session to adopt the group's first APR.[156]

The debate over the UN Secretariat's and OEWG's role in capacity building coordination

Thailand and **Singapore** requested that ***the UN Secretariat designate the ICT capacity-building focal point.*** **The EU**, **Canada**, and **New Zealand** did not support this, noting that it's ***better to use existing platforms and initiatives like the GFCE and regional efforts and ensure complementarity between them***. **Botswana**, **the USA**, and **Fiji**, on behalf of Pacific Island Forum, also ***noted the importance of the GFCE's work.***

Referring to the ***suggestions for the UN Secretariat to take a role in capacity-building coordination***, **Germany** stated that the ***OEWG, in capacity-building efforts, should build upon existing institutional structures and bring in the expertise of all stakeholders***, including the UN and other multilateral organisations, as well as the civil society actors such as the Global Forum of Cyber Expertise, when it comes to detailed coordination of activities. Germany considers the role of the OEWG in setting the framework for cyber capacity building and suggests elaborating on concrete proposals on how this can best be achieved during the upcoming sessions or the intersessional period. **The Netherlands** proposed to ***discuss the role of the UN Secretariat in the upcoming OEWG meetings***, while **Finland** ***stated that it does not see value in this way forward.***

The USA stated that, in capacity building, ***the OEWG should focus on articulating how capacity building can enable more states to implement and adhere to their commitments to the norms of responsible state behaviour.*** The USA was against including any capacity-building initiatives within the OEWG in the first APR that were not previously discussed by the states, and pointed out the existing capacity-building initiatives within the World Bank, ITU, and the GFCE.

---

[155] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.'
[156] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*.

Iran considered the OEWG as a negotiation process and not an implementation process. Therefore, ***the OEWG cannot take on capacity-building coordination***. Instead, Iran proposed that ***ITU take over the capacity-building coordination in the ICT as a permanent mechanism***. That should include not only the exchange of information and coordination, but also encouraging and facilitating non-discriminatory access of all states to ICT-related products, services, equipment, networks, science, and technology.

The outcome: The first APR acknowledges that the OEWG itself could be a platform to continue exchanging views and ideas on capacity-building efforts, including how best to leverage existing initiatives. The suggestions for the UN Secretariat, the GFCE, and the ITU to take over capacity-building coordination were not included in the first APR.

Connecting capacity building and development

Thailand and **Costa Rica** suggested ***integrating capacity-building efforts into the 2030 Sustainable Development Agenda to connect the OEWG to the SDGs.***

The ICC suggested ***the elaboration of cyber development goals (CDG)***, which would primarily be a common capacity-building tool at the national level and would depend on states' commitment to systematically track and report on implementation. This would bring clarity to what remains to be done to implement the existing cybersecurity framework in all states and allow the development of a targeted capacity.

The outcome: The first APR recognised that the OEWG can better integrate capacity-building efforts on security in the use of ICTs into the 2030 Sustainable Development Agenda.

Regional voices: Organisations share their initiatives

Regional organisations such as the African Union, the CSTO, the EU, the OSCE, the OAS, and the SCO shared their ongoing projects and programs in the CBMs and capacity building. Gafoor noticed that it was the first time for the OEWG to hear directly from regional organisations.

Governance and resources: Ongoing discussions on leadership and funding

As discussed in December 2022[157]

Capacity building must be needs-driven and adjusted to local contexts, states largely agreed. ***Regional approaches can ensure that the needs of the states will be taken into account***, as **Chile** and the Global Forum on Cyber Expertise (**GFCE**) highlighted. **Canada** stated that ***the GFCE should continue its coordination role in cyber capacity building, and that the OEWG could leverage GFCE in this role***.

The UK proposed ***better contact with digital development programmes to ensure alignment with capacity-building principles***.

[157] Gavrilovic, Ittelson, Petit-Siemens, Radunovic, Roellinger, Stadnik, 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs'.

France, Colombia, and the **Philippines** noted that ***the OEWG could support the mapping of capacity building needs using existing instruments and frameworks.***

France also highlighted that ***the PoA could strengthen capacity building initiatives***.

Raising the cyber capacities of developing countries was also discussed. Some countries, such as **Egypt, Iran** and **Indonesia,** stated ***the UN should facilitate resource allocation for capacity building programmes.*** **Iran** stated that ***a dedicated trust fund should be established to finance cybersecurity training and education, transfer of technology, technical assistance, and financial support***. This proposal was supported by **Pakistan** and **Nicaragua**. **Iran** proposed that ***ITU be considered for capacity building***.

To provide developing states with capacities that allow meaningful participation in cyber processes, ***creating a cyber fellowship programme under the UN and OEWG*** was proposed by **Egypt**. Supported by **Pakistan** and **Indonesia**, the proposed programme would be akin to the one presented by the Non-Aligned Movement (NAM) in the Programme of Action (PoA) on small arms and light weapons.

Leadership and funding: Ongoing debates in focus again

As discussed in March 2023[158]

States shared experiences about tailored programs for particular countries, such as the Cybersecurity Program of the OAS, ASEAN-Japan Cyber Security Policy Meeting, ASEAN-Singapore Cybersecurity Centre of Excellence, ASEAN Cyber Shield Project, Western Balkans Cyber Capacity ensured by EU CyberNet, the Gulf Cooperation Council, the ITU's regional and national cyber drills for capacity development, the UNDP program for cyber development, and of course, the GFCE.

The role of international organisations in capacity building

The **UK**, **Canada**, and the **USA** noted that ***the OEWG could advance a general understanding of what capabilities need to be built. Yet, capacity building would be in the PoA's remit.*** **The EU**, **UK**, **Chile**, **Albania**, **Czech Republic**, **Estonia**, and **Greece** highlighted that ***the PoA will be the primary future instrument to structure cybersecurity capacity building initiatives by coordinating donors' efforts and mapping the needs of recipient countries.***

Japan stated that the OEWG should focus on collaborating with existing regional and international capacity building efforts to **avoid duplications** rather than creating a new organisation under the UN to provide capacity building projects.

Iran reiterated the idea it brought up at the December session: ***ITU could be a permanent forum for dialogue, consultation, cooperation, and coordination among member states***, including developing technical capacities. **Cuba** supported this idea.

[158] Gavrilovic, Grottola, Ittelson, Kazakova, Petit-Siemens, Stadnik, 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session.'

Funding capacity building needs

As for the funding of capacity building needs, **the Dominican Republic** pointed to ***various existing international funding mechanisms that could be used for cyber capacity building***. Several states mentioned ***the World Bank Cyber Security Multi-donor Trust Fund***, launched in 2021, dedicated to providing knowledge, technical cooperation, and practical tools to support cyber and digital security capacity building. **Japan**, **Germany**, and **Estonia** had already contributed to that Fund. **Russia** suggested that ***the OEWG consider establishing a specific assistance fund for capacity building needs***.

Capacity building in developing countries

El Salvador, **Argentina**, and **Kenya** highlighted prioritising practical support for establishing capacity-building programs in developing countries to mitigate ICT risks and building capacity amongst states to effectively respond to cyber threats by increasing international cooperation both inter-regionally and within regions.

Greece highlighted the importance of needs-based partnerships for capacity building. **Algeria** stressed the need to consider the varying degrees of cybersecurity in different countries. **Nicaragua**, **Fiji,** and **Botswana** emphasised establishing a mechanism for technical and financial assistance to developing countries as a means of capacity building. **Ghana** proposed funding this mechanism through international development assistance and multilateral development banks. **Colombia** drew attention to a project proposed by UNIDIR on Unpacking Cyber Capacity-Building Needs, based on the 11 cyber norms to identify the areas in which developing countries require actions to develop.

The proposal for the GCSCP

States also discussed the **Indian** proposal on the Global Cyber Security Cooperation Portal (GCSCP) that would contain a document repository, a PoC directory, a mapping of the needs of states in capacity building, a calendar of conferences and workshops, and incident reporting.[159] However, **Singapore and the Netherlands** cautioned that it is important to look at the existing cooperation portals, like the UNIDIR cyber portal and the GFCE cyber portal. **India** explained that the proposed portal would combine other relevant sub-portals for a broader understanding of the latest developments in cyberspace, which also helps smaller delegations access multiple platforms and track different portals that otherwise consume time. **Croatia and the Netherlands** noted that proposals on repositories and portals could be explored in relation to their possible inclusion in PoA.

Existing mechanism: Creating synergies

As discussed in May 2023[160]

Calls to avoid the duplication of existing efforts are a staple in any UN discussion, and that includes the OEWG. The potential roles of UNIDIR and the Global Forum on Cyber

[159] India, Working Paper on Global Cyber Security Cooperation Portal, July 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_GCSCP.pdf.
[160] Gavrilovic, Kazakova, and Petit-Siemens, 'Informal OEWG consultations on capacity building.'

Expertise (GFCE) in sharing information and resources for cyber capacity building were consistently highlighted. What set this particular session apart from others was that ***countries went beyond merely urging against duplication. Instead, they proposed synergies between existing mechanisms, suggesting that these mechanisms could complement one another rather than being viewed as separate instruments.*** This departure from the usual approach signalled a shift towards seeking collaborative solutions and maximising the effectiveness of existing frameworks.

Japan, **the Philippines**, and **Iran** suggested ***instrumentalising initiatives already under the auspices of the UN*****. Japan** proposed using the UNIDIR cyber portal to share information on national and regional capacity-building initiatives. **The Philippines** and **Iran** suggested approaching existing initiatives under the UNODC and ITU in a collaborative manner, through knowledge sharing, tailored adaptation, and resource sharing. **Switzerland** noted that states should examine how the UNIDIR cyber policy portal and UNICEF are working together to create a new cyber capacity-building mechanism and how synergies with existing platforms like the GFCE cyber portal can be used.

Canada and **Chile** stressed the role of the GFCE for its active participation in formulating strategies for cooperation, assistance, and capacity building in all regions of the world.

However, ***some states feel existing mechanisms, instruments, and bodies are simply not enough***. For instance, **India** reiterated its proposal for developing a Global Cyber Security Cooperation Portal (GCSCP), a new coordination mechanism under the auspices of the UN.[161]

The role of regional organisations

Regional and sub-regional organisations were once again hailed as having an important role to play in providing and leading capacity-building programmes. **Chile** and **Colombia** noted that regional organisations should be acknowledged in the recommendation section of the second APR. **Singapore** proposed that the OEWG consider how to best utilise existing regional and international capacity-building programmes and compile a repository of best practices for programme design. **Singapore** proposed that the OEWG should organise an informal conference of capacity-building practitioners to exchange ideas and best practices.

A needs-based approach to capacity building

Many countries also underlined a needs-based approach to capacity building. This, of course, is one of the principles set forth in the first OEWG APR for developing capacity-building programmes.[162]

The **Netherlands** proposed a four-step cycle to identify and match needs with capacity-building resources.

The USA recommended briefings from expert organisations such as the International Committee of the Red Cross (ICRC) to identify countries' needs.

Bangladesh, **Singapore**, and **Syria** proposed training initiatives to address identified skill gaps in developing countries. **Syria** focused on developing countries gaining access to

[161] India, Working Paper on Global Cyber Security Cooperation Portal.

[162] Digital Watch Observatory, *OEWG 2021–2025 First Annual Progress Report (APR)*.

relevant technologies and technical assistance tools and equipment for detecting, responding to, and recovering from malign ICT activities.

Singapore suggested that capacity-building programmes should focus on five key dimensions: cyber policy, cyber operations, technical skills, international law in cyberspace, and diplomacy.

Bangladesh highlighted the rapid advancement of AI and emerging technologies and the need to address the skill gap by enhancing digital literacy, technical skills, and knowledge of AI and other emerging technologies.

The gender dimension of capacity building

During the discussion, ***integrating the gender dimension into capacity-building efforts emerged as a prominent topic across country interventions, a departure from previous sessions where it was seldom mentioned***. Several countries, including **Bangladesh**, **Japan**, **the Netherlands**, **the Philippines**, **Uruguay**, **South Africa**, **Switzerland**, **the UK**, **Ecuador**, and **Czechia**, emphasised the significance of incorporating a gender perspective into capacity-building initiatives. They stressed the importance of inclusivity, non-discrimination, and transparency in these cyber-capacity efforts.

However, despite the recognition of the gender dimension in ICT use and some countries' mention of their national efforts, ***there were limited concrete proposals on integrating gender into capacity-building mechanisms within the framework of the OEWG***.

PPS and the SDGs

Another topic many countries touched on was ***the importance of public-private partnerships with industry and civil society for greater capacity building.*** Many countries also advocated for ***integrating capacity building with the SDGs and the development agenda***.

Capacity building overview: Mapping existing programes, emphasising regional and gender dimensions

As discussed in July 2023[163]

In July 2023, states met at the fifth substantive session to adopt the group's second APR.[164] **Indonesia** proposed to connect ***the mapping of capacity building programmes*** to the implementation of the frameworks' recommendations. **The USA** strongly supported it, while some states (e.g. **Australia**, **Japan**, and **New Zealand**) raised concerns about resources in conducting such a mapping. **Hungary** shared the view that while mapping is needed to coordinate better the efforts of the growing number of donors and implementers, the UN could undoubtedly play a complementary role. Still, other stakeholders have their roles to play. **The USA** and **Japan**, in particular, called for the making of most of the existing capacity-building efforts undertaken by other international organisations, such as the ITU.

[163] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's fifth substantive session'.
[164] Digital Watch Observatory, *OEWG 2021–2025 Second Annual Progress Report (APR)*.

The outcome: The second APR recommended that the UN Secretariat is conduct a mapping exercise to survey the landscape of capacity-building programmes and initiatives.

The Netherlands said that the ***text of the APR is missing the sub-regional aspects and proposed that it be added to reflect efforts from the regional level***. **The EU** shared the same view and suggested that the UN could encourage and serve as a platform to enhance the implementation of the UN agreements and stipulate capacity building in this context, including cooperation with the multistakeholder community.

Egypt believed ***the APR should not refer to specific regional or sub-regional organisations***. **Australia** disagreed and ***stressed the importance of mentioning concrete organisations, such as the GFCE***.

The outcome: The second APR recognised that regional and sub-regional organizations could continue to play an important role in implementing the framework for responsible state behaviour. Regional, cross-regional and inter-organisational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. However, as not all states are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to its work.

Iran noted that their recommendation for creating a new capacity-building mechanism under the UN had been disregarded. Instead, ***the focus solely revolves around enhancing coordination among existing mechanisms, which Iran could not support.***

The outcome: The recommendation for creating a new capacity-building mechanism under the UN was not included in the second APR.

Some states (e.g. **Indonesia**, **Vietnam**, and **the Netherlands**) ***supported considering the gender perspective in capacity building***. In contrast, a group of like-minded states, such as **Russia**, **Cuba**, **China**, **Venezuela**, **Nicaragua**, **Iran** and others, ***had not supported adding the gender-related wording***. **Iran** and **Russia** wanted gender removed from the APR, and Iran specifically wanted paragraph 43 A, which relates to preparing a survey to identify countries' needs regarding gender equality in the field of ICT security, removed.

The outcome: The second APR acknowlegdes promoting gender-responsive capacity-building efforts, including through the integration of a gender perspective into national ICT and capacity building policies as well as the development of checklists or questionnaires to identify needs and gaps in this area.

Cyber capacity training: Foundational capacities and concrete actions undertaken

As discussed in December 2023[165]

Delegations emphasised ***the importance of cyber capacity in enabling countries to identify and address cyber threats while adhering to international law and norms for***

[165] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Stadnik, 'OEWG's sixth substantive session.'

responsible behaviour in cyberspace. Central to the dialogue was the pursuit of equity among nations in achieving cyber resilience, with a recurring emphasis on the 'leave no country behind' principle.

The core notion of foundational capacities was at the centre of the debates. The development of legal frameworks, dedicated agencies, and incident response mechanisms, especially Computer Emergency Response Teams (CERTs) and CERT cooperation, was highlighted. However, delegations also stressed the importance of national contexts and the lack of one-size-fits-all answers to foundational capacities. Instead, efforts should be tailored to individual countries' specific needs, legal landscape and infrastructure.

Other issues highlighted were ***the shortage of qualified cybersecurity personnel and the need to develop technical skills through sustainable and self-sufficient traineeship programs***, such as train-the-trainer initiatives. Notable among these initiatives was the Western Balkans Cyber Capacity Centre (WB3C), a long-term project fostering information exchange, good practices, and training courses developed by Slovenia and France together with Montenegro

Concrete actions emerged as a response to past calls from delegations. Two critical planned exercises, the mapping exercise and the Global Roundtable on CB, were commended. The mapping exercise scheduled for March 2024 aimed to survey global cybersecurity capacity-building initiatives comprehensively, enhancing operational awareness and coordination. The Global Roundtable, scheduled for May 2024, was lauded as a milestone in involving the UN, showcasing ongoing initiatives, creating partnerships, and facilitating a dynamic exchange of needs and solutions. These initiatives align with the broader themes of global cooperation, encompassing south-south, north-south, and triangular collaboration in science, technology, and innovation, emphasising needs-based approaches by matching initiatives with specific needs.

