UNIDIR

REPORT

Towards a regular institutional dialogue on international ICT security

Review of current proposals and considerations for effective dialogue

SECURITY AND TECHNOLOGY PROGRAMME

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. Work of the Security and Technology Programme on international cybersecurity is funded by the Governments of Australia, Canada, Czechia, France, Germany, Italy, the Netherlands, Norway, Singapore, Switzerland and by Microsoft.

About UNIDIR

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

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

This report was produced by **UNIDIR Security and Technology Programme**. Pavel Mráz, Andraz Kastelic and Giacomo Persi Paoli drafted the report; Samuele Dominioni, Lenka Filipová and Dominique Steinbrecher contributed to this report.

Abbreviations

AI	Artificial Intelligence
CBMs	Confidence-building measures
ECOSOC	Economic and Social Council
GGE	Group of Governmental Experts
ICT	Information and communication technology
OEWG	Open-ended Working Group
UNODA	United Nations Office for Disarmament Affairs

Contents

Executive summary

The purpose of this paper is to provide an overview of key areas pertinent to the establishment of a future permanent United Nations mechanism on international security aspects of information and communication technologies (ICTs). It aims to facilitate discussions by identifying areas of convergence and divergence among states regarding the purpose, objectives, guiding principles, scope, structure, and modalities of this future regular institutional dialogue. By drawing on relevant General Assembly resolutions, past consensus reports, and states' views and submissions, the paper seeks to outline potential pathways towards establishing a fit-for-purpose, single-track, and flexible regular institutional dialogue that meets states' aspirations and remains effective in face of evolving ICT challenges.

The initial version of this paper was developed as a food-for-thought document to support discussions among state representatives during UNIDIR workshop on future permanent mechanism convened in June 2024. This workshop aimed to explore existing proposals for establishing a regular institutional dialogue on international ICT security under United Nations auspices and to facilitate in-depth discussions around existing options for a future permanent mechanism.

Following the UNIDIR workshop, an updated version of the paper was shared with delegates ahead of the 8th substantive session of the Open-ended Working Group (OEWG) in July 2024, where formal deliberations on establishing a permanent mechanism on ICT security took place. In this session, states recommend the establishment of the future permanent mechanism based on the consensus elements contained in the paper entitled "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security", appended to the 2024 OEWG Third Annual Progress Report as Annex C.

This research paper highlights both the initial areas of convergence and divergence ahead of the July OEWG session as well as the latest consensus elements adopted by states, as contained in Annex C of the OEWG's Third Annual Progress Report (A/79/214). Additionally, this paper also includes an Appendix Summary Report of the June 2024 UNIDIR workshop, which outlines recurring themes, areas of agreement, and various insights and recommendations shared by participants.

The paper's main findings highlight significant areas of convergence as well as some remaining divergences among states. In particular, there is broad agreement on the regular institutional dialogue's primary objective of promoting international peace and security in cyberspace, its structure, and its guiding principles of inclusivity, flexibility, transparency, sustainability, complementarity, and non-duplication. However, some divergences remain regarding its precise modalities, thematic groups, and programmatic priorities. Specific issues such as the regular institutional dialogue's name, prioritization and sequencing of its activities, as well as operationalization of its guiding principles may also require further dialogue. Addressing these remaining divergences with the function of this permanent mechanism in mind will be crucial for designing a sustainable and effective regular institutional dialogue that can enhance international cooperation and strengthen global ICT security over time.

1. Introduction and context

In 1999, the United Nations General Assembly unanimously expressed concern about the potential **misuse of information and communication technologies (ICTs) to undermine international peace** and security. Since then, several time-bound multilateral processes, including Groups of Governmental Experts (GGEs) and Open-ended Working Groups (OEWGs), have been convened to address ICT-related issues in the context of international security. These processes have yielded valuable outcomes, including the evolving and cumulative United Nations framework for responsible state behaviour in cyberspace.

With the second OEWG set to conclude its work in 2025, there is a **universally recognized need for states' deliberations on international ICT security to continue** in a regular institutional dialogue (thereafter referred to as a "future mechanism" or simply "mechanism" in this paper) established under the auspices of the United Nations. Resolutions such as 75/240, 77/37 and 78/16 as well as consensus reports of the 2019–2021 GGE and both OEWGs have laid the groundwork for further action and deliberations on the establishment of such a mechanism.

Discussions within the OEWG and submissions from states highlight both the significant progress made to date and some of the challenges that lie ahead in establishing a future United Nations mechanism on ICT security. Notably, over the past three years, **states' views have converged around several foundational elements** of the future mechanism, including its general purpose, scope, guiding principles and structure.[1] However, a review of existing proposals, written submissions and discussions to date also indicates that there remain some diverging views among states. In particular, states are yet to build consensus around the specific modalities, thematic groups and programmatic priorities of this mechanism.

This **framing paper aims to provide an overview of key areas pertinent to the establishment** of a future United Nations mechanism on ICT security. It covers the purpose and objectives (in Section 2), guiding principles (Section 3), scope and function (Section 4), structure (Section 5), and modalities (Section 6) of this mechanism. The paper draws on relevant General Assembly resolutions, consensus reports of the past OEWGs and GGEs, reports of the Secretary-General, and the views and submissions of states. It is hoped that by **identifying both areas where states' views converge and areas where they diverge** on the subject, this framing paper can facilitate discussions on potential pathways towards a consensus establishment of a fit-for-purpose, single-track and flexible mechanism that fulfils states' aspirations and remains effective over time.