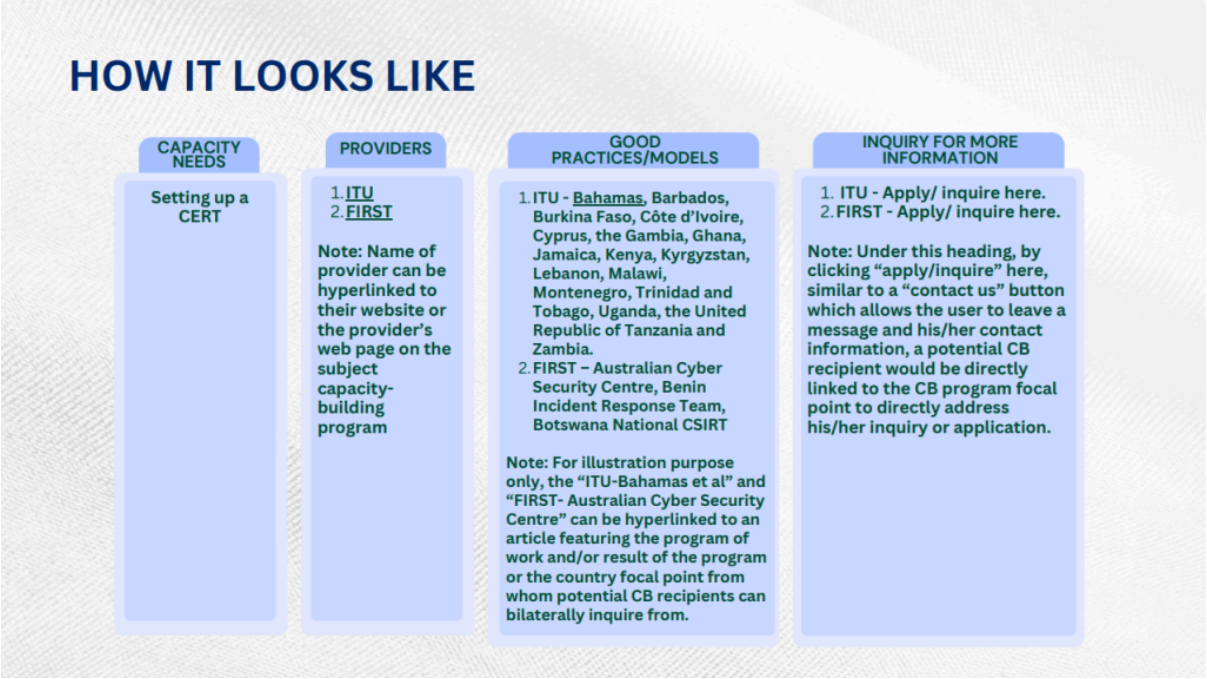
Additional points from the discussions included a presentation from **India** on the technical aspects of the Global Cyber Security Cooperation Portal, emphasising synergy with existing portals. Delegations also supported a voluntary checklist of mainstream cyber capacity-building principles proposed by **Singapore**. Furthermore, the outcomes of the Global Conference on Cyber Capacity Building, hosted by Ghana in November 2023 and jointly organised by the Cyber Peace Institute, the World Bank, and the World Economic Forum, garnered endorsement from many delegations. The 'Accra call,' is a practical action framework to strengthen cyber resilience as a vital enabler for sustainable development.[166] **Switzerland** announced its plan to host the follow-up conference in 2025 and urged all states to endorse the Accra Call for cyber-resilient development.

[166] Global Conference on Cyber Capacity Building (GC3B), The Accra Call for Cyber Resilient Development: An Action Framework, December 2023, https://gc3b.org/wp-content/uploads/2023/12/Accra-Call-Digital-Version_Final.pdf.

Scaling up: Bolstering efforts and funding

As discussed in March 2024[167]

Several noteworthy proposals were put forth by different countries, each aiming to bolster capacity building efforts. **The Philippines** introduced a comprehensive 'Needs-Based Capacity Building Catalogue,' designed to help member states identify their specific capacity needs, connect with relevant providers, and access application guidance for capacity building programmes.[168]



A scheme of the Philippine proposal. Source: UNODA.

Kuwait proposed an expansion of the Global Cybersecurity Cooperation Portal (GCSE), suggesting adding a module dedicated to housing both established and proposed norms, thus facilitating collaboration among member states and tracking the implementation progress of these norms.[169] **India**'s CERT expressed willingness to develop an awareness booklet on ICT and best practices with the contribution of other delegations, intending to post it on the proposed GCSE for widespread dissemination.

The crucial issue of funding for capacity building received substantial attention during the discussions, with multiple delegations bringing to the fore the need for additional resources to sustainably support such efforts. **Uganda** advocated establishing a

---

[167] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's seventh substantive session.'
[168] The Philippines, *Needs-Based Cyber Capacity-Building Catalog: A Philippine Proposal*, July 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_on_CB_Cyber_Catalog.pdf.
[169] Kuwait, *Module for Rules, Norms, and Principles within the Global ICT Security Cooperation and Capacity-Building Portal (GCSCP)*, 7 March, 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/KUWAIT_PROPOSAL%28%22%28GCSCP%29_Module_for_rules_norms_and_principle%29_-_final.pdf.

UN voluntary fund targeting countries and regions most in need. In contrast, others stressed the imperative of exploring structured avenues within the UN framework for resource mobilisation and allocation.

On the foundational capacities of cybersecurity, an emphasis was placed on developing ICT policies and national strategies, enhancing societal awareness, and establishing national cybersecurity agencies or CERTs.

Furthermore, ***the importance of self-assessment tools for improving states' participation in capacity building programmes was emphasised.*** **Pakistan** proposed implementing checklists and frameworks for evaluating cybersecurity readiness and identifying gaps. **Rwanda** advocated for reviews based on the cybersecurity capacity maturity model (CMM) to achieve varying levels of capacity maturity.[170] The discussions also commended existing initiatives, such as the Secretariat's mapping exercise and emphasised the need for a multistakeholder approach in capacity building efforts. Finally, **Germany** highlighted the significant contributions of organisations in creating gender-sensitive toolkits for cybersecurity programming, underscoring the importance of incorporating gender perspectives in implementing the UN framework on cybersecurity.

The Global Roundtable: Capacity building in the context of sustainable development

As discussed in May 2024[171]

The inaugural Global Roundtable on ICT Security Capacity Building, held under the auspices of the UN, brought together high-level representatives from various nations to address the critical need for cyber resilience in the context of sustainable development. The event provided a platform for sharing experiences and strategies to overcome the global capacity gap in ICT security.

A key issue identified during the roundtable was the widespread lack of cyber threat awareness, which poses a significant vulnerability across different sectors, including government and business.

The global shortage of skilled cybersecurity professionals was also highlighted as a major concern, necessitating the establishment of specialised training programs and centres of excellence, such as those in Singapore, to cultivate a new generation of experts.

The digital divide, particularly in rural and marginalised communities, was recognised as exacerbating cybersecurity vulnerabilities. ***The roundtable emphasised the need for concerted efforts to enhance technological access and digital literacy across all societal strata, promoting cyber hygiene as a fundamental aspect of building cyber resilience.***

International collaboration was identified as a crucial strategy for overcoming barriers to ICT security capacity building. Shared intelligence, best practices, and

[170] GCSCC, 'The Cybersecurity Capacity Maturity Model for Nations (CMM).'
[171] Digital Watch Observatory, *OEWG Roundtable on ICT Security Capacity Building*, 10 May 2024, https://dig.watch/event/global-roundtable-on-ict-security-capacity-building.

capacity-building initiatives were deemed essential for strengthening both individual and collective cybersecurity postures. The role of the private sector, especially platform providers, was underscored, with calls for a more proactive role in managing the security ecosystem and infrastructure to enhance collective cybersecurity efforts.

The roundtable discussions converged on the understanding that securing the ICT domain requires an inclusive and coordinated response that transcends borders, sectors, and disciplines. Cyber capacity building was highlighted as the necessary foundation for a secure, resilient, and stable digital environment, empowering nations to defend against evolving threats, enabling businesses and organisations to safeguard operations, and ensuring individuals can confidently engage with the digital domain without compromising safety.

Strengthening governance policies and processes was also discussed. The criticality of developing national cyber strategies and regulatory instruments, as well as improving governance structures to bolster cybersecurity, was underlined. Risks associated with the absence of such strategies and dedicated structures for implementation were explored. The discussion also delved into the challenges of implementing the framework, the essential policies and regulations needed, and the role of civil society, the private sector, and academia in these efforts. **Discussions concluded that national cyber strategies are vital for prioritising cybersecurity within a country and for guiding efforts towards cyber resilience.**

Foundational cyber capabilities and the essential pillars of cyber capacity building, including the role of public-private partnerships and the exchange of good practices, were also examined. The session featured an expert panel that discussed the importance of operational and technical capabilities, talent pipelines, and partnerships for various aspects of cybersecurity, such as law enforcement, threat intelligence sharing, and critical infrastructure protection. Challenges such as lack of trust, geopolitical issues, and resource limitations were identified. ***Recommendations included promoting south-to-south cooperation, treating cybersecurity as a prerequisite for digital transformation, and establishing cybersecurity funds at various levels.***

The UN was recognised for its pivotal role in facilitating international cooperation and capacity-building efforts, with a consensus on the need for the UN to continue coordinating the global response to ICT security challenges.

Trust fund and multistakeholder engagement: Looking to the future permanent mechanism

As discussed in July 2024[172]

In July 2024, states met at the eighth substantive session to adopt the group's third APR.[173]

Delegations welcomed the UN Secretariat's proposal to draft a report on establishing a UN voluntary trust fund on security and ICT use. However, concerns were raised about the fund's operationalisation, focusing on ensuring there is no duplication between the proposed fund and existing structures, including the World Bank Cybersecurity Multi-Donor Trust Fund and ITU funds and understanding the eligibility conditions of access to this fund.

The May high-level roundtable discussion on capacity building was commended by many delegations, along with the proposal to institutionalise these roundtables under a future permanent mechanism. Still, delegations such as **El Salvador asked** that the roundtables be held during the high-level week of the UN General Assembly to avoid overburdening smaller delegations. The country stated that delegations often face financial constraints and sometimes rely on external funding to attend these events.

The outcome: Most delegations welcomed the paragraph in the third APR, which outlines in detail the development of the voluntary trust fund, including specifics on its operationalisation, the role of the UN Secretariat, and the requirement to avoid duplication with existing initiatives. Moreover, it includes specific instructions for the UN Secretariat to address financial and administrative requirements, eligibility criteria, and monitoring mechanisms for the voluntary fund. Yet, Nicaragua held that the new formulation of the paragraph lacked focus on strengthening the security and capacity of states in the face of threats in the ICT realm. In response to El Salvador's concerns on future capacity-building high-level roundtables, the third APR includes a provision encouraging states in a position to do so to offer support to representatives and experts from developing countries to attend the roundtables to promote equitable geographical representation.

Support was expressed for **India's** proposal to create a Global ICT Security Cooperation and Capacity-Building Portal (GCSCP) and **the Philippines'** suggestion for a capacity-building catalogue, emphasising the need to align these initiatives with other ongoing efforts within and outside the UN to avoid redundancy and optimise resources. **The EU** asked that the APR reflect existing efforts by established actors in the ecosystem to ensure that the proposals in the capacity-building chapter would function well within the existing ecosystem. In the same vein, **Singapore** proposed that the envisaged portal should function as a plug-and-play platform to accommodate current and future capacity-building proposals by countries.

---

[172] Gavrilovic, Kazakova, Petit-Siemens, Roellinger, 'OEWG's eight substantive session.'

[173] Digital Watch Observatory, *OEWG 2021–2025 Third Annual Progress Report (APR)*.

While most delegations endorsed a multistakeholder approach in capacity building, recognising the significant roles of businesses, NGOs, and academia in cybersecurity capacity-building, **Russia** ***disagreed with overstating the involvement of non-governmental stakeholders and portraying them as equal participants in negotiations alongside states***.

Delegations, including **the USA** and **Australia**, ***requested language to be included in the third APR that would link to the proposals of the portal, the fund, and the future high-level roundtables on capacity building to the future permanent mechanism to ensure their continuity.***

The outcome: The third APR includes detailed considerations for avoiding duplication with existing capacity-building proposals. Moreover, the report describes the portal as a state-driven and modular one-stop-shop platform instead of a one-stop-shop tool, as stated in the first draft, to reflect Singapore's suggestion. The report emphasises multistakeholder engagement by explicitly recognising the roles of businesses, non-governmental organisations, academia, and youth in ICT security capacity-building efforts. It highlights the importance of inclusive platforms, regular high-level meetings, and collaborative support for capacity-building programs, thereby expanding the involvement and contributions of various stakeholders compared to the first version, which mentioned stakeholder engagement in a more general sense. On linking proposals to the future permanent mechanism, language was added to link the proposals of the roundtables, portal and fund to the future permanent mechanism.

Diverging views: Portal structure, voluntary fund, and existing initiatives coordination

As discussed in December 2024[174]

As usual, capacity building was one of the topics where there is a high level of consensus, albeit in broad strokes. There wasn't a single delegation denying the importance of capacity building to enhance global cybersecurity. However, ***opinions differed on several issues, including specific details on the structure and governance of the proposed portal, the exact parameters of the voluntary fund, and how to effectively integrate existing capacity-building initiatives without duplication.*** It was then expected that the OEWG would continue to speak about these issues at length to have concrete details in its final report and to allow the future mechanism to dive deeper into capacity building.

During the December 2024 session, ***delegations discussed the development and operationalisation of the Global Portal on Cooperation and Capacity-Building.*** Most delegations envisioned the portal as a neutral, member-state-driven platform that would adapt dynamically to an evolving ICT environment, integrating modules like the needs-based catalogue to guide decision-making and track progress, as well as **Kuwait**'s latest proposal to add a digital tool module to streamline norm adoption. On the contrary, **Russia** expressed

[174] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's ninth substantive session.'

concerns over the exchange of data on ICT incidents through the portal, stating that such data is confidential and could be used to level politically motivated accusations.

The session also discussed the creation of a Voluntary Contribution Fund to support capacity building in the future permanent mechanism. **South Africa** and other delegations highlighted the need for clearly defined objectives, governance, and operational frameworks to ensure the fund's efficiency and transparency. Monitoring mechanisms were deemed essential to guarantee alignment with objectives. Delegates broadly agreed on avoiding duplication of efforts, emphasising that the portal and the fund should complement existing initiatives such as the UNIDIR cyber policy portal, the GFCE civil portal, and the World Bank Cyber Trust Fund, rather than replicate their functions or those of regional organisations.

Further deliberations addressed the timing of the next High-Level Global Roundtable on capacity building. The roundtable's potential overlap with the 2025 Global Conference on Cyber Capacity Building in Geneva presented scheduling challenges, prompting consideration of a 2026 date.

Discussions on UNODA's mapping exercise revealed mixed views: while it highlighted ongoing capacity-building efforts, many felt it inadequately identified gaps, leading to calls for a yearly mapping exercise.

Finally, multistakeholder engagement emerged as a contentious issue, with **Canada** and the **UK** criticising the exclusion of key organisations like FIRST and the GFCE from formal sessions. ***Delegates called for reforms to ensure broader, more inclusive participation from non-governmental and private sector entities essential to global cybersecurity efforts.***

Backing for fund and portal ideas; Uncertainty surrounds details

As discussed in February 2025[175]

The capacity-building agenda item was resolutely oriented towards pragmatic discussions. Many delegations shared their national and regional practices and initiatives (the **EU**, **Columbia**, **Singapore**, **Bosnia and Herzegovina**, **Poland**, **Korea**, **Thailand**, **Canada**, **Israel**, **Albania**, **Japan**, **Morocco**, **Oman**, **Ukraine**, **Russia**).

A large number of states specifically highlighted the benefits of various fellowships (**Kuwait**, **Iran**), among which the Women in International Security and Cyberspace Fellowship (**Mauritius**, **Ghana**, **Albania**, **Kazakhstan**, **Democratic Republic of Congo**, **Samoa**, **Paraguay**, **El Salvador**) and the UN-Singapore Fellowship (**Mauritius**, **Ghana**, **Albania**, **Nigeria**, **Democratic Republic of Congo**).[176] In that vein, **Nigeria** and **Kuwait**

[175] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's tenth substantive session.'
[176] Global Forum on Cyber Expertise (GFCE), "Women in International Security and Cyberspace Fellowship," accessed August 1, 2025, https://thegfce.org/project/women-in-international-security-and-cyberspace-fellowship/. and Global Cybersecurity Capacity Centre (Cybil Portal), 'UN – Singapore Cyber Fellowship (UNSCF),' Cybil Portal, accessed August 1, 2025, https://cybilportal.org/projects/un-singapore-cyber-fellowship/

proposed to hold new fellowship programs under the auspices of the UN, similar to other UN fellowships related to international security matters.

Cyber-capacity building on a budget

Another item discussed was the Secretariat's paper about the Voluntary Fund.[177] ***Quite a few number of states expressed their support for the fund*** (**El Salvador**, **Columbia**, **South Africa**, **Rwanda**, **Morocco**, **Zimbabwe**, **Brazil**, **Kiribati**, **Cote d'Ivoire**, **Ecuador**, **Fiji** and the **Democratic Republic of Congo**) and consensus largely emerged on the need to not duplicate existing funding initiatives and reflect on its link with the World Bank Multi-Donor Trust Fund (**Germany**, **European Union**, **Kuwait**, **Australia**).[178] However, **France** ***specifically questioned whether the UN was a fit structure to support such capacity-building activities, and argued that it could be better positioned to play a role in linking existing initiatives.***

Western countries shared their capacity-building initiatives and specifically addressed the issue of costs. **The Netherlands** voiced the need to consider the cost efficiency of this initiative, and **Canada** asked for a more detailed budget, given that the costs presented are higher than those for similar activities that Canada usually finances. **Australia** reminded the audience that a new trust fund does not mean new money and that it could not support the proposal under its current formulation.

A large share of countries nevertheless positioned themselves in favour of open contributions from interested stakeholders other than member states, such as the private sector, NGOs, academia or philanthropic foundations (**Argentina**, **Paraguay**, **Malawi**, **Mauritius**, **Nigeria**, **Mexico**). Yet, **Russia** ***voiced its wariness concerning NGOs and companies sponsoring the fund as they may attempt to exert pressure.***

Cuba and **Iran** ***warned against the constraining aspect of the fund.*** **Iran** specified that the principles guiding capacity-building mentioned in paragraph 10 did not enjoy consensus among member states and warned against attempts to condition capacity-building activities on the adoption of norms.

A portal, yes– but what for?

A second pivotal discussion item was the Secretariat's paper about the development of a dedicated portal for cooperation and capacity-building based on a proposal made by India and member states' views.[179] Again, positions were consensual on the idea of a portal (**Columbia**, **United Kingdom**, **Morocco**, **Oman**, **Zimbabwe**, **Ecuador**, **Nigeria**, **El Salvador**, **South Africa**, **Rwanda**). Consensus also emerged around the fact that it should not duplicate the already existing portals and initiatives, such as UNIDIR Cyber Policy Portal

---

[177] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 14 January 2025* (A/AC.292/2025/2), 14 January 2025, https://docs.un.org/en/A/AC.292/2025/2.
[178] World Bank. Cybersecurity Multi-Donor Trust Fund. Accessed August 1, 2025. https://www.worldbank.org/en/programs/cybersecurity-trust-fund.
[179] OEWG Secretariat, *Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal*, 14 January, 2025, https://docs.un.org/en/A/AC.292/2025/1, and India, Working Paper on Global Cyber Security Cooperation Portal (GCSCP) – Rev.1, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_GCSCP_Rev1_Clean.pdf.

and the Global Forum on Cyber Expertise (GFCE) Cybil Knowledge Portal (**Fiji**, **Mexico**, **Tonga**, **Latvia**, **Mauritius**, **Germany**, **France**, **Samoa**, **Indonesia**, **Switzerland**, **Brazil**, **Mexico**, **Argentina**, **the Netherlands**).[180]

Some delegations tackled the issue in a very pragmatic way. **Korea** questioned whether simply including direct links to existing portals was appropriate (supported by the **UK**) and proposed to have a technical review of the integration of the portal, including the PoC directory into a new portal to establish an integrated platform (backed by **Malaysia**). **Latvia** reflected on potential existing administrative limitations and UN procurement rules about linkages with other websites, based on a previous IGF experience.

The Secretariat wrapped up this discussion by specifying that ***the sections pertaining to the technical and administrative requirements were coordinated with the ICT office in charge of UN-hosted platforms and websites, and encouraged member states to take a closer look at these sections.*** Still pertaining to pragmatic questions, **Mauritius** and **India** proposed that the portal be multilingual.

The level of publicity and accessibility of the portal was also discussed. **Korea** and **Kazakhstan** proposed that the portal remain fully accessible to the public. Other states introduced nuance in the publicity. **The Netherlands** asked for the PoC directory to remain accessible to member states only, whereas **Côte d'Ivoire** proposed that only modules 1 and 5 (respectively, the repository of documents and resources and the platform for exchange of information, including the potential participation of non-governmental entities) could be made public. **India** further suggested 3 levels of access: member states, stakeholders and the general public.

A major point of contention remained the exact content of this portal. Some states reaffirmed an incremental approach to the content of the portal (**Kazakhstan**, the **EU**, **Australia**), starting with basic functionalities, without necessarily specifying what those basic functionalities should be. **China** and **Russia** specifically warned against the use of the portal to facilitate information sharing regarding response to threats and incidents.

Indonesia suggested a specific section for stakeholders to share their own best practices, research papers, etc., whereas **Russia** asked for NGO contributions to be published only for state information. On a side note, **Cote d'Ivoire** proposed to have a publication of an indicative quarterly or annual calendar along with the monthly publication of capacity-building initiatives and events.

The future permanent mechanism: How to tackle capacity building

States also tackled the structuring of capacity-building discussions within the future permanent mechanism. **Iran**, **Argentina**, **Brazil** and **Paraguay** ***supported the proposal to have a dedicated working group on capacity-building***, as circulated in the chair's discussion paper.[181] A vast majority of states have defended a cross-cutting approach to capacity-building, with this agenda item being discussed across thematic groups (**Tonga**, **Vanuatu**, **Canada**, **Kazakhstan**, **Kiribati**, **Ireland**, **Ukraine**, **Fiji**).

---

[180] United Nations Institute for Disarmament Research (UNIDIR), Cyber Policy Portal, accessed 1 August, 2025, https://cyberpolicyportal.org/. and Global Forum on Cyber Expertise (GFCE), Cybil Knowledge Portal, accessed 1 August, 2025, https://thegfce.org/outputs/cybil-knowledge-portal/.
[181] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Letter dated 27 January 2025 (A/AC.292/2025/3).

Some delegates proposed mixed approaches, such as the **EU** and **Australia's** similar view that thematic groups can help identify gaps and specific challenges pertaining to capacity-building, and that these reflections can fuel a horizontal capacity-building discussion in plenary. **Indonesia** suggested that the thematic groups were the place to focus on technical recommendations rather than duplicating high-level policy discussions. In that vein, **Indonesia** also suggested establishing terms of reference to frame these discussions.

Finally, ***states expressed their support for the organisation of high-level panels*** such as the Global Roundtable on ICT Capacity Building held in May 2024 (the **UK**, **Morocco**, **Zimbabwe**, **Kazakhstan**, **Ukraine**, **Germany**).[182] **Thailand** recommended that such high-panels be held on a biannual basis, and **Australia** suggested considering them as a 'capacity-building exposition'. **Canada** argued that it should be held at other levels than the ministerial-level to distinguish it from plenary work. It further proposed that it could be a venue for beneficiaries to meet organisations deploying capacity-building activities. The chair recalled the initial scepticism around this initiative but recommends that in the final report a decision should be made about the next Global Roundtable.

Alignment on principles; A fractured path to operationalisation

As discussed in July 2025[183]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[184] Echoing previous sessions, there was broad recognition of capacity building's foundational role in implementing norms, fostering international legal dialogue, and reinforcing confidence-building measures.

Yet, ***as the final OEWG session unfolded, this familiar consensus was accompanied by a renewed urgency to move beyond conceptual alignment. Action-oriented capacity building became a recurring buzzword, capturing the shared ambition to shift from declaratory commitments toward concrete, needs-based mechanisms.***

This convergence created early momentum for advancing capacity building structures. ***Still, despite alignment on principles, the pathway to operationalisation remained fractured along critical lines.***

What role for the UN?

During negotiations, two opposing positions reflected fundamentally different priorities: ***Western states emphasised flexibility and minimal commitments, while many developing countries viewed the early operationalisation of capacity building as essential to anchoring the future mechanism in tangible delivery and ensuring it addresses the digital divide.***

---

[182] UNIDIR, Inaugural Global Roundtable on ICT Security Capacity Building: Recap and Key Highlights, May 16, 2024, https://unidir.org/inaugural-global-roundtable-on-ict-security-capacity-building-recap-and-key-highlights/.
[183] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Radunovic, Roellinger, 'UN OEWG concludes.'
[184] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

At one end of the spectrum, **the USA *opposed all new CB mechanisms and rejected any operational role for the UN, citing its ongoing financial crisis***. **France** and **Canada** adopted a more cautious stance, advocating ***a step-by-step approach centred on mature initiatives*** and warning against the premature creation of new structures.

In contrast, countries such as **Nigeria (on behalf of the African Group), Tunisia (on behalf of the Arab Group), Brazil, Iran, and Egypt *called for a more active UN role, supported by predictable and well-resourced mechanisms, including calls to include more concrete language on the operationalisation of a UN Voluntary Fund.***

Consistent with this approach, the **African Group**, **Latin American states**, and others ***backed the creation of a Dedicated Thematic Group (DTG) on capacity building within the permanent mechanism*** to ensure coordination, needs mapping, implementation tracking, and inclusive participation, functions they feared would be sidelined if CB remained a merely cross-cutting issue. **The USA** and **Canada *opposed this, arguing that issue-specific groups risked bureaucratic redundancy and inefficiency.***

The outcomes: The final outcomes reflects a carefully negotiated compromise: it advances the institutional scaffolding of the future mechanism but falls short of the ambitions expressed by many developing states. The agreement to establish a DTG on capacity building stands out as a meaningful step, providing formal recognition of capacity buidling as a core pillar. Yet, substantive elements, particularly related to funding, were left unresolved. The UN-run Global ICT Security Cooperation and Capacity-Building Portal (GSCCP) will proceed through a modular, step-by-step development model, and roundtables will continue to promote coordination and information exchange. However, proposals for a UN Voluntary Fund and a fellowship program were deferred, with references downgraded to non-binding language and postponed for further consideration. While the framework reflects principles of gradualism and inclusivity, it also exposes the limits of consensus: Western states succeeded in prioritising flexibility and minimal commitments, while developing countries, especially those from the Arab and African Groups, voiced frustration that the outcome lacked the concrete, adequately resourced mechanisms needed to close enduring digital divides. Without progress on predictable funding and operational tools, they warned, the credibility and effectiveness of the DGT group on capacity building risks would be undermined from the outset.

Regular institutional dialogue

UN processes: Achieving complementarity[185]

As discussed in June 2021

From 2019 to 2021, two concurrent processes were discussing the peaceful use of ICTs under the auspices of the UN: The OEWG on ICT security 2019-2021 and the fifth Group of Governmental Experts (GGE). In October 2020, a proposal for the Programme of Action (PoA) was also put forward as an option for establishing a permanent process for discussions.[186] In December 2020, before the OEWG 2019-2021 even ended, the UNGA renewed the group from 2021 to 2025.[187]

During the OEWG's organisational session, **Switzerland**, **Thailand**, and **the Philippines** ***underlined the complementarity between the OEWG and GGE.*** It seemed that **Russia** was not opposed to the GGE format either. Russia's elaborate proposal of subgroups did not include an OEWG subgroup on norms, rules, and principles of state behaviour. This could have been quite telling – the country may have been one of the most vocal co-sponsors of the OEWG in 2019, but it seemed very possible that it would want the GGE to continue tackling norms, rules, and principles.

The PoA proposal enjoyed broad support from the UN member states. Five delegations suggested the proposed PoA to be discussed in the OEWG, and one of its main co-sponsors, **France**, stressed that there is work underway to ensure the complementarity of the PoA and OEWG.

At this point in time, the GGE/OEWG/PoA saga looked convoluted. The UNGA was to decide on the GGE's fate in September 2021. The OEWG would last until 2025. The proposal for the PoA had not been elaborated in detail yet, and many countries expressed that the OEWG would be the best venue to do so.

Establishment of thematic subgroups

Quite a few delegations favoured establishing thematic subgroups within the OEWG. **Pakistan** stated that the establishment of thematic subgroups would prove helpful in fulfilling the mandate of the OEWG and facilitating the exchange of views. The **EU and its member states** noted that, in case of establishing any subgroups, those should have an added value to the work of the OEWG and contribute to the overall objective, and pointed out that the PoA would provide for a permanent infrastructure for this purpose.

---

[185] Gavrilovic, 'What's New with Cybersecurity Negotiations? The Second Cyber OEWG's Organisational Session.'
[186] Joint Contribution by Argentina, Australia, Canada, Chile, Colombia, Estonia, Germany, Japan, the Netherlands, New Zealand, Norway, the Republic of Korea, and the United Kingdom, The Future of Discussions on ICTs and Cybersecurity at the United Nations, 8 October 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.
[187] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/75/240, 30 March 2021, https://docs.un.org/en/A/RES/75/240.

South Africa, Poland, and Venezuela proposed the creation of six subgroups on threats, norms, international law, CBMs, capacity building, and institutional dialogue. **Australia and Romania** noted that thematic subgroups, if at all established, should deal with those six topics.

According to some delegations, subgroups could lead to fragmentation of the discussion if not held consecutively. Delegations that made statements to this effect were **Argentina**, **Egypt, Indonesia, Malaysia**, **Mexico**, **Norway**, **Poland**, and **South Africa. Chile, France, and South Africa** also pointed out that inclusiveness would suffer if subgroups were not held consequently, due to limitations of smaller delegations.

Russia suggested setting up ***a hierarchy between subgroups*** by establishing a priority subgroup on threats and rules of responsible behaviour, as well as subsidiary subgroups on applicability of international law in the ICT sphere, on CBMs, capacity building measures, and regular institutional dialogue. However, **Brazil, Costa Rica, India, Canada, New Zealand, the UK, and Switzerland** explicitly ***noted that they are against creating a hierarchy between subgroups and themes, since all of the themes discussed at the OEWG are equally important.*** Due to such concerns, **Costa Rica** and **India** ***decided not to support the idea of subgroups.***

Peru thought that there needs to be a balance between the subgroups, but elaborated no further.

A few delegations opposed the formation of subgroups**. Colombia** stated that the work should not be divided into subgroups, as it would be too difficult to participate in the work of the OEWG. **Canada, Costa Rica, and Ecuador** also preferred to continue having thematic discussions and plenaries under the guidance of the Chair and in a format which reproduces the successful approach of the previous OEWG, as this would reduce the organisational burden on the Secretariat and member states.

The modalities of stakeholder engagement

Concerning the involvement of stakeholders in the work of OEWG 2021–2015, the states did not come to a conclusion. The main issue, as pointed out by Gafoor, is whether the states would adopt the precedent of the first OEWG in involving other stakeholders or if a different arrangement would be adopted.

Argentina, Canada, the EU, Ecuador, Mexico, the UK, Cuba, New Zealand, Suriname, Ireland, Switzerland, Norway, and France ***wanted to see the involvement of all stakeholders***, as the interconnected and complex nature of cyberspace requires joint efforts by government, private sector, civil society, technical community, and academia.

Mexico asked for ***a formal adoption of the multistakeholder model***, noting that a mechanism allowing other stakeholders to present their input should be established.

Russia voiced its support for the multistakeholder dialogue, but wanted to see ***only the involvement of NGOs with consultative status at ECOSOC***. **Costa Rica** thought that all NGOs which countries deem important, not just those with consultative status at ECOSOC, should be engaged in multistakeholder dialogue.

Chile's viewpoint was that there needs to be new practices for allowing participation of new stakeholders, and it suggested that other stakeholders should be able to contribute in official

sessions. **South Africa** noted that civil society, the private sector, and academia can be engaged in specific thematic subgroup discussions. **Switzerland** advised to look at the language agreed by the UN group to fight cybercrime regarding the participation of non-state actors, which is as follows: 'Encourages the Chair of the Ad Hoc Committee to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention.'

Iran, Nicaragua, **India, and Indonesia** suggested that ***the participation of other stakeholders should be addressed in the same way as the previous OEWG, in an informal setting.***[188]

The possible formats: The OEWG, the PoA, and their possible interplay

As discussed in December 2021[189]

With the GGE 2019-2021 concluding its work in May 2021, states could look to the OEWG or the PoA as the formats in which regular institutional dialogue on ICT security would be held.[190]

Cuba, Indonesia, and **Russia** ***endorsed the OEWG format*****. Indonesia** saw the OEWG process as the only multilateral and inclusive intergovernmental body to address international security in the use of ICTs. According to **Russia**, the OEWG format had already proven its effectiveness and relevance. As the experience of the first OEWG had shown, it has all the features that the international community requires. Russia did not exclude the possibility of making the OEWG a long-term mechanism or its transformation into a permanent mechanism if states find it necessary.

The PoA was much discussed. **France**, as one of the POA sponsoring countries, along with Egypt, drew attention to the submission of a Working paper for a Programme of Action (PoA). ***France shared core elements the proposal consists of: the PoA should seek to establish a permanent institutional structure – a platform that could tackle concrete projects such as, for instance, capacity building, and could ensure regular follow-up through periodic meetings. The PoA could regularly assess progress made in implementing those norms, analyse the evolution of needs expressed by the states, and identify, if necessary, new priority areas of action.***

Concerning the possible modalities for the establishment of the PoA, **Egypt** said that ***inclusive consultations will be conducted to seek states' views on the PoA***. The consultations would provide opportunities to share and discuss further options for modalities and analysis and lessons learned from previous program actions such as the Program of Action on Small Arms and Light Weapons.