2. Purpose and objectives

For the purposes of this paper, **"objectives" refer to the broader goals** that states hope to achieve via a future permanent mechanism. These can include advancing the implementation and further development of the framework or the development and operationalization of additional confidence-building measures. Relatedly, **"functions" in this paper refer to specific programmatic activities** that would be undertaken within the mechanism to support the attainment of agreed objectives. To advance implementation, those functions could include voluntary reporting, mapping challenges faced by states when implementing the framework, identifying good practices and solutions to support national implementation efforts, conducting framework gap analysis, or exchanging lessons learned.

Over the years, views have progressively converged on the purpose of the future mechanism, which should act as a **permanent**[2] **intergovernmental forum for United Nations action on international aspects of ICT security**.[3] The primary objective of a mechanism would be to promote international peace, security and stability in the ICT environment[4] by advancing the evolving and cumulative framework[5] for responsible state behaviour in cyberspace in an action-oriented manner.[6] Latest proposals submitted by groups of states suggest that, in addition to a deliberative role, the future mechanism would also undertake decision-making,[7] coordination and facilitation.[8]

Table 1. Summary of the proposed objectives for the future mechanism

Several objectives have been proposed for the future mechanism, including:

- Coordination of capacity-building[9]
- Advancing the implementation and further development of the framework for responsible state behaviour in cyberspace
- Developing and operationalizing additional confidence-building measures (CBMs)
- Advancing discussions on international law[10]
- Negotiating additional commitments

While these objectives are identified in a number of submissions, states may have diverging views on their prioritization and appropriate sequencing.

Although there has been significant convergence in states' views on the broad purpose and objective of the future mechanism over the past few years,[11] written submissions indicate **several areas where consensus is yet to emerge**. These include the mechanism's name, primary goals and specific objectives, and the potential prioritization and sequencing of its programmatic activities (see Table 2). Specifically, several names have been proposed, including the "Programme of Action"[12] and the "Permanent Decision-Making OEWG" and combinations thereof.[13]

Table 2. Purpose and objectives of a future mechanism: areas of convergence and divergence

CONVERGENCE	DIVERGENCE
Advancing responsible state behaviour in the use of ICTs in an action-oriented manner	The primary goals and specific objectives to be achieved
A permanent forum for United Nations discussions on international ICT security	The name
Strengthening international security and stability in the ICT environment	The specific programmatic priorities and their sequencing

In United Nations practice, **subsidiary bodies of the General Assembly may take on many forms and names**.[14] Such bodies may include Commissions, Committees, Councils, Programmes of Actions, Open-ended Working Groups and Working Groups, Forums, Open-ended Informal Consultative Processes and Task Forces pursuing various objectives.[15] Historically, all of the above bodies have been associated with distinct functions within the United Nations system. States may therefore wish to further discuss and define specific functions of this mechanism before deciding on the most appropriate name. Furthermore, the broadly shared aspiration for an action-oriented mechanism may require further discussions among states in order to define in greater detail its expected outcomes as well as specific programmatic activities that will be undertaken to arrive at such outcomes.

In terms of the prioritization and sequencing of individual objectives, states may consider where they wish to pursue multiple programmatic priorities simultaneously and where a sequential approach – one where programmatic activities flow from and organically build on one another – is more desirable. **Identifying specific cross-thematic policy objectives – across all pillars of the framework** consisting of norms, international law,[16] CBMs and capacity-building – and means of achieving them may provide a useful foundation for states' consideration of other aspects of the mechanism. This would include questions such as how to design a fit-for-purpose institutional architecture and specific modalities to ensure that the form of the future mechanism follows its desired function.

Table 3. Purpose and objectives agreed by states in the OEWG third annual progress report

Purpose

- Establish of a future permanent mechanism that will be open-ended and action-oriented in nature and would take as the foundation of its work the consensus agreements on the framework of responsible State behavior in the use of ICTs from previous OEWG and GGE reports.
- Facilitate integrated, policy-oriented and cross-cutting discussions on ICT security.

Objectives

- Continue to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment.
- Strengthen the ICT security capacity of all States.

3. Guiding principles

States' discussions on the establishment of the future mechanism have **converged around several guiding principles deemed essential for its effective functioning**.[17] These include inclusivity, flexibility, transparency, sustainability, complementarity and non-duplication.[18] These principles have been frequently invoked as foundational values that should underpin the design, operation and decision-making processes of the mechanism. Specifically, **inclusivity** is often cited as the openness of a mechanism to all Member States of the United Nations and all relevant stakeholders.[19] While this principle is not widely contested, states may wish to consider how to enshrine this aspiration in the modalities of the mechanism (see Section 6 for details). **Flexibility** is understood to reflect the shared aspiration of states to allow the permanent mechanism to evolve over time.[20] **Complementarity** is often cited in the context of ensuring that the mechanism would be a single-track process,[21] would not duplicate existing efforts and would act in coordination with other relevant United Nations processes.[22] Finally, **sustainability** is also widely supported by states as a foundational principle, although it remains relatively undefined.[23] Further discussions concerning this principle may be needed, particularly as the number of meetings, review cycles, working groups and programmatic activities proposed for this mechanism would likely require substantial financial support.