---

[188] Gavrilovic, 'What's New with Cybersecurity Negotiations? The Second Cyber OEWG's Organisational Session.'
[189] Digital Watch Observatory, *UN OEWG 2021–2025 – Regular institutional dialogue*, 17 December, 2021, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue.
[190] Gavrilovic, 'What's new with cybersecurity negotiations? The UN GGE 2021 Report.'

Chile, **the Czech Republic, Italy**, **Spain**, and **Ukraine** ***expressed their support for the PoA.***

Austria, Colombia, **Ecuador**, **Estonia**, **Finland, on behalf of the Nordic states**, **Ireland**, **Latvia**, **the Netherlands**, **South Korea**, **Switzerland**, and **the UK** also noted that ***the PoA could help states focus on implementing the agreed-upon normative framework.*** In **Ecuador**'s view, the ***PoA would be a point of departure toward establishing a legally binding instrument in the future.***

Several countries also noted that ***the PoA could help facilitate cyber capacity-building.*** These include **Argentina**, **Ecuador**, **Germany**, **Finland on behalf of the Nordic states**, **Ireland**, **Latvia**, **the Netherlands**, **Poland**, **Portugal**, **South Korea**, **Switzerland, and Romania.**

Russia viewed ***the PoA as a mechanism for reviewing the implementation of norms.*** Russia suggested that the PoA could be discussed as part of a thematic discussion on rules, norms, and principles of conduct.

Considering inclusiveness and effectiveness, **Israel** stated that a dialogue on ICT should be voluntary and non-legally binding. Israel considered it ***premature to adopt a position on the PoA since the modalities and characteristics were not yet clear***.

The interplay between the OEWG and the PoA

Some countries, such as **the Netherlands,** also underlined that future dialogue should not duplicate the existing UN mandates or efforts. **Germany** considers that the PoA would strengthen states' capacities and expertise to actively contribute to debates in all relevant UN forums such as the OEWG. **Colombia**, **the EU on behalf of the EU member states, the Republic of North Macedonia, Montenegro, and Albania, Ireland**, **Poland**, **Romania,** and **Switzerland** also stressed that the PoA is complementary to the OEWG.

In **the EU's** view, the OEWG could hold informal meetings with participants to exchange views on challenges for implementation, providing valuable input for the establishment of the PoA. The OEWG could facilitate timely and dedicated exchanges on the PoA, including the participation of the multistakeholder community. Australia aligned with these points.

Competing visions: The OEWG vs the PoA

As discussed in March 2022

The PoA processed to get more support in 2022: 57 states and the EU expressed the desire to establish the PoA as a permanent institutional mechanism. During the meeting, delegates from **Chile**, **Thailand**, **the Netherlands**, **Austria**, **South Africa**, **Canada**, **Australia**, **Switzerland**, **Japan**, **Singapore**, **El Salvador**, **Colombia**, **the UK**, and **Argentina** reiterated their support of the PoA proposal or expressed the wish to join it.

Egypt noted that ***the co-sponsors are working to improve the PoA working paper to be submitted against the third session of the OEWG in July, which will contain more practical steps towards establishing the PoA***. For example, a regular meeting would be held every two years, and a review conference would be held every six years. Technical

working groups would be established to work during the intersessional period to address the exponentially evolving nature of the cyber issues. Therefore, Egypt stressed that the OEWG should consider establishing the POA through its annual progress report to complement the group's work.

The EU suggested the OEWG could facilitate timely and dedicated exchanges on the POA, considering the specific views and needs of all states and relevant stakeholders and ensuring that the OEWG is regularly informed about the state of play.

France and **the Netherlands** said that the PoA would allow states to establish a dialogue and structured cooperation with private actors and civil society in fields where they see necessary.

Chile noted that the main aim of the PoA should be to facilitate the implementation of a consensus framework for the responsible behaviour of states in the use of ICTs. For this reason, the PoA would support capacity building based on the state's own needs assessment.

Thailand noted that the PoA would play a significant role in developing a universally accepted and common understanding of international law applicable in cyberspace, especially in the absence of a legally binding instrument on this matter. Also, the PoA must be aligned with and complementary to the OEWG.

Canada supposed the OEWG could continue to work on the aquis, but that the PoA would then focus on implementing this aquis.

Switzerland, **Singapore**, **Argentina**, **Colombia** and **Japan** claimed that the PoA should be the regular institutional dialogue under the auspices of the UN and complementary to the current OEWG. It would focus on implementation capacity building and allow for inclusion of the multistakeholder community.

While the PoA was imagined as a complementary track for the OEWG, there was still a minority of states that pointed out that ***the OEWG should remain the only negotiating platform for cyber issues.***

Iran said that the OEWG should continue its function as an inclusive intergovernmental body for consultation, cooperation, and decision-making in cyber-related issues established by the UN. The PoA proposal was build on the same logic as the UN small arms and light weapons program of action. Still, this experience' shows that procedural approaches such as the POA are inherently challenging and, instead, states should move towards legally binding, instrument on cybersecurity and think of establishing an OEWG subgroup for the commencement of negotiations on a comprehensive cybersecurity convention.

Cuba supported action-oriented initiatives, but did not favour parallel mechanisms that seek to replace the work of the OEWG. Cuba also noted that any cybersecurity initiative must result from a recommendation of the OEWG, and it must be based on a broad-based process of discussion among member states and should be adopted by consensus.

Russia said the OEWG should remain the only negotiating mechanism under the UN to deal with cyber issues. The decision on the future format for regular institutional dialogue,

whether through the continuation of the OEWG or its transformation into a permanent mechanism, could be worked out by states at a later stage of this group.[191]

It had remained to be seen if heir opposition would matter – the co-sponsors' original PoA proposal suggested that 'a resolution could be adopted at the First Committee of UNGA to establish the PoA', and decisions in the First Committee are made by the majority of votes of members present and voting. Co-sponsors promised to enhance the PoA working paper with practical steps for its establishment before the July session.[192]

Building momentum: The PoA recognised in the APR

As discussed in July 2022[193]

In July 2022, states met at the third substantive session to adopt the group's first APR.[194]

Whether a Programme of Action will be established or not, and its purpose would be, was still a point of contention. Countries which are co-sponsors of the PoA voiced their support for the PoA. Some countries, such as **Colombia**, **El Salvador**, and **Canada**, suggested that the PoA should be the future institutional dialogue to implement the aquis. **France** and **Korea** indicated that it may become a permanent mechanism for capacity building.

The OEWG was still preferred by **Russia** and **Iran**. Russia stated that the institutional dialogue should be pursued through continued work of the OEWG, noting that the OEWG could become a permanent mechanism. Iran stated that the OEWG should remain the only negotiating mechanism within the UN on the security of and in the use of ICTs.

However, **Russia**, **Iran** and **Thailand** ***supported the proposal in the draft APR that the scope, contents, and other elements of a PoA should be discussed within the OEWG.***

The outcome: The first APR recognised the centrality of the OEWG as the mechanism within the UN for dialogue on security in the use of ICTs. States would also engage in focused discussions on the relationship between the PoA and the OEWG, as well as on the scope, content, and structure of a PoA.

---

[191] Digital Watch Observatory, *UN OEWG 2021–2025 – Regular institutional dialogue*, April 1, 2022, https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue.
[192] Diplo Team, 'What's New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.'
[193] Diplo Team, 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.'
[194] OEWG 2021–2025 First Annual Progress Report (APR).

First Committee approval: PoA resolution ignites OEWG discussions

As discussed in December 2022[195]

In November 2022, a the UN First Committee **adopted a resolution on the PoA.** It was adopted by a recorded vote of 157 in favour to 6 against (**China**, **Democratic People's Republic of Korea**, **Iran**, **Nicaragua**, **Russia**, **Syria**), with 14 abstentions.[196] This development set the tone of the December 2022 discussions on the regular institutional dialogue.

Many states welcomed the PoA during the December 2022 session, with a number of countries supporting meetings within OEWG in 2023 to discuss modalities of PoA, including **Egypt, France, South Africa, Japan, the EU, the Netherlands, the USA, Colombia, Germany,** and **Pakistan**.

Some states expressed their opposition to the PoA. **Nicaragua, Syria,** and **Iran** stressed that the OEWG should remain the only negotiating mechanism. **Russia, Nicaragua, Israel, Iran,** and **China** advanced the view that ***the PoA or any new mechanism should be adopted on a consensus basis within the OEWG rather than imposed by a group of states.*** **Russia** also qualified the conceptual basis of the PoA as 'irrational', as it is a mechanism which will be established in 2025 to implement voluntary norms agreed upon in 2015.

However, **Nicaragua**, **Syria** and **Iran** noted ***that the PoA could be discussed at the OEWG, even as they did not put much faith in its success***. **Russia** stated, at that point in time, the OEWG had three years until 2025 – more than enough time to jointly develop an understanding on the utility of creating a PoA.

Other proposals regarding the modalities of the institutional dialogue emerged during the discussion. **Russia** thought of ***a mechanism that would allow formalising decisions as soon as the group agrees upon them.*** In the same vein, **Iran** argued that it was ***essential to resume the practice of paragraph-by-paragraph negotiation***. The UK and **France** also raised the idea of ***building a checklist of the key components that any future mechanism should include***, as UNIDIR did for the PoC directory.

---

[195] Gavrilovic, Ittelson, Petit-Siemens, Radunovic, Roellinger, Stadnik, 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs'.
[196] Digital Watch Observatory, *Resolution on the Programme of Action (PoA) on Cybersecurity Adopted*, 3 November, 2022. https://dig.watch/updates/resolution-on-the-programme-of-action-poa-on-cybersecurity-adopted.

Sustained focus: PoA stays in the OEWG discourse

As discussed in March 2023[197]

States continued to discuss the PoA in March 2023 as this was the first official substantive session the OEWG held after the First Committee of the UNGA adopted the PoA resolution 77/37.

The supporters of the PoA emphasised the complementarity of the OEWG and the PoA. They also stressed engaging with other stakeholders more constructively. Interestingly, during this substantive session, several states mentioned the possibility of discussing additional cyber norms under the PoA, if needed – the point of past contradictions between the 'two camps'.

Brazil, El Salvador, South Africa, India, and Malaysia ***warned once again of the problem of parallel tracks of discussions that require more resources to participate in.*** **Germany** said that the work on the PoA should not conflict with the OEWG meetings, but that the PoA should be ready by the end of the OEWG's mandate in 2025.

The Nordic countries, Egypt, Canada, the Netherlands, Portugal, Colombia, France, Switzerland, and **Australia** ***called for a dedicated session in 2023–2024*** to provide all states with the opportunity ***to have comprehensive discussions on the structure, content and objectives of the PoA.*** Calls for this session could be reflected and answered in the APR.

A few countries remained staunch against the PoA. **China** noted that states who supported the PoA resolution were undermining the status of the OEWG as a single and inclusive process under the UN auspices. **Cuba** claimed that OEWG had proven its value and should be the central mechanism for regular institutional dialogue until 2025. **Iran, Pakistan, and Syria** stressed that any proposals on regular institutional dialogue should be discussed within the OEWG on an equal footing.

A new UNGA body for regular institutional dialogue

Russia, **Belarus, and Nicaragua** suggested an alternative to the PoA initiative.[198] The mandate of the future body (under the UN General Assembly auspices as an open-ended working group/commission/committee/review conference) should include the entire spectrum of issues related to ICT security. It should be oriented towards the practical implementing agreements reached in the OEWG. In particular, its mandate could include:

- drafting a legally binding international instrument on international information security;
- implementing the CBMs through developing mechanisms for practical cooperation among states;

---

[197] Gavrilovic, Grottola, Ittelson, Kazakova, Petit-Siemens, Stadnik, 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session.'

[198] Russian Federation and co-sponsors (Republic of Belarus; Republic of Nicaragua), Concept Paper of the Russian Federation on Establishing a Regular Institutional Dialogue on Security of and in the Use of ICTs under UN Auspices, 21 February 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Regular_institutional__dialogue_Proposal_of_the_Russian_Federation.pdf

- establishing mechanisms to assist states in enhancing their capacities to protect national information resources.

The role of stakeholders should be strictly informal, while observers can only be from accredited organisations.

Upheld entrenched positions: Differences hold firm

As discussed in May 2023[199]

The overall atmosphere of the discussions reflected the long-held divisive opinions. Some delegations prepared elaborate proposals for the PoA, some delegations outright opposed the PoA at this stage, and some delegations just wanted to avoid duplication of efforts.

Among the supporters of the PoA, coordinating capacity-building efforts and implementing the already agreed-upon framework were considered to be within the scope and goals of the PoA.

A number of countries expressed that the PoA can coordinate capacity-building efforts and create synergies across existing instruments. The **EU**, the **Netherlands** and **Estonia** mentioned that the POA should seek to leverage relevant existing initiatives and build on existing capacity-building structures and platforms to coordinate capacity-building efforts and map the capacity-building needs of countries worldwide.

Egypt and **Mexico** both suggested that the POA should lay the groundwork for international cooperation around capacity building. Egypt added that it should facilitate and monitor the implementation of the agreed framework through the provision of tailored capacity-building programmes, and Mexico focused instead on the role of the POA as a platform to exchange information, experiences, and best practices related to the prevention and mitigation of cyber incidents.

Czechia proposed that the POA could be used as a platform to exchange views and ideas and act as a coordinator for donor efforts and mapping the needs of recipient countries.

The PoA could also play a role in norms implementation—**The EU** noted that the PoA could guide national efforts to implement frameworks of responsible state behaviour by supporting the exchange of best practices and lessons learned, implementing relevant norms through concrete capacity-building projects, and cooperation with the private sector that owns many critical infrastructures in states.

A number of delegates also elaborated on what should be under the PoA's purview. The **EU** and **Czechia** noted that the PoA should have the flexibility to develop new norms and in the case of the EU, new CBMs. **Australia** and **Mexico** proposed that existing and emerging threats and measures to address them should also be in the scope of the PoA, with **Mexico** suggesting that the exchange of information, experiences and best practices related to the prevention, management and mitigation of cyber incidents could also be included in the PoA. The Mexican delegation also believed that the PoA could serve, in the

[199] Gavrilovic, Kazakova, and Petit-Siemens, 'Informal OEWG consultations on capacity building.'

long term, as an umbrella instrument under which the efforts of other parallel mechanisms could converge.

Additionally, ***diverse views have been shared on how the PoA could be organised***, how often the review of the programme should be conducted, and which structure and format of work it should have, including annual meetings, intersessional meetings, review conferences, and technical working groups.

A group of countries that opposes the PoA, shared different views on the future regular institutional dialogue. **China** noted that some states 'tried to impose a UNGA Resolution on a PoA last year and split the UN process on ICT security and undermine the OEWG'. The Chinese delegation stressed that in accordance with the OEWG mandate, 'there is only a regular institutional dialogue, and there is no so-called PoA'. China proposed that the future mechanism should be developed based on two principles: (1) upholding the agreed-upon framework and (2) formulating new international rules in response to evolving situations, particularly data security issues. However, no concrete suggestions on the future regular institutional discussion came from this group.

For instance, **Russia** stressed that the agenda of the PoA is considerably narrower than that of the OEWG, and that the Western countries attach very specific political meaning to the PoA, publicly promoting it as an anti-Russian course. Instead, for the future regular institutional dialogue, Russia continued advocating for other modalities for the future process, where, as proposed, among other points, only accredited non-state actors should be allowed the right to participate in official events as observers.[200]

Brazil called for a single-track discussion in the UNGA and proposed that the OEWG's final report recommends the UNGA start a negotiation process throughout 2026, culminating in a high-level meeting to endorse a document that would, on the one hand, consolidate and reaffirm the agreed upon framework, and on the other hand, establish the modalities of work of the future regular institutional dialogue.

Other delegations did not directly express views on the PoA during this session but rather called for avoiding polarisation and the duplication of efforts.

[200] Russian Federation, Updated concept of a UN Convention on International Information Security. 15 May 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

Structuring institutional dialogue: Balancing mechanism choice, mandate, and consensus

As discussed in July 2023[201]

In July 2023, states met at the fifth substantive session to adopt the group's second APR.[202]

Which mechanism for regular institutional dialogue should the APR mention?

The critical point of contention lay between those favouring the Program of Action (PoA) and those advocating for equal consideration of all proposals in the APR. The division among delegations was stark, splitting the EU, the USA, Korea, France, and other Western democracies on one side and Cuba, Iran, Pakistan, Syria and Russia on the other side.

The USA proposed inserting a new paragraph 49 b, highlighting discussions on UNGA resolution 7737, which supports a new PoA for responsible state behaviour in cyberspace. **France**, **the EU**, and **the USA** proposed that the APR reflect the Secretary-General's report on scope, structure, and content of the PoA and intersessional meeting outcomes regarding the POA's modalities. Additionally, the UN Secretariat was requested to brief the OEWG during the OEWG's sixth session about the POA's scope, content, and structure.

Portugal and **Korea** also supported the PoA, citing its considerable support under the UN's umbrella, referencing broad approval from member states through General Assembly resolution 7737.

Numerous countries advocated for dedicated intersessional meetings to delve into specific discussions and elaborate on the modalities of the PoA.