While the aforementioned principles are not contested, **states may have diverging views on how they would be operationalized in practice** (see Table 4 for a summary). Additionally, states may wish to clarify the extent and the manner in which the mechanism could accommodate additional principles mentioned across various proposals, such as sovereignty, non-interference and peaceful settlement of disputes.[24] Similarly, states may wish to discuss how best to mainstream the capacity-building principles adopted by the final report of the 2019–2021 OEWG, including gender-sensitivity and human rights, in the work of the future mechanism.[25]

Table 4. Guiding principles of a future mechanism: areas of convergence and divergence

CONVERGENCE	DIVERGENCE
Principles of inclusivity, flexibility, complementarity, and sustainability	How these principles would be operationalized in practice
Promotion of trust and cooperation among states	Substantive principles the mechanism could support, such as sovereignty, non-interference or human rights

Given the lack of clarity around these foundational principles, states may also wish to consider how the principles of inclusivity, flexibility, transparency, sustainability, complementarity and non-duplication would be translated into concrete modalities of the mechanism (which are addressed in Section 6). For example, in terms of inclusivity, states may consider how to define 'relevant stakeholders' (e.g., by elaborating guidelines) and how to encourage participation of capital-based experts from developing countries (e.g., through a voluntarily funded sponsorship programme).[26] States may also wish to **discuss and clarify the process through which the framework would evolve**, and whether such evolution would require further approval by the General Assembly. Finally, while the principle of complementarity and non-duplication is widely accepted, practical questions arise as to how such coordination could take place and which United Nations processes and organizations would be most relevant in this regard.

Table 5. Guiding principles agreed by states in the OEWG third annual progress report

Guiding Principles
• The mechanism would be a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee of the United Nations General Assembly. • It would be an open, inclusive, transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and developments in the ICT environment.

4. Scope and function

Related to the convergence around its guiding principles, there is **broad consensus among states on the scope and some functions of the future mechanism**. In terms of scope, states broadly agree that the mechanism should focus on advancing the framework across its pillars (See Table 6).

Table 6. Summary of proposals covering the scope and main functions of a future mechanism

A number of written submissions reference the **following areas in relation to the proposed scope** of the future mechanism:

- Identifying ICT threats[27]
- Supporting the implementation of the existing framework[28] across norms, international law[29] and CBMs[30]
- Strengthening capacity-building through practical action[31]
- Further developing the cumulative and evolving framework, where appropriate.[32]

Additionally, **several concrete functions** of the mechanism have been proposed. These include:

- Mapping specific needs and challenges faced by states[33] when implementing the framework[34]
- Identifying good practices and solutions to support national implementation efforts[35]
- Conducting voluntary reporting[36] and framework gap analysis across norms and international law[37]
- Exchanging lessons learned
- Elaborating threat-mitigation and incident-response measures
- Establishing international attribution mechanism
- Strengthening communication channels and elaborating procedures for de-escalation in the event of ICT incidents
- Mobilizing and pairing available resources with requests for capacity-building support[38]
- Negotiating additional commitments to increase international cooperation on ICT security.[39]

Many proposals also assume that the mechanism would report back to the General Assembly on its work at regular intervals in line with the established practice of past OEWGs and GGEs.[40] While proposals reference most, if not all, of the above functions in some form or another, written submissions tend to **prioritize different functions, such as mapping implementation challenges versus negotiating additional legally binding commitments**.[41] Proposals also assign varying levels of importance to different pillars of the framework: that is, norms, CBMs, capacity-building and international law. This varied emphasis also translates into diverging views as to the appropriate sequencing of various activities and the prioritization of specific tasks undertaken within the mechanism (see Table 7 for a summary).

Table 7. Scope and function of a future mechanism: areas of convergence and divergence

CONVERGENCE	DIVERGENCE
Identifying challenges related to upholding and evolving the framework and proposing solutions, including via General Assembly reporting requirements	The specific tasks and activities undertaken within the mechanism
Providing practical support for framework implementation and capacity-building efforts	The mechanism's role in implementation and development of the framework across norms and international law

To bridge these divergences, states may wish to identify how many priority activities they wish to undertake via this mechanism. For example, designing **a mechanism with a broad scope and with a structure that decouples various thematic areas and programmatic activities** from one another (e.g., by establishing dedicated thematic committees and programmatic working groups for each activity) may be desirable if states wish to tackle many activities that require participation of capital-level experts with different types of expertise. Such an institutional architecture may also be useful to safeguard against institutional gridlock by ensuring that a lack of progress in one area does not result in a permanent deadlock of the mechanism.

Alternatively, if states wish to undertake fewer activities that link a large number of issues, then they may choose to establish **a mechanism with a narrower and more focused scope with a streamlined structure and a narrow set of objectives**. Such mechanisms can be permanent, but more frequently they have a time-limited mandate and cease to exist once the set objectives are achieved. A third, **hybrid option might involve establishing a permanent mechanism with a broad scope alongside dedicated time-bound subsidiary organs** mandated to accomplish specific tasks.[42]

To build consensus around which option may be more appropriate, states may wish to first identify specific functions of the mechanism and then discuss which should be undertaken on a permanent basis and which could be more appropriately achieved in a time-bound manner. States may also wish to **consider the appropriate sequencing of the proposed programmatic activities** and the extent to which these activities should be linked, decoupled or built upon one another within the mechanism. These considerations may also inform states' preferences for the structure of the future mechanism, which is addressed in the next section.

Table 8. Scope and functions functions agreed by states in the OEWG third annual progress report

Scope

- Address the issue of ICT security in the context of international security, including existing and potential threats; voluntary, non-binding norms of responsible State behaviour; international law; confidence-building measures; and capacity-building.

Functions

- Develop and implement the cumulative and evolving framework for responsible State behaviour in the use of ICTs.
- Continue to study how international law applies in the use of ICTs and 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.
- Develop and implement confidence-building measures.
- Develop and implement capacity building, including action-oriented approaches such as matching needs with resources and technical assistance.
- Facilitate the continued operationalization and further development of all existing initiatives set up under the auspices of the OEWG 2021–2025 and/or other previous processes, including, *inter alia*, the Global POC Directory and the Global Roundtable on ICT security capacity-building.

5. Structure

There is an **emerging consensus around several elements** of the institutional structure of the future mechanism. First, states broadly agree on the need to continue plenary discussions in line with the existing OEWG practice.[43] Additionally, the possibility of **establishing subsidiary groups** to facilitate technical exchanges and in-depth consideration of specific programmatic issues (e.g., capacity-building, international law[44] or critical infrastructure protection[45]) has also been broadly acknowledged.[46] Various proposals also identify the United Nations Office for Disarmament Affairs (UNODA) as the appropriate Secretariat for this mechanism.[47] Many proposals also reference the need for periodic high-level review meetings to examine the state of implementation, assess the evolving threat landscape, identify priority actions and provide political guidance on a way forward.[48]

The **remaining divergences mostly relate to the frequency of meetings**, the number of layers within the mechanism (i.e., a two- or a three-tier structure), its location and the level of detail regarding its leadership (see Table 9).[49] Additionally, while all contributions propose a review process, there are **some divergences as to how often such reviews should occur**.[50] For example, some proposals include a three-tier structure composed of review conferences held every 4–6 years, biannual plenaries and intersessionally convened technical working groups.[51] In contrast, other proposals, while also calling for biannual plenaries and the potential establishment of subsidiary bodies, suggest progress reports could be adopted every two years.[52] While some proposals do not elaborate in detail on the leadership element of the future mechanism, other proposals include more details, such as the establishment of a regionally representative Bureau led by a Chair with a two-year mandate.[53]

Table 9. Structure of a future mechanism: areas of convergence and divergence

CONVERGENCE	DIVERGENCE
Plenaries and subsidiary groups for specific thematic areas	The number of institutional layers within the mechanism
UNODA acting as a Secretariat	The level of detail regarding intergovernmental leadership and the process of its appointment
Periodic high-level meetings to review thee framework and decide on next steps	The scope, nature and frequency of reviews conducted within the mechanism

The resolution of these outstanding issues relates to states' expectations regarding the function of the future mechanism. For example, if states wish to allocate more time and resources to high-level political discussions on international aspects of ICT security, they may opt for fewer institutional layers, more plenary meetings and frequently negotiated progress reports. Alternatively, if states prefer to advance discussions on ICT security at the technical level, it may then be desirable to increase the number of institutional layers as well as the frequency of intersessional meetings between formal plenary sessions where dedicated subject-matter experts from capitals can participate,[54] while increasing the time between high-level political reviews.

Table 10. Structure agreed by states in the OEWG third annual progress report

Structure
• Five-year cycle consisting of two biennial cycles followed by a one-year review cycle. • Review conference convened every fifth year to review functioning, provide strategic direction to plenary sessions and thematic groups and modify elements of the mechanism. • One substantive plenary session per year of at least one week to carry out discussions and to consider the work and recommendations of thematic groups. • Thematic groups would be established as required to undertake focussed discussions and to report updates and recommendations to substantive plenary sessions. • Intersessional Meetings convened by the Chair to discuss specific issues, reports, and recommendations as necessary. • UNODA to serve as the Secretariat of the permanent mechanism. • Formal meetings convened at the UN Headquarters in New York. • Chair elected to serve for a period of two years (one year during the review cycle) on the basis of equitable geographical representation.

6. Modalities

Unless states otherwise specify, as a subsidiary body of the General Assembly,[55] the General Assembly's Rules of Procedure would govern all operational and procedural aspects of the future mechanism. These rules would notably regulate the mechanism's membership (i.e., opening it to all Member States), decision-making (i.e., simple majority voting) and modalities for stakeholder participation (i.e., non-governmental organizations accredited to the Economic and Social Council (ECOSOC)). However, as highlighted above, **states have converged around key principles for this mechanism, including its "inclusivity" and "consensus-driven" nature** (see Table 11 for a summary).[56] Operationalizing these principles in practice would require adjustment of the mechanism's modalities. This could be done in the General Assembly resolution that establishes the mechanism, in a follow-up resolution on modalities or via a dedicated preparatory process.