On the other hand, **Cuba** and **Iran** urged the incorporation of all future mechanism proposals into the APR. **Russia** voiced concerns about the existing draft of the APR, arguing that the section on regular institutional dialogue was biassed in favour of the PoA. **Syria** asserted that prioritising the PoA gave the impression of broad consensus, contrary to the working group's mandate to consider various security initiatives. Syria also noted that discussions revealed differing viewpoints on the effectiveness of the PoA and recommended evaluating it before any definitive steps.

The IBSA forum (**India**, **Brazil** and **South Africa**) proposed a comprehensive institutional dialogue mechanism encompassing crucial aspects of the ICT environment, including trust-building and deeper discussion on aspects lacking a common understanding. This mechanism should be intergovernmental, open, inclusive, transparent, flexible, and action-oriented, operating by consensus to prevent stagnation while avoiding a potential veto power.

Finally, **China** introduced a potential compromise, suggesting compiling common elements from various positions and proposals to reduce differences and find convergences. They emphasised the importance of a balanced representation of all parties' positions in the APR.

---

[201] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's fifth substantive session'.
[202] OEWG 2021–2025 Second Annual Progress Report (APR).

The outcomes: To settle divergence on the proposals for the future mechanism, the APR reflects other proposals made for regular institutional dialogue while highlighting the progress made in discussing the PoA. The wording on the future permanent mechanism followed the compromise suggested by China. As an initial step to building confidence and convergence, states will propose some common elements that could underpin the development of any future mechanism for regular institutional dialogue. Other noteworthy aspects integrated into the APR encompassed focused dialogues on the relationship between the PoA and OEWG and acknowledgement of the relevance of previous OEWG and GGE work, both proposals made by Vietnam. The proposal on dedicated intersessional meetings to continue discussions on the PoA received broad support and was included in the APR. There was no mention of UNGA resolution 7737 in the APR. However, the Secretariat was still requested to brief the OEWG at its sixth session on the report of the Secretary-General submitted to the General Assembly at its seventy-eighth session.

Preparing a legally binding instument: In the future group's mandate?

Pakistan, **Iran** and **Russia** advocated for ***the work of the future mechanism to be based on the recommendations of the OEWG and the possibility of crafting a legally binding ICT instrument within that framework.***

However, France suggested that the paragraph that contains reference that the mandate of the future permanent mechanism might include by preparing a draft legally-binding international instrument on ICTs.

However, several delegations, including **Belgium**, **South Korea**, **the EU**, **the USA**, and **Japan**, among others, supported France's proposal to ***remove the draft paragraph due to concerns about incorporating language about a legally binding instrument.*** **South Korea** viewed such an instrument as premature and suggested that if it were included at all, it should be under the international law section. **Vietnam** deemed the text inappropriate in acknowledging diverse views and ideas discussed in the working group.

The principle of consensus and the regular institutional dialogue

A new debate about the consensus in the future regular institutional dialogue emerged: **France** noted that ***the APR should not prejudge that the decision-making processes in the future mechanism will be consensus-based.*** **Australia** and **Austria** supported France's suggestion. **Iran** said that the draft text does not reflect the need to pay attention to a step-by-step negotiation approach. **The USA** noted that the text is too prescriptive – ***states do not need to agree by consensus on establishing a future mechanism for regular institutional dialogue, as the General Assembly does not require it.*** Austria supported this view.

The outcome: States recognised the importance of the principle of consensus regarding both the establishment of the future mechanism itself as well as the decision-making processes of the mechanism.

Two roads ahead: The PoA or a new OEWG

As discussed in December 2023[203]

The 6th substantive session of the OEWG 2021-2025 marked halfway to the end of the mandate, and the fate of the future dialogue on international ICT security remained open. The situation was exacerbated with a new plot twist: in addition to the Program of Action (PoA) that was proposed by France and Egypt back in 2019 and noted by GA resolutions in 2022 and 2023 (77/37 and 78/16), Russia tabled a new concept paper introducing a permanent OEWG as an alternative.[204]

All supporters of the PoA stressed the number of votes that resolution 78/16 got in the GA: 161 states upheld the option to create a permanent, inclusive and action-oriented mechanism under the UN auspices upon the conclusion of the OEWG 2021-2025 and no later than 2026, implying PoA. Notably, ***supporters of the resolution stressed that the final vision of the PoA would be defined at the OEWG in a consensus manner***, considering the common elements expressed in the second APR. Several states noted that no PoA discussions may be held outside the OEWG to maintain consistency.

There was, however, no consolidated view of the details of the PoA architecture. Egypt and Switzerland provided some ideas about the number and frequency of meetings and review mechanisms. However, Slovakia, Germany, Switzerland, Japan, Ireland, Australia, Colombia, the Netherlands and France suggested including in the PoA architecture already discussed initiatives like PoC, Cyber Portal, threat repository, national implementation survey and other future ideas. The PoA recognised the possibility of developing new norms (beyond the agreed framework). Through the future review mechanism, it would identify gaps in existing international law and consider new legally binding norms to fill them if necessary. Some states pointed out that the PoA should allow multistakeholder participation during meetings, especially in the private sector, and allow them to submit positions. However, the final decision-making will remain with states only.

The Russian proposal of a permanent OEWG after 2025 was co-sponsored by 11 states. It offered several principles for the group's future work, stressing the consensus

---

[203] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Stadnik, 'OEWG's sixth substantive session.'
[204] Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 18 July 2022 from the Chair of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 addressed to the President of the General Assembly* (A/RES/77/37), 18 July, 2022, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/737/71/PDF/N2273771.pdf?OpenElement. and Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Letter dated 13 March 2023 from the Chair of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 addressed to the President of the General Assembly*, (A/RES/78/16), 13 March, 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/386/76/PDF/N2338676.pdf?OpenElement. and Republic of Belarus et al., *Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, UNODA*, 8 March 2024, 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.

nature of decisions and stricter rules for stakeholder participation. It also provided detailed procedural rules and modalities of work.

The consensus issue was crucial at this substantive session, as many states stressed this in statements. The problem may lie in the 78/16 resolution that does not specify the consensus mode of work except that the mechanism should be 'permanent, inclusive and action-oriented'.

Another divergence between the two formats—the PoA and the OEWG—is the main scope. According to the statements by PoA supporters, ***the PoA should focus on implementing the existing framework of responsible state behaviour in cyberspace and concentrate efforts on capacity building to enable developing countries to cope with that.*** There may be a place for a dialogue on new threats and norms, but this would not be a primary task. ***On the contrary, a permanent OEWG will concentrate on drafting legally binding norms and mechanisms of its implementation as elements of a new treaty or convention on ICT security.*** However, other aspects, such as CBMs and capacity building, will also remain in its scope.

The Chair planned to convene intersessional meetings on regular institutional dialogue in 2024 to deliberate on this issue carefully.

Structural streamlining: The push for a single track process

As discussed in March 2024[205]

In 2024, states were still divided on the issue of regular institutional dialogue. What they agreed on is that there must be a singular process, its establishment must be agreed upon by consensus, and decisions it makes must be made by consensus.

France delivered a presentation on the PoA's future elements and organisation. Review conferences would be convened in the framework of the POA every few years. The scope of these review conferences would include (i) assessing the evolving cyber threat landscape, the results of the initiatives and meetings of the mechanism, (ii) updating the framework as necessary, and (iii) providing strategic direction and mandate or a program of work for the POA's activities. The periodicity would need to be defined as not being a burden to delegations, especially delegations from small countries and developing countries. However, the PoA would need to keep up with the rapid evolution of technology and of the threat landscape.

The PoA would also include open-ended plenary discussions to (i) assess the progress in the implementation of the framework, (ii) take forward any recommendations from these modalities (iii) to discuss ongoing and emerging threats, (iv) to provide guidance for open ended technical meetings and practical initiatives. Inter-sessional meetings could also be convened if necessary.

Furthermore, four modalities would feed discussions on the implementation of the framework: capacity building, voluntary reporting by states, practical initiatives, and

[205] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's seventh substantive session.'

contributions from the multistakeholder community. The POA could leverage existing and potential capacity building efforts in order to increase their visibility, improve their coordination, and support the mobilisation of resources. The review conferences and the discussions would then provide an opportunity to exchange on the ongoing capacity building efforts and identify areas where additional action is needed. Voluntary reporting of states could be based either on creating a new reporting system or by promoting existing mechanisms. The PoA would contain, enable, and deepen practical initiatives. It would build on existing initiatives and develop new ones when necessary. The PoA would enable that engagement and collaboration with the multistakeholder community.[206]

France also noted that a cross-regional paper to build on this proposal will be submitted at the next session.

Multiple delegations expressed support for the PoA, including **the EU**, **the USA**, **the UK**, **Canada**, **Latvia**, **Switzerland**, **Côte d'Ivoire**, **Croatia**, **Belgium**, **Slovakia**, **Czechia**, **Israel**, and **Japan**.

The Russian Federation, ***the country that originally suggested the OEWG, is the biggest proponent of its continuation.*** Russia cautioned against making decisions by a majority in the General Assembly, noting that such an approach will not be met with understanding by member states, first and foremost, developing countries, which long fought to get the opportunity to directly participate in the negotiations process on the principles governing information security. ***Russia stated that after 2025, a permanent OEWG with a decision-making function should be established. Its pillar activity would be crafting legally binding rules, which would serve as elements of a future universal agreement on information security.*** The OEWG would also adapt international law to the ICT sphere. It would strengthen CBMs, launch mechanisms for cooperation, and establish programmes of funds for capacity building. **Belarus**, **Venezuela**, and **Iran** were also in favour of another OEWG.

A number of countries didn't express support for either the PoA or the OEWG but noted some of the elements the future mechanism should have.

Many delegations noted that the future permanent mechanism would have quite a role to play when it comes to implementing and developing the existing framework. **China** noted that the future mechanism should implement the existing framework, but also formulate new norms and facilitate the drafting of legal instruments. The **Arab Group** noted that the future mechanism should develop the existing normative framework to achieve new legally binding norms. **Indonesia** also noted that the mechanism should create rules and norms for a secure and safe cyberspace.

Latvia and **Switzerland** noted that the mechanism must focus on the implementation of the existing framework. However, **Switzerland** and the **Arab Group** noted that the mechanism could identify gaps in the framework and could develop the framework further.

---

[206] Cross-regional group of states, *Proposition de groupes thématiques dédiés pour le Dialogue Institutionnel Régulier (RID) du futur mécanisme – PoA pour examen par l'OEWG* (working paper in French), May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Proposal_of_structure_of_the_RID_future_mechanism_-_PoA_for_consideration_of_the_OEWG_(FR).pdf

South Africa highlighted that discussion on voluntary commitments, such as norms or CBMs, should be developed without prejudice to the possibility of a future legally binding agreement. **The UK** noted that the mechanism should also discuss international law.

Many delegations noted that capacity building must be an integral part of the regular mechanism, such as **South Africa, Bangladesh, the Arab Group, Switzerland, Indonesia,** and **Kenya**.

States also expressed opinions on which topics should be discussed under the permanent mechanism. **Malaysia**, **South Africa**, **Korea**, and **Indonesia** stated that the topics under the mechanism should be broadly similar to those of the OEWG. The **UK**, **Latvia** and **Kenya** stated that it should discuss threats, while **Bangladesh** outlined the following emerging threats: countering disinformation campaigns, including deepfakes, quantum computing, AI-powered hacking, and addressing the use of ICTs for malicious purposes by non-state actors

States also discussed the operational details of the future mechanism. For instance, Egypt suggested that the future mechanism hold biannual meetings every two years, review conferences to be convened every six years, and intersessional meetings or informal working groups that may be decided by consensus. The future mechanism should ensure the operationalisation and review of established cyber tools, including PoC's directory and all other proposals to be adopted by the current OEWG. **Sri Lanka** noted that the sequence of submitting progress reports, be it annual or biennial, should correspond with the term of the Chair and its Bureau.

Brazil ***suggested a moratorium on First Committee resolutions until the end of the OEWG's mandate to allow member states to focus on their efforts in the OEWG.*** This suggestion was supported by **El Salvador, South Africa, Bangladesh,** and **India**.

The future mechanism: Key elements defined

As discussed in July 2024[207]

In July 2024, states met at the eighth substantive session to adopt the group's third APR.[208]

The functions and scope of the future mechanism

The functions and scope of the future mechanism were in the spotlight in July 2024, with countries building a laundry list of wishes.

Russia noted that capacity building should be stipulated to refer to providing assistance to states, not to implementing the framework, which was written in the zero draft of this APR. Similarly, **Nicaragua** and **Iran** noted that there should be a reference to international cooperation and assistance within the mandate of the future mechanism. **Argentina** noted that the future mechanism should be mandated to provide technical assistance, mobilise resources and enable the transfer of technologies.

[207] Gavrilovic, Kazakova, Petit-Siemens, Roellinger, 'OEWG's eight substantive session.'
[208] OEWG 2021–2025 Third Annual Progress Report (APR).

Russia noted that the mandate of the future mechanism should clearly state the intention to create new international norms and the incorporation of already agreed norms into national legislation. Israel highlighted that references to additional binding obligations and developing new norms have not received the necessary consensus. However, **the Netherlands**, **the EU**, **the USA**, and **Switzerland** highlighted that starting with implementing the framework is the best option, as implementation will uncover gaps in the framework that the future mechanism could address at review conferences. **Japan** and **the UK** asked that references to additional legally binding obligations be removed. These countries considered such references to be premature.

The outcome: It was decided that the mechanism would strengthen ICT security capacity for all states, implement and further develop the existing framework for responsible state behaviour in ICT use, address existing and potential threats, and address voluntary norms while recognising that additional norms could be developed over time; study international law's application to ICTs and identify any potential gaps in its application and consider new legally binding obligations if appropriate; and develop and implement confidence-building measures and capacity-building initiatives.

Structure of the mechanism

The concept of establishing thematic groups within the mechanism to allow for deeper discussions was generally welcomed. But, there was no agreement on which themes these groups should tackle. For instance, **Nicaragua**, **Belarus**, and **Cuba** suggested that the thematic groups should follow the thematic areas that the OEWG discusses, as those themes result from previously achieved consensus. **Czechia** preferred thematic groups to focus on specific issues, such as the protection of CI or cyber incident response, while **Belgium** suggested a thematic group on victim assistance.

Some states warned that creating too many thematic groups would be challenging for smaller delegations to participate, making the groups non-inclusive. **Iran** noted that two-week-long substantive sessions would be preferable to ensure all delegations are present.

A number of delegations brought up the possibility of hybrid meetings and a sponsorship programme which would allow smaller delegations to attend meetings.

The outcome: One substantive plenary session, at least a week long, would be held annually to discuss key topics and consider thematic group recommendations. States decided that thematic groups within the mechanism would be established to allow for deeper discussions. The chair may convene intersessional meetings for additional issue-specific discussions. The possibility of some hybrid meetings was included in the APR. The APR does not mention the possibility of a sponsorship programme. A review conference every five years will monitor the mechanism's effectiveness, provide strategic direction, and decide on any modifications by consensus.

Multistakeholder engagement

Another challenging question was the modalities of stakeholder engagement with the mechanism. Some states, such as **the Netherlands**, **the EU**, **Australia**, **the UK**, and **Switzerland**, considered the Ad-hoc committee on cybercrime modalities for

multistakeholder engagement to be the gold standard, where stakeholders attend any open formal sessions of the ad hoc committee, make oral statements (time permitting) after member states' discussions, and submit written statements.[209] Others, like **Russia** and **India**, cautioned that the OEWG's own much-discussed modalities should be applied because they are the hard-won result of a delicate compromise.[210] **The USA**, on the other hand, suggested modalities from the proposed PoA, where state objections to a stakeholder's participation would be subject to transparency and a subsequent vote of all member states to determine whether the prospective stakeholder should be excluded.

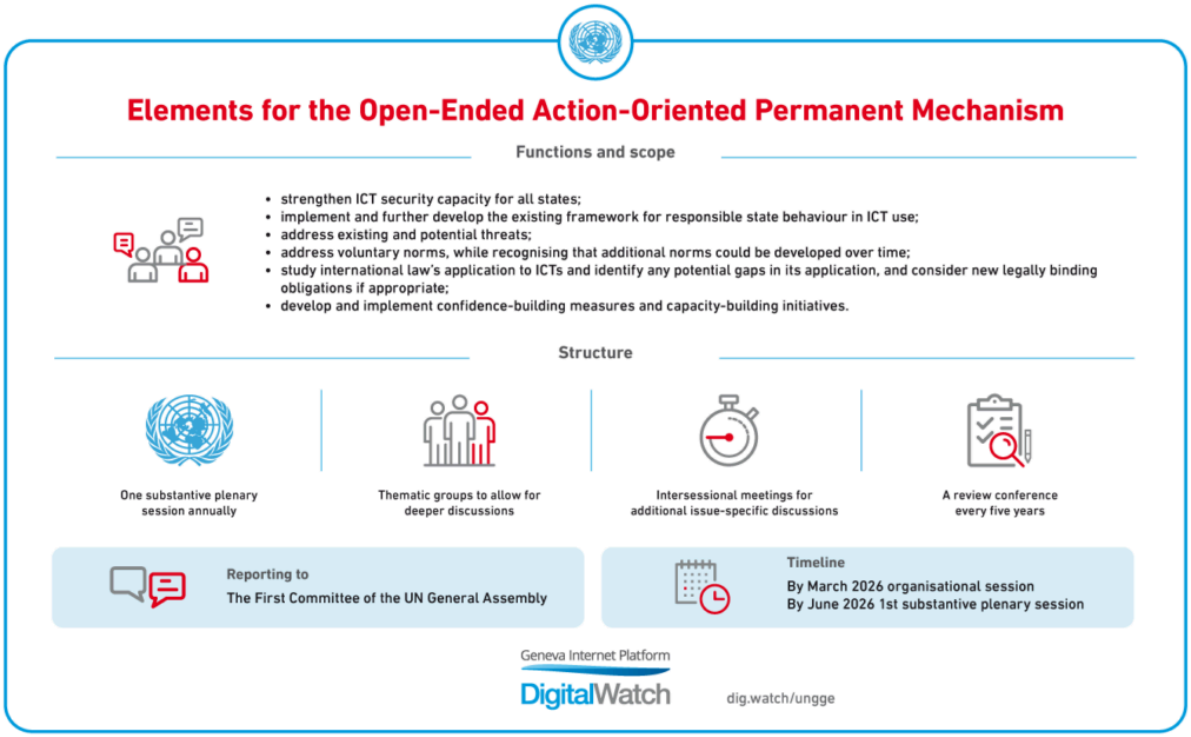
The outcome: This issue was ultimately deferred to the group's next meeting.

The Programme of Action

A number of countries noted that the APR should contain a direct reference to the PoA, considering that it was much discussed in previous and that multiple delegations and groups of delegations submitted papers on its possible elements.

The outcome: The APR does not contain direct references to the PoA. It does, however, acknowledge that the elements for establishing an open-ended action-oriented permanent mechanism on ICT security were formulated by building on the resolution A/RES/78/16 on the programme of action (PoA) on cybersecurity.[211]

[209] United Nations Office on Drugs and Crime (UNODC), Modalities of the Participation of Multi-Stakeholders in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, annex II to document A/AC.291/6, approved by Member States on 14 December 2021, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/Modalities_Stakeholders_AHC.pdf.
[210] Chair, Open-Ended Working Group on ICT Security, Letter dated 22 April 2022.
[211] Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security. Draft resolution, A/C.1/77/L.73, General Assembly First Committee, 13 October 2022, https://digitallibrary.un.org/record/3991743/files/A_C.1_77_L.73-EN.pdf.



Designing the process:Spotlight on thematic groups and multistakeholder participation

As discussed in December 2024[212]

At the December 2024 substantive session, states continued discussing the number and scope of dedicated thematic groups and modalities of stakeholder participation.

Thematic groups in the future mechanism

There was a general divergence between states regarding the scope of thematic groups. **Russia, Cuba, Iran, China,** and **Indonesia** ***insisted on keeping traditional pillars of the OEWG agenda (threats, norms, international law, CBMs and capacity building)***. However, **the EU, Japan, Guatemala, the UK, Thailand, Chile, Argentina, Malaysia, Israel, and Australia** ***advocated for such groups' more cross-cutting and policy-oriented nature.***

France and **Canada** gave suggestions in that vein. **France** suggested creating three groups that would discuss (a) building the resilience of cyber ecosystems and critical infrastructures, (b) cooperation in the management of ICT-related incidents, and (c) prevention of conflict and increasing stability in cyberspace. **Canada** suggested addressing practical policy objectives, such as protecting critical infrastructure and assisting states during a cyber incident, including through focused capacity building. The USA suggested the same two groups and highlighted that the new mechanism should maintain the best of the OEWG format but also allow for more in-depth discussion via the cross-cutting working groups on

[212] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's ninth substantive session.'

specific policy challenges. **Israel** suggested having rotating agendas for thematic groups to keep their number limited.

The chair noted that the pillars could help organise future plenary sessions and that cross-cutting groups do not have to signal the end of pillars.

Some states asked for a dedicated group on the applicability of international law (**Switzerland, Singapore**), but **Australia *objected***. Also, states proposed a ***dedicated group to create a legally binding mechanism*** (**Cuba, Russia, Iran, South Africa, Thailand**).

Multistakeholder participation in the future mechanism

One issue that the OEWG has been struggling with from the start is the modalities of multistakeholder engagement. The extent and nature of stakeholder participation also remained an issue at this session.

The main contention was whether to adopt new modalities of stakeholder engagement, and a few delegations had proposals to that effect. **The EU** called for meaningful stakeholder participation without a veto from a single state. **Canada** proposed an accreditation process for stakeholders while emphasising that states would retain decision-making power. **Mexico** proposed creating a multistakeholder panel to provide inputs on agenda items and suggested considering the UN Convention on Climate Change model for stakeholder participation. **Israel** suggested adopting stakeholder modalities similar to the Ad Hoc Committee on Cybercrime. In contrast, **Iran** and **Russia *argued for maintaining current OEWG modalities***, limiting stakeholder participation to informal, consultative roles on technical matters.

Several questions remain open, the Chair noted. For instance, is there a need for a veto mechanism for stakeholder participation in the future process? If yes, is there a need for an override or screening mechanism? Is there a need for identical modalities for stakeholder participation in different parts of the future process?

As for the timing of meetings, states also expressed concerns that sessions are too lengthy and that attending numerous thematic sessions and intersessionals will be burdensome for small state delegations. The option to turn some of them into hybrid/virtual meetings was also criticised because states miss the opportunity for in-person interaction on-site. Another way to condense all the activities into 2-3 weeks at once also causes problems, as there will be no room for reaching any agreement without properly consulting the capital.

Argentina and **South Korea** asked for **a report on the budget implications** of the specialised groups, other mechanism initiatives, and the secretariats' work.

Finally, **Canada, Egypt, the USA, the Philippines, New Zealand, the UK, Malaysia, Switzerland, Israel, Colombia,** and **Czechia *expressed the wish to dedicate more time to discussing the next mechanism at the beginning of the next substantive session.*** At the same time, **Brazil, Argentina and South Africa** suggested spending the entire February session on this issue.

Disagreements persist: Consensus seemingly distant

As discussed in February 2025[213]

The agenda item on the regular institutional dialogue captured the most attention of the 10th substantive session — more than 60 delegations spoke on this issue. This was not surprising: the OEWG's 2021-2025 mandate would end in less than 6 months, and the Chair still did not have a sense of general consensus on what the future permanent mechanism would be. ***The countries' statements showed that few states are ready to make concessions and be flexible in discussing the modalities of multistakeholder participation in the future permanent mechanism and its architecture.***

As the delegations began to repeat their positions from last year, a sharp intervention from the Chair warned them that there is very little time left until the OEWG's mandate ends. If states do not want to disrupt the process that has been going on for more than 20 years, then they must consider where they can be flexible in their positions.

The Chair also cautioned against equating the future permanent mechanism with the OEWG or the PoA, noting that some participants remain attached to these frameworks. Instead, the future permanent mechanism should be seen as a synthesis of various proposals, including OEWG and PoA elements. The Chair pointed out the high risk of not having a consensus on the future permanent mechanism in the end, and 'the risk is even higher than ever before in this 5-year process'.

The long-running issue of multistakeholder modalities

The problem of stakeholder participation remained the hottest one. Many **European** and **South American states**, as well as **Canada, *put together a joint proposal to make the accreditation a more transparent process with disclosure of the basis for objections, and mechanisms to provide participation to as many stakeholders as possible.***[214] The main principle is 'to have a voice, not a vote'. They argued that stakeholders can serve as experts, especially in thematic groups whose work requires a deeper dive into the issues on the table. Some states advocated for giving the floor to stakeholders during plenaries, too.

On the contrary, **Russia *and other like-minded states insisted on keeping the already agreed-upon OEWG modalities of multistakeholder participation***. The non-objection rule must be in place, and this group of states considered the option to disclose the reasons for objection as a violation of a state's sovereign right. They were also opposed to letting the Chair discuss the accreditation of a particular stakeholder with other states to overcome a veto by voting or any other procedure. Additionally, they don't like that stakeholders who have received objections should be designated as provisional participants.

---

[213] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Roellinger, Stadnik, 'OEWG's tenth substantive session.'

[214] Cross-regional group of states, Practical Modalities to Enable Meaningful Stakeholder Participation in the Future UN Mechanism on Cybersecurity, February 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cross_Regional_Paper_-_Practical_Modalities_to_Enable_Meaningful_Stakeholder_Participation_in_the_Future_UN_Mechanism_on_Cybersecurity_-_Feb_2025.pdf.

Another option was to seek already existing modalities for participation, and states recalled the Ad-hoc committee on Cybercrime, but **Iran** said it was not suitable since it was a temporary body with a specific mandate and limited working period.

The many proposals for thematic groups

The topic that brought the most variation to the discussion was the number and scope of dedicated thematic groups. Some of the proposals were:

- to keep the 'OEWG pillars' structure and have the same groups, but that raised concerns about whether it would duplicate the plenaries.
- to merge some groups and introduce new ones (Chair's proposal)
- to have three thematic cross-cutting thematic groups on resilience, cooperation, and stability (France)
- to have three groups on threat prevention and response, application of IL and existing and future norms and capacity building (the African group of states).

Most states voiced the option to have a special group on capacity building or provide for practical discussions in capacity building across other groups that will be created.

Also, there was a discussion on whether to create a dedicated group on international law or combine international law with norms. This idea was criticised by the **USA**, **Russia**, **Israel**, and **Germany** since it merges two distinct areas of binding and voluntary regulation. **Switzerland** suggested discussing international law as a cross-cutting issue..

Additionally, there were thoughts on creating a dedicated group to prevent conflicts and a dedicated group to critical infrastructure, but they didn't meet a lot of supporters.

As for the French proposal, which was upheld by the **EU member states**, ***the 'cross-cutting policy-issue-focused working groups' would go deeper on each OEWG pillar in a balanced way and then would feed it back into the plenary, which would be structured the same way as the OEWG 2021-2025.***[215]

The Chair intervened in the middle of the discussion, asking the delegates to stop thinking binary: to have either a pillar approach or cross-cutting for the thematic groups and contemplate how to combine them.

Some states, as well as the Chair, reminded that the thematic groups do not have to be cemented immediately, and that shifting agendas could be an option, as well as the creation of ad-hoc ones, and rearrangement of the groups after the first review conference of the future permanent mechanism.

Overall, the general impression was that states are inclined to have three groups rather than five to meet the concerns of smaller delegations.

---

[215] France, *Action-oriented Thematic Groups to Advance Responsible State Behaviour in Cyberspace*, 5 March 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Action_oriented_thematic_groups_(FR)_-_OEWG_working_paper.pdf.

The format of thematic groups: hybrid or in-person

Delegations also expressed concerns about whether the format will be hybrid or in-person only. Both options have advantages, but some states are worried about limited resources for delegations to attend group meetings and plenaries in New York. In contrast, others question whether the hybrid format will be suitable for formal meetings and provide for closer bilateral and group engagements.

At the finish line: Framing the future

As discussed in July 2025[216]

In July 2025, states met at the eleventh substantive session to adopt the group's final report.[217]

Thematic groups: Debating the design

One of the most significant debates during the session centred on the thematic groups to be established under the future mechanism. These groups were originally conceived as a means to allow delegations to deepen discussions on key issues. However, ***countries quickly ran into a stumbling block: how many thematic groups should there be, and what topics should they cover?*** While views varied, the vast majority of states, as well as the Chair, agreed that this was a matter that had to be resolved during this final substantive session of the OEWG. Deferring the decision to the future global mechanism, they warned, would risk unnecessary delays in getting the new process off the ground.

Zero Draft: The starting point for negotiations

Chair's Zero Draft proposal was the basis for the beginning of discussions on this issue. His initial proposal was 3 DTGs:

- The first would focus on action-oriented measures to enhance state resilience and ICT security, protecting critical infrastructure, and promoting cooperative action to address threats in the ICT environment. **(DTG1)**
- The second group would continue the discussions on how international law applies to the use of ICTs in the context of international security. **(DTG2)**
- The third group would address capacity-building in the use of ICTs, with an emphasis on accelerating practical support and convening the Global Roundtable on ICT security capacity-building on a regular basis. **(DTG3)**

This proposal is what the states discussed Monday through Wednesday. A number of states, for instance, **Nigeria**, **Senegal**, **South Africa**, **Thailand**, **Colombia**, **Côte d'Ivoire**, **Indonesia**, **Brazil**, **El Salvador**, **Botswana**. expressed support for the creation of the three proposed DTGs. Some countries suggested minor changes, for example, **Indonesia** suggested that DTG1 can be streamlined to resilience and ICT security of states. **South**

[216] Gavrilovic, Kazakova, Ittelson, Petit-Siemens, Radunovic, Roellinger, 'UN OEWG concludes.'
[217] Digital Watch Observatory, *UN OEWG 2021–2025 Final Report*.

Africa suggested that clearly showing how time will be divided among the group's workstreams in the illustrative timeline would be very helpful.

However, a number of countries were against DTG1. **Nicaragua** noted that the scope and approach of DTG1 are not clear, and that greater discussion is needed. **Iran** similarly noted that the mandate of DTG1 remains vague and overly complex and therefore requires further strengthening and clarification in line with the pillars of the OEWG. **China** cited the use of vague terms like 'resilience' that could undermine the OEWG's agreed framework. **Russia** cautioned that the discussion of the three pillars of the mandate within the same group may be challenging. Russia also stated that norms and CBMs deserve separate groups. **Nicaragua** suggested establishing a separate thematic group on norms. **South Africa** was in favour of a DTG2 that would discuss norms in addition to international law. **Belarus** suggested a thematic group on standards and on CBMs.

DTG2 was much debated. A number of countries were in favour, for various reasons. For instance, **Switzerland** and **Mauritius** noted that such a group should discuss how existing international law applies in cyberspace. **Mexico** highlighted that states need to have a permanent space in which to review, when appropriate, their compatibility with the existing legal framework. **Thailand** noted that this group will enable focused and sustained discussion, including on related capacity building, aimed at bridging legal and technical gaps and promoting more inclusive participation by states on this specialised topic. On the other hand, **Zimbabwe** noted that the DTG could help elaborate a comprehensive legal instrument to codify the applicable rules and principles governing state conduct in cyberspace.

However, various reasons against establishing DTG2 were also brought up. **The EU** emphasised that the OEWG's five pillars are interdependent, and isolating one—such as international law—risks siloed, incoherent outcomes. **Australia**, **Romania** and **Estoni**a echoed this view, arguing that international law should be addressed through cross-cutting DTGs. In **China's** view, DTG 2 undermines the balance between norms and international law.

The **USA** opposed DTG2, citing that some states have already affirmed that they will seek to use conversations in the international law DTG to advance new legally binding obligations contrary to the consensus spirit of the OEWG.

However, seemingly in response, **Egypt** stated that states should not preempt the discussions in DTGs. It stressed that the groups are intended for open dialogue, as has been the practice over the past four years, without any predetermined conclusions. Egypt underlined that, according to Paragraph 15 of the OEWG report, any recommendations emerging from the DTGs will remain draft and subject to consensus-based decision-making.

Much support was expressed for DTG3. **Nigeria**, on behalf of the African Group, said the group would offer a focused platform to strengthen developing countries and bridge the digital gap. **Paraguay** supported a specialised working group to facilitate national efforts in policy development and information exchange. **Mexico** emphasised that the DTG could help develop action-oriented recommendations, map needs and resources, follow up on implementation, coordinate with the global roundtable, and promote diversity and inclusion. **El Salvador** highlighted the importance of the DTG for Central America, noting it should not be limited to financing but also cover technical assistance and knowledge exchange. **Botswana** noted that the DTG will assist states in organising national cybersecurity efforts,

developing policy frameworks, protecting critical and information infrastructures, implementing existing voluntary norms, and formulating national positions on the applicability of international law in cyberspace. Uruguay noted that DTG would go beyond training to identify specific needs and ensure targeted support, allowing for a more comprehensive approach to capacity building.

Indonesia said the group should focus on CBMs, technical training, capacity needs of developing countries, and strengthening initiatives like the Global PoC Directory and the new Global ICT Security Cooperation and Capacity Building Portal. **South Africa** suggested that discussions on CBMs could be placed under this DTG instead of DTG1, if states agreed.

France's detailed proposal for cross-cutting groups was highly regarded by many delegations, such as **Australia**, **the USA**, **Finland**, **Switzerland**, **Italy**, **South Korea**, **Denmark**, **Japan**, **Canada**, **Sweden**, **Romania**, and **Estonia**. This proposal, regarded as an honest bridging proposal, suggested three thematic groups, which would draw on the pillars of the framework for responsible State behaviour in the use of ICT. They would consider, in an integrated, policy-oriented and cross-cutting manner, action-oriented measures to:

- Increase the resilience and ICT security of states, including the protection of critical infrastructure, with a focus on capacity-building in the use of ICTs in the context of international security, and to convene the dedicated Global Roundtable on ICT security capacity-building **(DTG1)**
- Enhance concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment, including to continue the further development and operationalisation of the Global PoC Directory **(DTG2)**
- Promote maintaining peace, security and stability in the ICT environment **(DTG3)**

Australia noted that the proposal explicitly draws on the five pillars of the framework in each dedicated thematic group. **Australia**, **the USA**, **Switzerland**, and **Estonia** noted that the proposal is action-oriented. Per **South Korea**, the proposal would allow for more practical and integrated discussion.