In terms of inclusivity, states have converged around the need for the future mechanism to remain open to all United Nations Member States and to engage with civil society, the private sector and academia.[57] While these elements are not contested, there is an ongoing debate[58] as to the most appropriate modality[59] for stakeholder participation to balance the principle of inclusivity with the need to safeguard the intergovernmental decision-making of the mechanism. Another element that has been suggested to increase the inclusiveness of the mechanism is a potential sponsorship travel fund composed of voluntary contributions to support the attendance at relevant meetings by capital-based experts from developing countries.[60]

In terms of decision-making, the preference for a consensus-driven mechanism enjoys universal support. [61] However, it remains to be clarified whether states prefer the **"rule of consensus"** as the only means of making all procedural and substantive decisions, or whether the **"principle of consensus"**, which may imply potential fallback options (e.g., simple or two-thirds majority voting), is to be written into the mechanism. Such fallback options are sometimes used to guard against institutional paralysis by providing alternative means to resolve potential deadlocks over procedural issues (e.g., election of officers) or even issues of substance (e.g., framework review).[62] Furthermore, states may also wish to clarify whether the same decision-making modality would also apply to the process of its establishment when, for example, a dedicated preparatory conference is convened to advance the mechanism's establishment.[63]

Table 11. Modalities of a future mechanism: areas of convergence and divergence

CONVERGENCE	DIVERGENCE
Strong preference for a consensus-based decision-making modality	The rule or the principle of consensus and its application
An inclusive mechanism open to all United Nations Member States	The means of support for participation of capital-based experts from developing countries
Engagement with relevant stakeholders, where appropriate	The means of inclusion of stakeholders without ECOSOC accreditation

While all current proposals acknowledge the potential role of stakeholders, there are diverging views on the extent of their involvement and the nature of their participation in the mechanism's activities.[64] While no proposal assumes direct stakeholder participation in decision-making, states envision **different degrees of engagement and consultations with relevant stakeholders**, such as the private sector, academia and civil society.[65] To build further convergence around this issue, states may wish to clarify which stakeholders are relevant for which objectives, and where in the process and structure of the mechanism such stakeholders can most meaningfully support state deliberations (e.g., study groups, plenaries, review process, etc.). This would allow states to design a fit-for-purpose modality centred around their needs (See Table 12 for non-exhaustive list of options).

Table 12. Non-exhaustive list of options for stakeholder inclusion and engagement

To facilitate engagement with and the inclusion of relevant stakeholders, states may wish to seek inspiration in the modalities and existing practices of other international organizations and processes. This could include:

- **Adopting clear and objectively applied guidelines** and criteria for the admission of stakeholders.
- **Delegating the responsibility for stakeholder accreditation** to a state where the stakeholder entity is domiciled or registered.
- **Adopting a gradual approach to stakeholder inclusion** starting with more limited involvement in initial stages and gradually expanding participation over time.
- **Inviting stakeholders on an ad hoc basis as briefers** under the discretionary authority of the Chair and working group Vice Chairs.
- **Designing flexible modalities for stakeholder engagement** by establishing multiple channels for inputs, such as advisory groups, task forces and thematic consultations with a wide range of stakeholders.

In July 2024, States agreed by consensus on several elements relevant to the modalities and the process of establishment of the future mechanism (see table 13 below). Importantly, states have agreed to continue discussions within the current OEWG and to submit recommendations in the Final Report of the OEWG to be adopted in July 2025 on modalities on the participation of other interested parties and stakeholders, including businesses, non-governmental organizations and academia, in the future permanent mechanism.

Table 13. Modalities agreed by states in the OEWG third annual progress report

Modalities

- The permanent mechanism to be established as a subsidiary body of UNGA reporting to the First Committee.
- The permanent mechanism would take all decisions based on the principle of consensus.
- Plenary sessions, thematic groups, and intersessional meetings will not be held in parallel.
- Possibility of some meetings held in a hybrid format.
- An e-portal and/or website to be established to facilitate the mechanism's work.
- The Global POC Directory to serve as a voluntary standing tool for use by States.

Stakeholder Participation

- The permanent mechanism would promote engagement and cooperation with interested parties and stakeholders, including businesses, non-governmental organizations and academia. This participation will be guided by the following principles:
  - **Inclusive discussions drawing on relevant expertise** to support the work of the mechanism;
  - **Opportunities for consultations with stakeholders** within plenary sessions, thematic groups, intersessional meetings and review conferences;
  - **Permanent mechanism to remain a state-led process** with negotiations and decisions remaining the prerogative of states.

Process of Establishment

7. Conclusion

In the light of the rapid advancement of information and communication technologies and the accompanying challenges to international stability and security, the establishment of a permanent United Nations mechanism on ICT security is both timely and essential. The deliberations in the United Nations and the proposals to date highlight a **significant convergence of views on key foundational elements**, many of which are captured in Annex C of the OEWG Third Annual Progress Report titled "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security".[56] These elements include agreement on the need for a permanent, consensus-driven and action-oriented mechanism as well as its objectives, scope, general functions, and institutional structure. The guiding principles of inclusivity, flexibility, complementarity and sustainability are now also formally adopted, providing a strong foundation for further elaborating the institutional design and fit-for-purpose modalities of this future mechanism.

Furthermore, the **latest proposals consistently emphasize the importance of practical cooperation**, engaging relevant stakeholders and ensuring transparent processes. Additionally, they stress the need to align the work of the future mechanism with existing multilateral agreements on international law and norms on state use of ICT while **working towards both the implementation and further development of the framework**, where appropriate, to respond to the evolving ICT threat landscape.