Rev 2: Down to DTG1 and DTG2

However, the Chair's Rev2 brought significant changes to DTGs. It suggested:

- An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to address specific challenges in the sphere of ICT security in the context of international security in order to promote an open, secure, stable, accessible, peaceful, and interoperable ICT environment, with the participation of, inter alia, technical experts and other stakeholders. **(DTG 1)**
- An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to accelerate the delivery of ICT security capacity-building, with the participation of, inter alia, capacity-building experts, practitioners, and other stakeholders. **(DTG 2)**

DTG1 was not met with much enthusiasm. **Ghana** noted that the DTG1 lacks clarity on how the various focus areas will be discussed and effectively distributed within the allocated time frame. **Russia** also noted that it is unclear what exactly the group will work on.

Nicaragua noted that the group's scope is overstretched, while **El Salvador** warned against excessive generalisation of discussions. **Nicaragua** and **Russia** noted the risks of duplication of discussions in the DTG1 and the plenary sessions. **France** and the **USA** regretted the removal of language around cooperation, resilience, and stability.

Delegations made a few suggestions to improve DTG1. **Canada** called for clearer language and a focus on critical infrastructure. **Ghana** suggested that either a clearer framework for the internal distribution of time among the focus areas be established, or the OEWG revert to the three DTGs suggested in Rev1. **Nicaragua** suggested that the OEWG establish the DTG2 on capacity building and defer the decision on other possible DTGs to the organisational session of the future permanent mechanism in March 2026.

A small number of countries, namely **Indonesia**, **Turkiye**, **the Philippines**, **Ukraine**, and **Pakistan,** accepted the new DTG1 as outlined in Rev 2.

A number of countries expressed regret at the removal of the DTG on international law. Among them were **Nigeria** on behalf of the **African Group**, **Egypt**, **Colombia**, **El Salvador**, **Russia**, **Brazil**, and **Mauritius**. However, this group did not make it into the Final report. **Brazil**, for instance, noted that it will be difficult to ensure the meaningful participation of legal experts when the issue of international law is so diluted in DTG 1's overly broad mandate. **Egypt** stated that the group on international law, along with the group on capacity building, were the source of balance vis-a-vis DTG1 and its everything, everywhere, all at once approach. **Tunisia**, on behalf of the Arab Group, noted that it will ask the chair of the mechanism to hold a conference on the application of international law, while **Egypt** was in favour of a roundtable.

DTG2 on capacity building, which was widely supported as DTG3 while countries were still discussing Rev1, wasn't much discussed as it seemed countries were in favour of establishing it. **Canada** called for a clear link and no duplication between the global roundtable on capacity building on capacity building and DTG2. **France** and **Australia** suggested that DTG2 be responsible for organising the global roundtable on capacity building as well as its follow-up. **Costa Rica** emphasised the need to include more operational detail, such as identifying, planning, and implementing capacity building, as well as improving the connection between providers and recipients. However, **Egypt** stressed that without concrete steps—such as establishing a UN-led capacity building vehicle, activating the Voluntary Fund and Sponsorship Program, and ensuring predictable resources—the DTG2 discussions would fall short of their potential and risk undermining the credibility of the new mechanism.

Additional ad hoc groups

Thailand, **Côte d'Ivoire**, **South Africa**, and **Colombia** supported the idea of creating additional ad hoc dedicated thematic groups with a fixed duration to engage in focused discussions on specific issues as necessary, while Iran noted that such groups must be created by consensus. **Australia** opposed ad hoc groups, noting that they could create additional uncertainties and potential burdens for smaller delegations.

The outcome: The final report confirms the establishment of DTG 1 on specific challenges and DTG 2 on capacity building, as outlined in Rev2. The final report acknowledges the possibility of establishing additional ad-hoc dedicated thematic groups.

Multistakeholder engagement in UN cyber dialogue: An old issue persistently on the agenda

Should a state be able to object to an MSH participating in the OEWG? Opinions are divided.

Answer A: Yes, the principle of non-objection must be observed

A group of states is saying YES. **Türkiye**, **Iran**, **Nigeria** on behalf of the **African Group**, **China**, **Zimbabwe**, **Nicaragua**, **Tunisia** on behalf of the **Arab Group**, **Indonesia**, **Egypt**, **Nicaragua**, **Russia**, and **Cuba** advocated for keeping the OEWG 2021-2025 modalities of stakeholder engagement.[218] Per these modalities, ECOSOC-accredited stakeholders may attend formal OEWG meetings without addressing them, speak during a dedicated stakeholder session, and submit written inputs for the OEWG website. Other relevant stakeholders may also apply by providing information on their purpose and activities; they may be invited to participate as observers, subject to a non-objection process. A state may object to the accreditation of specific non-ECOSOC-accredited organisations, and must notify the OEWG Chair that it is objecting. The state may, on a voluntary basis, share with the Chair the general basis of its objections.

Iran supported the proposal made by **Russia** during the town hall consultations to empower the chair and the secretariat of the future permanent mechanism to assess the relevance of ECOSOC-accredited NGOs that have applied to participate in the mechanism and to inform the state of the outcome of such assessment. **Egypt** stated that it does not see merits in the additional consultative layers that will overload the chairperson of the future permanent mechanism without necessarily resolving any potential divergence of views.

China questioned the push for increased NGO participation when member state concerns remain unresolved and highlighted the issue of inappropriate remarks by states, raising doubts about ensuring appropriate NGO contributions.

This group of states does not want experts participating in DTGs. **Russia** and **Nicaragua** noted that the DTGs are to provide a platform for dialogue, specifically for government experts. **Iran** stated that, given that technical experts from states will participate in the thematic groups and will engage in technical rather than political or diplomatic discussions, the expert briefings, as well as the participation of other stakeholders in DTGs, don't offer additional value and could therefore be deleted.

Answer B: No, multistakeholder participation cannot be limited

A group of states is saying NO. Their much different position is outlined in the paper titled 'Practical Modalities for Stakeholders' Participation and Accreditation Future UN Mechanism on Cybersecurity,' co-ordinated by Chile and Canada and supported by 42 states.[219]

This group notes that a state may object to the accreditation of specific non-ECOSOC-accredited organisations. However, the notice of intention to object shall be

[218] Chair, Open-Ended Working Group on ICT Security, Letter dated 22 April 2022
[219] Cross-regional group of states, Practical Modalities to Enable Meaningful Stakeholder Participation in the Future UN Mechanism on Cybersecurity, cross-regional paper, June 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Practical_Modalities_to_Enable_Meaningful_Stakeholder_Participation_in_the_Future_UN_Mechanism_on_Cybersecurity_-_cross-regional_paper_-_June_2025.pdf.

made in writing and include, separately for each organisation, a detailed rationale for such objection(s). One week after the objection period ends, the Secretariat will publish two lists: one of accredited organisations and another of those with objections, including the objecting state(s) and their reasons. These lists will be made public. At the next substantive plenary session, any state that filed an objection may formally oppose the accreditation. If the Chair considers that every effort to reach an agreement by consensus has been exhausted, a majority vote of members present and voting may be held to decide on the contested accreditations, following the Rules of Procedure of the UN General Assembly.

This group has also proposed broader participation rights for stakeholders in the future mechanism. Their proposal includes:

- Allowing stakeholders to deliver oral statements and participate remotely in plenary sessions, thematic groups, and review sessions.
- Permitting non-accredited stakeholders to attend plenary sessions silently.
- Granting the Chair (or Vice Chairs) the authority to organise technical briefings by stakeholders and states during key sessions, ensuring geographic balance and gender parity, and fostering two-way interaction.
- Enabling Chairs (or Vice Chairs) of thematic groups to invite stakeholders to submit written reports, give presentations, and provide other forms of support.

The proposal, its proponents believe, is a fair and practical way to enhance stakeholder participation in the future mechanism by promoting transparency and inclusiveness.

Answer C: Yes, but!

The Chair's proposal tried to bridge these two positions. If a member state objects to accrediting a stakeholder, it must inform the Chair and may voluntarily share the general reason for the objection. The Chair will then consult informally with all member states for up to three months to try to resolve the concern and facilitate accreditation. After the consultations, if a consensus has been reached, the Chair may propose to the Global Mechanism to confirm the accreditation. If consensus is not yet possible, the Chair will continue informal consultations as appropriate. Therefore, this proposal contains the principle of objection, but that can also be revoked.

Accredited stakeholders will be able to attend key sessions, submit written inputs, and deliver oral statements during dedicated stakeholder sessions. They may also speak after member states at substantive plenary sessions and review conferences, time permitting and at the Chair's discretion. The Chair will also hold informal or virtual meetings with stakeholders during intersessional periods. Participation is consultative only—stakeholders would engage in a technical and objective manner, and their contributions 'shall remain apolitical in nature'. Negotiation and decision-making are exclusive prerogatives of member states.

The outcome: The Chair's proposed modalities were adopted as part of the Final report. Nicaragua, Belarus, Venezuela, China, Cuba, Eritrea, Iran, Niger, Russia, Sudan, and Zimbabwe welcomed that accredited stakeholders will participate on a non-objection basis and obtain a solely consultative status, highlighting that the future permanent mechanism is strictly an intergovernmental process.

What's in a name?

Towards the end of the session, another disagreement popped up: the future permanent mechanism's very name.

While France suggested that the future mechanism should 'advance responsible state behavior', a proposal that had quite some proponents, Iran and Russia, for instance, insisted on using 'security of and in the use of ICT', terminology used in the OEWG's name.

The outcome: The division on the name of the future mechanism resulted in its rather unwieldy name: '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'.

Next steps for the mechanism

There is still work to be done before the Global Mechanism actually starts. Singapore will table a simple draft resolution in the First Committee to endorse the OEWG's final report and enable its formal approval by the General Assembly and the Fifth Committee. Emphasising that the resolution should be seen as procedural, not an opportunity to reopen debates, the Chair urged delegations to support a single, unified resolution on ICT security, in line with the agreed single-track process.

The launch of a permanent UN Global Mechanism on cybersecurity will mark a turning point in the international community's decades-long journey toward collective digital security. The agreement to establish a standing mechanism was not inevitable—it is a diplomatic achievement that reflects a shared recognition that cyber-related threats are enduring and require sustained dialogue and cooperation.

For years, states have engaged in time-bound processes, from GGEs to OEWGs, each with limited mandates and uncertain futures. This permanence offers a crucial shift in dynamics. Previous negotiations often operated under the looming question of whether the process would continue at all. Now, with a permanent structure in place, the process may no longer be driven by existential urgency. This could prove to be an advantage. Without the pressure to simply secure the next mandate, states may be freer to engage more deeply with substantive issues.

At the same time, a standing mechanism carries its own risks. Without fixed endpoints or deliverable deadlines, negotiations may lose momentum. States could fall back on well-worn talking points, dragging discussions out over years without reaching new conclusions. The mechanism's success will therefore depend on its ability to maintain relevance, clarity of purpose, and steady progress.

A range of pressing questions remains unanswered. Will the international community build on the existing framework of norms and elaborate additional rules of responsible state behaviour in cyberspace? Will the much-discussed Voluntary Checklist of Practical Actions be formally adopted? Can consensus be reached on the need for a new legally binding instrument—or will this remain a point of division? Furthermore, will the applicability of IHL and IHRL to the cyber context be given the space for serious consideration?

Other practical dimensions also await clarification. Will new CBMs be introduced to deepen trust between states? Can an agreement be reached on a standardised template for communication among national PoCs, a step that could improve transparency and crisis response? How will the work of the dedicated thematic groups be structured to ensure balanced attention across all key topics?

The answers to these questions will shape the trajectory of the new global mechanism. But for now, the fact that such a mechanism exists at all is a step forward. It is an acknowledgement that cybersecurity is not a fleeting concern but a foundational issue in global peace and security—one that demands ongoing, inclusive, and solution-oriented dialogue.

Bibliography

1. African Union (AU). Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace. Adopted by the Peace and Security Council at its 1196th meeting, January 29, 2024. https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y.
2. African Union Peace and Security Council. CAP Communiqués FULL. Adopted at the 1196th meeting, 29 January 2024. African Union. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/CAP_Communiques_FULL_0e34eb5799.pdf.
3. Albania, Argentina, Australia, Austria, Belgium, Bulgaria, Chile, Colombia, Croatia, Cyprus, Czechia, Denmark, Dominican Republic, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Paraguay, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Senegal, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Türkiye, Ukraine, United Kingdom of Great Britain and Northern Ireland, United Republic of Tanzania, and United States of America. Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security. Draft resolution, A/C.1/77/L.73, General Assembly First Committee, 13 October 2022. https://digitallibrary.un.org/record/3991743/files/A_C.1_77_L.73-EN.pdf.
4. Argentina, Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Dominican Republic, Fiji, Germany, Israel, Jordan, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay. Joint Working Paper on Confidence-Building Measures and Capacity Building. April 23, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Working_Paper_CBMs_&_Capacity_Building.pdf
5. Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, Republic of Korea, Mexico, Netherlands, Singapore, and Uruguay. Implementing CBMs Globally: Towards the UN Point of Contact Directory. December 5, 2022. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PoC_Directory_Next_Steps_CBM_joint_group.pdf.
6. Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, the Pacific Island Forum member states, Poland, and South Africa. Joint Proposal for a National Survey of Implementation of UNGA Resolution 70/237. April 16, 2020. https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf.

7. Australia, Colombia, El Salvador, Estonia, and Uruguay. 'Working Paper: Application of international law in the use of ICTs: areas of convergence.' May 30, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-(2021)/240530-Cyber_OEWG-Working_paper_on_the_application_of_international_law_in_the_use_of_ICTs-_submitted_by_a_group_of_States.pdf.
8. Australia, Colombia, El Salvador, Estonia, and Uruguay. Applicability of International Law, in Particular the United Nations Charter, in the Use of ICTs: Areas of Convergence. July 24, 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.
9. Australia, Colombia, El Salvador, Estonia, and Uruguay. Joint Statement on International Law. Delivered at the seventh session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG7_-_Legal_Grouping_-_Joint_Statement_-_Final.pdf.
10. Australian Government. Joint OEWG Proposal: Survey of National Implementation. April 2020. https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf.
11. Brazil, Canada, Chile, Colombia, Czech Republic, Estonia, Germany, Netherlands, Mexico, Republic of Korea, Senegal, Sweden, and Switzerland. Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts. March 1, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations.pdf.
12. Canada and Switzerland. A Practical Approach to International Law in the 2021–2025 Open-Ended Working Group. December 7, 2022. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20221207_Canadian_-_Swiss_Concept_Papier_on_International_law_PPT.pdf
13. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Organizational Note (A/AC.292/2021/CRP.1). May 2021, https://docs.un.org/en/A/AC.292/2021/CRP.1
14. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 15 November 2021. November 15, 2021. https://documents.unoda.org/wp-content/uploads/2021/11/OEWG-2021-2025_Chairs-letter_final.pdf
15. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 17 December 2021, December 17, 2021. https://documents.unoda.org/wp-content/uploads/2021/12/Chairs-letter-17-December-2021.pdf.

16. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 29 May 2024. May 29, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_29_May_2024.pdf.
17. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 12 November 2024 (A/AC.292/2024/5). November 12, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_12_November_2024.pdf
18. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 14 January 2025 (A/AC.292/2025/2). January 14, 2025, https://docs.un.org/en/A/AC.292/2025/2.
19. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 27 January 2025 (A/AC.292/2025/3). 27 January 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_27_January_2025.pdf.
20. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 18 July 2022. July 18, 2022. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/737/71/PDF/N2273771.pdf?OpenElement.
21. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 13 March 2023. March 13, 2023. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/386/76/PDF/N2338676.pdf?OpenElement.
22. Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Letter dated 22 April 2022. April 22, 2022. https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf
23. Cross-Regional Group of States, ‘Proposal on Thematic Groups for the Regular Institutional Dialogue (RID)’. December 6, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/FR_Statement_on_RID_(proposal_on_groups)_ENG.pdf
24. Cross-Regional Group of States. Joint Statement on International Law. July 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG10_-_Joint_statement_on_international_law_-_cross-regional_group_-_final.pdf.