Most divergences centre around issues such as the name of the mechanism and which programmatic activities should be prioritized over others, rather than around the mechanism's structural design. The remaining differences – particularly those regarding structure, modalities, and prioritization among and sequencing of the proposed programmatic priorities – underscore the importance of continued dialogue of states' expectations and needs in relation to the future mechanism. Key considerations include the frequency of informal meetings, concrete policy priorities and thematic focus of future working groups, and modalities for stakeholder participation. Addressing these issues while taking into account the desired functions of the mechanism will ensure that it can deliver on states' expectations and remains relevant in the face of the evolving ICT threat landscape.

Ultimately, the success and long-term viability of a permanent United Nations mechanism on ICT security will depend on finding a balance between high-level political discussions and technical exchanges. By **building on the areas of convergence and by including, by design, discussions on areas of divergence in the new mechanism**, states can establish a sustainable mechanism capable of enhancing international cooperation and strengthening global ICT security over time while minimizing the risk of institutional gridlocks. This collective effort will not only advance responsible state behaviour in cyberspace but will also contribute to a more open, peaceful, secure and stable ICT environment for all.

Towards a regular institutional dialogue on international ICT security

Appendix: Workshop Summary Report

SECURITY AND TECHNOLOGY PROGRAMME

Contents

Introduction and context

On 14 June 2024, UNIDIR, with the co-sponsorships of governments of Brazil and France, convened a one-day closed-door workshop with government officials representing a diverse, cross-regional group of countries. The workshop's primary goal was to further discuss existing proposals for establishing a regular institutional dialogue under United Nations auspices on international aspects of the security of information and communications technology (ICT).

With the second Open-ended Working Group (OEWG) set to conclude its work in 2025, there is a **universally recognized need for states' deliberations on international ICT security to continue** in a new mechanism established under the auspices of the United Nations. Discussions within the OEWG and submissions from states highlight both the significant progress made to date and some of the challenges that lie ahead in establishing a future United Nations mechanism on ICT security.

The **UNIDIR workshop aimed to complement the OEWG deliberations on a permanent mechanism by facilitating informal exchanges of existing and novel ideas** on the subject matter, thereby contributing to transparency and confidence-building among states. Participants were provided with detailed scenarios, guiding questions and a UNIDIR framing paper outlining areas of convergence and divergence in states' discussions to date.

Due to logistical constraints, **UNIDIR was only able to convene a workshop with a limited number of participants**. To ensure an interactive discussion among a diverse cross-regional group of states, UNIDIR encouraged participation of representatives from governments with a publicly stated position on the future mechanism on international ICT security. This included states that had made at least one dedicated intervention at the OEWG about regular institutional dialogue at the 6th or the 7th substantive session, at a dedicated March 2024 OEWG informal "town hall" meeting on regular institutional dialogue, at the May 2024 OEWG intersessional meetings, or states that have contributed to a dedicated report of the UN Secretary-General (A/78/76). These logistical constraints notwithstanding, the conveners of this workshop acknowledge the importance of ensuring an inclusive discussion on the topic of regular institutional dialogue and shall endeavour to repeat this exercise with a more representative group of states and stakeholders in the future to further validate the findings contained in this report.

Throughout the event, **participants engaged in in-depth, focused and scenario-based discussions on how this mechanism could advance international aspects of ICT security**. These discussions focused on ICT threats, the implementation and development of norms, advancement of international law, confidence-building measures (CBMs), and capacity-building.

This report provides a summary of discussions from the workshop, highlighting recurring themes, areas of convergence, as well as proposals, insights and observations expressed by participants during the discussions. The findings presented in this report are representative only of the discussion held among those state representatives that participated in this UNIDIR workshop. While they reflect views of a diverse cross-regional group of states, they do not necessarily represent the perspectives and preferences of the entire UN Membership; different participation base may produce different results.

1. Key highlights

Many workshop participants acknowledged that deliberations on setting up a permanent mechanism on international aspects of ICT security at the United Nations are occurring in a complex geopolitical environment. Despite this, there was a consensus that current circumstances should not limit the ambitions for the future mechanism. Some participants emphasized that the challenges of today should not hinder the design of a mechanism for the future that is fit for its purpose and flexible. Crises will pass, but a well-designed mechanism should persist and remain relevant beyond a particular set of circumstances.

There was a strong call for a mechanism that allows for discussions on all aspects of the framework of responsible state behaviour in cyberspace. It could thus combine technical or thematic discussions in working groups that could inform high-level political discussions in regular plenaries and identify possible gaps and limitations to be discussed at review meetings. This structure would provide strategic direction to the mechanism, but also allow for in-depth exchanges among technical experts. Several participants also expressed a wish for the mechanism to engage with relevant stakeholders while preserving the intergovernmental nature of all decisions that it makes. Many participants hoped the new mechanism would establish subsidiary bodies (i.e., working groups) to drive discussions forward in a more concrete and action-oriented manner.

Many participants also agreed that the existing separation of discussions into thematic pillars, as seen in the Groups of Government Experts (GGEs) and Open-ended Working Groups (OEWGs), may need to be reconsidered in the light of the interconnectedness of ICT challenges. Recent instances of malicious ICT activities have shown the complexity and difficulty of discussing existing pillars – composed of threats, norms, international law, CBMs and capacity-building – separately. A mechanism that enables discussions to explore topics both in isolation as well as their interconnections was broadly welcomed.

Table 1. Summary of key hightlights

Challenging geopolitical environment:

- A high level of ambition is needed, and the current complex environment should not deter states from the creation of a fit-for-purpose and flexible mechanism to meet future needs.

Mechanism structure:

- These was broad agreement on the need for a mechanism that combines technical and thematic discussions in working groups with high-level plenaries and review meetings to provide strategic direction.
- A mechanism allowing interconnected discussions across different pillars may be desirable.

Inclusive mechanism:

- The mechanism should engage relevant stakeholders appropriately while preserving the inter-governmental nature of decisions.
- Exploration of practical ways to encourage participation of technical experts, particularly from developing countries, may be desirable.

Subsidiary bodies:

- The establishment of subsidiary bodies (i.e., working groups) to drive concrete, action-oriented outcomes was broadly supported.

2. Cross-cutting observations from breakout groups

Prompted by the pre-prepared scenarios, participants engaged in in-depth group discussions on the specific objectives and functions that the future mechanism could pursue across ICT threats, norms, international law, CBMs and capacity-building. Over the course of breakout group discussions, many participants identified three cross-cutting objectives that the mechanism should contribute to: (a) prevention of ICT incidents, (b) de-escalation and cooperation, and (c) long-term ICT threat mitigation.

Preventive functions of the mechanism could include sharing information on ICT threats and good practices to counter them as well as support for capacity building and implementation of the framework. Such functions would ensure that all states are in a better position to prevent ICT incidents like those discussed in the breakout sessions. When prevention fails and ICT incidents do occur, the future mechanism could use the existing Global Points of Contacts Directory as a platform for rapid information sharing. This could de-escalate tensions, avoid misperceptions and promote international cooperation to restore functionality of ICT resources and services. Finally, in the aftermath of ICT incidents, through the exchange of good practices, lessons learned, and facilitation of capacity-building and mutual learning, the mechanism should contribute to mitigating the risk of ICT incidents over time, thereby increasing cyber resilience of all.

Table 2. Possible objectives of the mechanism

Prevention & preparedness:

- The mechanism could ensure that states can prevent ICT incidents effectively through capacity-building, sharing information on ICT threats and good practices to counter them.

De-escalation & cooperation:

- When prevention fails, the mechanism could provide a platform for de-escalation and international cooperation making use of the existing Global Points of Contacts Directory.

Cyber resilience & mutual learning:

- The mechanism could contribute to incident mitigation through the exchange of good practices, lessons learned and capacity-building.

To achieve these objectives, many participants concluded that there needs to be a permanent platform within the mechanism that allows for reflection on past ICT incidents, existing and evolving threats, and possible future threats. Such a platform could also consider how these incidents and threats impact on and relate to the United Nations framework of responsible state behaviour in cyberspace. Furthermore, some participants concluded that, in order to facilitate knowledge-building and capacity-building, the mechanism may need to incorporate several key features to be effective over time, as outlined in the next section.

3. Possible features of the future mechanism

The breakout groups identified several possible key features for the new mechanism. First, many participants emphasized that the **mechanism should enable cross-sectoral discussions**, acknowledging that it is difficult to address different elements of the framework in isolation. For example, a dedicated group for critical infrastructure protection could be established to consider this issue across various pillars of the framework. This could mean examining the evolving ICT threats facing critical infrastructure; applicable critical infrastructure norms and their implementation; existing international law applicable in specific contexts; CBMs that can be used to exchange information and de-escalate possible tensions stemming from ICT incidents targeting critical infrastructure; and identifying specific capacity-building activities to boost cyber resilience of critical infrastructure.

Second, **flexibility and adaptability were emphasized as essential features of the mechanism** given the evolving ICT threat landscape, technological advancements, geopolitical challenges and context-specific implementation issues. Most participants also called for the mechanism to include a thorough review process to allow states to determine whether identified challenges indicate simply problems in implementation or, rather, gaps in the existing normative framework. Relatedly, such review could identify policy responses to address specific challenges. For instance, if evidence shows that artificial intelligence (AI) and machine learning systems are increasingly used to drive malicious use of ICTs to undermine international security, states could assess whether the existing framework remains fit-for-purpose and decide on appropriate measures, perhaps pertaining to implementation, capacity-building or the development of new rules.

Third, **inclusiveness was often cited as a key feature of the new mechanism**, indicating the need to ensure participation of states and engagement with relevant stakeholders. While states should own the process, stakeholders may have crucial knowledge in key areas of the mandate of the new mechanism, such as in mapping new and emerging threats. Several participants also highlighted the need for a broadly accessible and inclusive mechanism to facilitate the participation of capital-based experts with diverse expertise. Additionally, the involvement of technology providers and critical infrastructure operators in the implementation of norms was mentioned. Establishment of a voluntarily funded trust fund was suggested to support the participation of capital-level technical experts from developing countries.