25. Cross-regional group of states. Practical Modalities to Enable Meaningful Stakeholder Participation in the Future UN Mechanism on Cybersecurity. February 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cross_Regional_Paper_-_Practical_Modalities_to_Enable_Meaningful_Stakeholder_Participation_in_the_Future_UN_Mechanism_on_Cybersecurity_-_Feb_2025.pdf.
26. Cross-regional group of states. Practical Modalities to Enable Meaningful Stakeholder Participation in the Future UN Mechanism on Cybersecurity. Cross-regional paper, June 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Practical_Modalities_to_Enable_Meaningful_Stakeholder_Participation_in_the_Future_UN_Mechanism_on_Cybersecurity_-_cross-regional_paper_-_June_2025.pdf.
27. Cross-regional group of states. Proposition de groupes thématiques dédiés pour le Dialogue Institutionnel Régulier (RID) du futur mécanisme – PoA pour examen par l'OEWG. May 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Proposal_of_structure_of_the_RID_future_mechanism_-_PoA_for_consideration_of_the_OEWG_(FR).pdf.
28. Digital Watch Observatory. 'OEWG Chair releases Zero Draft of the final report, setting stage for final talks.' May 26, 2025. https://dig.watch/updates/oewg-chair-releases-zero-draft-of-the-final-report
29. Digital Watch Observatory. 'UN GGE: Quo Vadis?' Digital Watch newsletter – Issue 22 – June 2017. https://dig.watch/newsletter/june2017#UN-GGE-Quo-Vadis-.
30. Digital Watch Observatory. 'UN Group of Governmental Experts and Open-Ended Working Group Processes.' Accessed August 1, 2025. https://dig.watch/processes/un-gge
31. Digital Watch Observatory. 2024. UN OEWG Chair Publishes Discussion Paper on Norms Implementation Checklist. February 21, 2024. https://dig.watch/updates/un-oewg-chair-publishes-discussion-paper-on-norms-implementation-checklist.
32. Digital Watch Observatory. Capacity-building – UN OEWG 2021–2025 (1st Substantive Session). December 16, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/capacity-building
33. Digital Watch Observatory. Conclusions on the UN Security Council's Open Debate on Cybersecurity. June 21, 2024. https://dig.watch/updates/conclusions-on-the-un-security-councils-open-debate-on-cybersecurity
34. Digital Watch Observatory. Modalities of multistakeholder participation. December 13, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation.
35. Digital Watch Observatory. OEWG 2021–2025 First Annual Progress Report (APR). July 2022. https://dig.watch/resource/oewg-2021-2025-first-annual-progress-report-apr.
36. Digital Watch Observatory. OEWG 2021–2025 Second Annual Progress Report (APR). July 2023. https://dig.watch/resource/oewg-2021-2025-second-annual-progress-report-apr.

37. Digital Watch Observatory. OEWG 2021–2025 Third Annual Progress Report (APR). July 2024. https://dig.watch/resource/open-ended-working-group-on-security-of-and-inthe-use-of-information-and-communicationstechnologies-2021-2025
38. Digital Watch Observatory. OEWG Chair releases Zero Draft of the final report, setting stage for final talks. May 26, 2025. https://dig.watch/updates/oewg-chair-releases-zero-draft-of-the-final-report
39. Digital Watch Observatory. OEWG Roundtable on ICT Security Capacity Building. May 10, 2024. https://dig.watch/event/global-roundtable-on-ict-security-capacity-building.
40. Digital Watch Observatory. Resolution on the Programme of Action (PoA) on Cybersecurity Adopted. November 3, 2022. https://dig.watch/updates/resolution-on-the-programme-of-action-poa-on-cybersecurity-adopted.
41. Digital Watch Observatory. The significance of the OEWG POC directory, Digital Watch newsletter – Issue 90 – June 2024. https://dig.watch/newsletters/dw-monthly/digital-watch-newsletter-issue-90-june-2024#PoC
42. Digital Watch Observatory. UN OEWG 2021–2025 – Capacity-building. December 16, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/capacity-building
43. Digital Watch Observatory. UN OEWG 2021–2025 – Confidence building measures (CBMs). December 16, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/confidence-building-measures-cbms.
44. Digital Watch Observatory. UN OEWG 2021–2025 – Existing and potential threats. December 14, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/existing-and-potential-threats
45. Digital Watch Observatory. UN OEWG 2021–2025 – International law. December 14, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/international-law
46. Digital Watch Observatory. UN OEWG 2021–2025 – Regular institutional dialogue. December 17, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue.
47. Digital Watch Observatory. UN OEWG 2021–2025 – Regular institutional dialogue. April 1, 2022. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue.
48. Digital Watch Observatory. UN OEWG 2021–2025 – Rules, Norms, and Principles of Responsible State Behaviour in Cyberspace. December 15, 2021. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/rules-norms-and-principles-of-responsible-behaviour-of-states.
49. Digital Watch Observatory. UN OEWG 2021–2025 – Rules, Norms, and Principles of Responsible State Behaviour in Cyberspace. March 30, 2022. https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-rules-norms-and-principles-of-responsible-state-behaviour-in-cyberspace.

50. Digital Watch Observatory. UN OEWG 2021–2025 Final Report. July 2025. https://dig.watch/resource/oewg-report-2021-2025.
51. Diplo Team. ‘What’s New with Cybersecurity Negotiations: OEWG 2021–2025 Second Substantive Session.’ DiploFoundation Blog, April 25, 2022. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-second-substantive-session/.
52. Diplo Team. ‘What’s new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted.’ DiploFoundation Blog. August 13, 2022. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/
53. European Union (EU). Declaration on a Common Understanding of the Application of International Law to Cyberspace. Approved by the Council on November 18, 2024. https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.
54. France. Action-oriented Thematic Groups to Advance Responsible State Behaviour in Cyberspace. OEWG working paper. March 5, 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Action_oriented_thematic_groups_(FR)_-_OEWG_working_paper.pdf.
55. Gavrilovic, Andrijana, Anastasiya Kazakova, and Salome Petit-Siemens. 2023. ‘What’s new with cybersecurity negotiations? The informal OEWG consultations on capacity building.’ Diplo Foundation Blog, July 24, 2023. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-informal-oewg-consultations-on-capacity-building/.
56. Gavrilovic, Andrijana, Anastasiya Kazakova, Jeanne-Louise Roellinger, Salome Petit-Siemens. ‘OEWG’s eighth substantive session: third progress report adopted, what’s next for ICT discussions?’ Digital Watch Observatory, July 30, 2024. https://dig.watch/updates/oewgs-eighth-substantive-session-the-highlights.
57. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Jeanne-Louise Roellinger, Salome Petit-Siemens and Ilona Stadnik. 'OEWG’s fifth substantive session: The highlights.' Digital Watch Observatory, May 15, 2024. https://dig.watch/updates/oewgs-fifth-substantive-session-the-highlights.
58. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Jeanne-Louise Roellinger, Salome Petit-Siemens and Ilona Stadnik. ‘OEWG’s seventh substantive session: the highlights.’ Digital Watch Observatory, March 28, 2024. https://dig.watch/updates/oewgs-seventh-substantive-session-the-highlights
59. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens and Ilona Stadnik. 'OEWG’s sixth substantive session: The highlights.' Digital Watch Observatory, December 28, 2023. https://dig.watch/updates/oewgs-sixth-substantive-session-the-highlights .
60. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik. 'OEWG’s Ninth Substantive Session: Limited Progress in Discussions.' Digital Watch Observatory, December 30, 2024. https://dig.watch/updates/oewgs-ninth-substantive-session-limited-progress-in-discussions.
61. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Jeanne-Louise Roellinger, and Ilona Stadnik. ‘OEWG’s tenth substantive session: Entering the eleventh hour.’ Digital Watch Observatory, February 27, 2025. https://dig.watch/updates/oewgs-tenth-substantive-session-entering-the-eleventh-hour.

62. Gavrilovic, Andrijana, Anastasiya Kazakova, Pavlina Ittelson, Salome Petit-Siemens, Vladimir Radunovic, Jeanne-Louise Roellinger, 'UN OEWG concludes, paving way for permanent cybersecurity mechanism.' Digital Watch Observatory, July 17, 2025. https://dig.watch/updates/un-oewg-concludes-paving-way-for-permanent-cybersecurity-mechanism.
63. Gavrilovic, Andrijana, Pavlina Ittelson, Vladimir Radunović, Jeanne-Louise Roellinger, Salome Petit-Siemens, and Ilona Stadnik. 'What's new with cybersecurity negotiations? The informal OEWG consultations on CBMs.' DiploFoundation Blog. December 16, 2022. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-informal-oewg-consultations-on-cbms/
64. Gavrilovic, Andrijana, Stefania Grottola, Pavlina Ittelson, Anastasiya Kazakova, Salome Petit-Siemens, Ilona Stadnik. 'What's new with cybersecurity negotiations: OEWG 2021–2025 fourth substantive session'. DiploFoundation Blog. March 23, 2023. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-fourth-substantive-session/
65. Gavrilovic, Andrijana. 'A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers.' Diplo Foundation Blog. March 18, 2021. https://www.diplomacy.edu/blog/new-landmark-global-cybersecurity-negotiations-un-cyber-oewg-in-numbers/.
66. Gavrilovic, Andrijana. 'What's new with cybersecurity negotiations? The UN GGE 2021 Report.' DiploFoundation Blog. June 6, 2021. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/
67. Gavrilovic, Andrijana. 'What's New with Cybersecurity Negotiations? The Second Cyber OEWG's Organisational Session.' DiploFoundation Blog. June 16, 2021. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-second-cyber-oewgs-organisational-session/
68. Global Conference on Cyber Capacity Building (GC3B). The Accra Call for Cyber Resilient Development: An Action Framework. December 2023. https://gc3b.org/wp-content/uploads/2023/12/Accra-Call-Digital-Version_Final.pdf.
69. Global Cyber Security Capacity Centre (GCSCC). 'The Cybersecurity Capacity Maturity Model for Nations (CMM).' Accessed August 1, 2025. https://gcscc.ox.ac.uk/the-cmm.
70. Global Forum on Cyber Expertise (GFCE). Cybil Knowledge Portal. Accessed August 1, 2025. https://thegfce.org/outputs/cybil-knowledge-portal/.
71. India. Working Paper on Global Cyber Security Cooperation Portal (GCSCP) – Rev.1. Open-Ended Working Group on Information and Communication Technologies (OEWG), 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_GCSCP_Rev1_Clean.pdf.
72. India. Working Paper on Global Cyber Security Cooperation Portal. July 2022. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_GCSCP.pdf.

73. India. Working Paper on the Application of International Humanitarian Law to the Use of ICT Operations: Update 2025. July 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/OEWG_Working_Paper_IHL_ICT_Operations_Update_2025.pdf.
74. International Conference of the Red Cross and Red Crescent. 'Resolution: Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict.' 34th International Conference of the Red Cross and Red Crescent. October 2024. https://rcrcconference.org/app/uploads/2024/11/34IC_R2-ICT-EN.pdf.
75. Joint Contribution by Argentina, Australia, Canada, Chile, Colombia, Estonia, Germany, Japan, the Netherlands, New Zealand, Norway, the Republic of Korea, and the United Kingdom. The Future of Discussions on ICTs and Cybersecurity at the United Nations. October 8, 2020. https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.
76. Kenya. Draft Working Paper on the Establishment of a Threat Repository within the United Nations. May 22, 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated22May23_Kenya_Draft_Working_Paper_Threat_Repository.pdf.
77. Kuwait. Module for Rules, Norms, and Principles within the Global ICT Security Cooperation and Capacity-Building Portal (GCSCP). March 7, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/KUWAIT_PROPOSAL%28%22%28GCSCP%29_Module_for_rules_norms_and_principle%29_-_final.pdf.
78. Multistakeholder group. Letter for the OEWG Chair on Modalities. December 2021. https://documents.unoda.org/wp-content/uploads/2021/12/Multi-Stakeholder-Letter-for-OEWG-Chair-on-Modalities-.pdf.
79. OEWG Secretariat. Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal. 14 January 2025. https://docs.un.org/en/A/AC.292/2025/1.
80. Organization for Security and Co-operation in Europe (OSCE). 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures. Vienna: OSCE Secretariat, October 2023. https://www.osce.org/files/f/documents/f/7/555999_1.pdf.
81. Pacific Islands Forum countries (Australia, Fiji, Kiribati, Federated States of Micronesia, Marshall Islands, Nauru, New Zealand, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu). Statement on the Application of International Law to the Use of ICTs. Delivered at the Ninth Session of the Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025. December 4, 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PIF_Statement_OEWG_ICTS_Int_Law.

82. Republic of Belarus, Burkina Faso, Burundi, Cuba, Democratic People's Republic of Korea, Eritrea, Mali, Myanmar, Nicaragua, Russian Federation, Syrian Arab Republic, Sudan, Bolivarian Republic of Venezuela, and Zimbabwe. Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies. March 8, 2024. 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.
83. Republic of Korea Ministry of Foreign Affairs. 2024. 'Statement at the Security Open Debate on Cyber Security (Foreign Minister Cho Tae-yul).' June 20, 2024. https://overseas.mofa.go.kr/un-en/brd/m_26611/view.do?seq=158.
84. Russian Federation. Concept of work of the UN Open-ended Working Group on security of and in the use of information and communications technologies submitted by Russian Federation. June 1, 2021. https://documents.unoda.org/wp-content/uploads/2021/06/Concept-paper-on-the-New-OEWG-ENG.pdf
85. Russian Federation. Statement by the Russian Interagency Delegation on the Adoption of the Final OEWG Report. 11 July 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/Russia_-_OEWG_-_Adoption_of_the_final_report_-_ENG.pdf
86. Russian Federation. Updated concept of the convention of the United Nations on ensuring international information security. April 2023. 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.
87. Russian Federation and co-sponsors (Republic of Belarus; Republic of Nicaragua). Concept Paper of the Russian Federation on Establishing a Regular Institutional Dialogue on Security of and in the Use of ICTs under UN Auspices. Working paper submitted to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, February 21, 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Regular_institutional__dialogue_Proposal_of_the_Russian_Federation.pdf.
88. Russian Federation and like-minded states. Concept of a UN Convention on Ensuring International Information Security. April 2023. 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.
89. Russian Federation and like-minded States. Concept of a UN Convention on Ensuring International Information Security. April 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

90. Russian Federation. Updated concept of a UN Convention on International Information Security. May 15, 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.
91. The Phillipines. Needs-Based Cyber Capacity-Building Catalog: A Philippine Proposal. July 2022. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/WP_on_CB_Cyber_Catalog.pdf.
92. UNIDIR. Inaugural Global Roundtable on ICT Security Capacity Building: Recap and Key Highlights. May 16, 2024. https://unidir.org/inaugural-global-roundtable-on-ict-security-capacity-building-recap-and-key-highlights/.
93. United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/75/240). Adopted December 30 2020. https://dig.watch/resource/developments-field-information-and-telecommunications-context-international-security
94. United Nations General Assembly. Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/RES/73/266). Adopted 5 December 2018. https://dig.watch/resource/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international.
95. United Nations General Assembly. Countering the Use of Information and Communications Technologies for Criminal Purposes. A/75/L.87/Rev.1. May 24, 2021. https://undocs.org/en/A/75/L.87/Rev.1.
96. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/53/70). Adopted January 4, 1999. https://undocs.org/en/A/RES/53/70.
97. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. (A/RES/65/41). Adopted 8 December 2010. Accessed August 5, 2025. https://dig.watch/resource/un-gge-report-2010-res-a65201.
98. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/68/243). Adopted 9 December 2013, accessed August 5, 2025. https://dig.watch/resource/un-gge-report-2013-a6898.
99. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security, (A/RES/70/174.) Adopted 8 December 2015. Accessed August 5, 2025. https://dig.watch/resource/2015-un-gge-report-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-a-res-70-174.
100. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security (A/AC.290/2021/CRP.2). Adopted December 16, 2021. https://dig.watch/resource/oewg-2021-report.
101. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. (A/RES/75/240). March 30, 2021. https://docs.un.org/en/A/RES/75/240.

102. United Nations General Assembly. Establishment of the UN Open-Ended Working Group on Cybersecurity. (A/RES/73/27). Adopted 5 December 2018. https://dig.watch/resource/un-ga-resolution-establishment-oewg-ares7327.
103. United Nations Institute for Disarmament Research (UNIDIR). Cyber Policy Portal. Accessed July 27, 2025. https://cyberpolicyportal.org/en/.
104. United Nations Institute for Disarmament Research. UNIDIR PoC preliminary results v3, December 2022. UNIDIR. Accessed 23 July 2025. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNIDIR_POC_preliminary_results_v3_dec2022_0.pdf
105. United Nations Office for Disarmament Affairs. Preliminary overview of State inputs on PoC directory: OEWG intersessional, December 2022. 5 December 2022. Accessed 23 July 2025. UNODA. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Preliminary_overview_of_State_inputs_on_PoC_directory_OEWG_intersessional_Dec_2022.pdf
106. United Nations Office on Drugs and Crime (UNODC). Modalities of the Participation of Multi-Stakeholders in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Annex II to document A/AC.291/6. Approved by Member States on 14 December 2021. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/Modalities_Stakeholders_AHC.pdf.
107. United Nations. Charter of the United Nations: Repertory of Practice—Article 51. Codification Division, Office of Legal Affairs. Accessed August 5, 2025. https://legal.un.org/repertory/art51.shtml.
108. United Nations. Letter dated 31 January 2022 from the Chair Designate of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. January 31, 2022. https://documents.unoda.org/wp-content/uploads/2022/02/2022-01-31-Letter-from-the-Chair-Designate_organizational-matters_enclosures.pdf.
109. World Bank. Cybersecurity Multi-Donor Trust Fund. Accessed August 1, 2025. https://www.worldbank.org/en/programs/cybersecurity-trust-fund.

ISBN 979-8-9898028-1-4

diplomacy.edu