Many **participants also called for a robust stakeholder inclusion within the new mechanism** to ensure that states can benefit from expertise that may reside elsewhere. Several ideas and options were proposed on how to include non-governmental entities that are not accredited with the UN Economic and Social Council in the new mechanism. These proposals ranged from deciding on admission of stakeholders by consensus to using a simple majority vote or a silent procedure to accredit stakeholders. Other options included elaboration of guidelines for admission of stakeholders or allowing states to decide on the appropriateness of participation of stakeholders under their jurisdiction or sovereignty. Some participants expressed a view that states should be the only interlocutors in formal discussions, while stakeholders could participate in informal discussions. In working group meetings, the chair or vice-chair could decide which stakeholders might deliver briefings and on what subjects.

Fourth, many participants expressed a desire for the mechanism to **bring together political and technical communities of practice**. Some participants suggested political discussions could occur in New York, while technical discussions could be held in dedicated informal working groups convened in Geneva and/or by host countries on voluntary basis across different regions. This would leverage existing expertise and avoid duplication of efforts while promoting a cross-regional ownership of the new mechanism. Ensuring that technical capital-level expertise is involved in meetings was deemed crucial by many to facilitate inclusive, expert-based and depoliticized discussions, from which all states – and developing states in particular – can benefit.

Participants also broadly agreed that the **structure of the mechanism could include working groups** that communicate their recommendations to the plenary. To promote collective ownership of the mechanism, working group discussions could be held in Geneva, in locations where specific expertise exists, in developing countries or across different regions. These groups should communicate among themselves and with the plenary on a regular basis to ensure synergies and avoid duplication or contradictory outcomes. Discretion to allow the chairs and vice-chairs to structure the work of their working groups and decide on briefings from specific stakeholders was also emphasized.

Table 3. Possible features of the future mechanism

Cross-sectoral discussions:

- The mechanism could enable discussions on interconnected aspects of ICT security (e.g., the protection of critical infrastructure) across various pillars of the framework.

Flexibility and adaptability:

- The mechanism could be adaptable to evolving threats, technology and geopolitics, with a review element to consider whether issues are purely implementation challenges or reveal gaps in the framework.

Inclusiveness:

- The mechanism could involve states and relevant stakeholders, ensuring that the technical community is included to depoliticize contentious issues and drive progress.
- Hybrid participation options should be available.

Bridging political and technical expertise:

- Political and technical discussions could inform and enrich one another, with political discussions in New York and technical discussions in Geneva or regional settings.

Structure and modalities:

- Informal working groups could be established to communicate recommendations to the plenary.
- Stakeholder participation rules could vary depending on the discussion level (working groups versus plenary) and type (formal versus informal).

4. Possible functions of the future mechanism

The workshop participants discussed specific functions of the mechanism, across threats, norms, international law, CBMs and capacity-building.

In **scenario-based discussion on threats**, some participants proposed that the mechanism could develop templates and protocols for incident reporting and a threat repository. It may be necessary to engage practitioners with knowledge on ICT threats, particularly from the private sector and academia, to inform deliberations by states. The subject of threats was deemed to be complex enough to require dedicated working group discussions. It was also suggested that discussions on threats should serve specific policy goals, such as increasing resilience, cooperation, prevention and stability in the ICT environment.

The mechanism **could also have a dedicated process to recognize new threats and initiate a framework review** when necessary. For example, the increasing use of AI in malicious cyber activities was cited as one example that could potentially prompt the development of additional rules, such as those related to data security. The growing threat of cybercrime and ransomware and their increasing impact on national security and international peace and stability was also cited as one potential area that could be addressed via the new mechanism. To avoid duplication, such discussions could remain coordinated with efforts of the United Nations Office on Drugs and Crime (UNODC).

On norms, there was general agreement that the mechanism should strengthen the framework of responsible state behaviour in cyberspace. This could involve elaborating additional guidance and driving implementation of existing norms through dedicated working groups and task forces. Voluntary reporting was cited as a promising function of the mechanism, which would inform states' decisions to revise the framework and develop additional norms, when appropriate. Establishment of a dedicated working group to build an organic link between studies on ICT threats and discussions on norms was recommended. Some participants proposed establishing dedicated task forces for each of the 11 norms of responsible state behaviour to study implementation good practices, potential gaps and lessons learned in detail for each norm separately.

For international law, most participants broadly agreed that a dedicated working group could be created to advance multilateral deliberations on how international law applies to state use of ICTs. This group could study potential gaps in international law and consider the appropriateness of negotiating additional legally binding obligations. Some participants suggested focusing on the implementation of existing commitments first, then considering the development of new legally binding rules. Other participants believed that these efforts could proceed in parallel. Another view expressed was that the mechanism should balance implementation and development requirements, acting as a platform for sharing national positions and supporting states in developing their positions on how international law

applies and what additional measures may be needed. Discussions on new technologies, emerging threats, new actors to be regulated by international law and potential gaps could also be considered. Scenario-based discussions, perhaps modelled on those convened by UNIDIR, were suggested by some participants as a means to build convergence among legal experts on specific issues over time.

In terms of capacity-building, the mechanism should support and encourage investment in cyber capacity-building to drive the implementation of the existing normative framework across all its pillars. Capacity-building should be demand-driven and aligned with principles outlined by the first OEWG, with stakeholders playing a role as providers of assistance. Identifying national capacity-building needs of states on a continuous basis through voluntary self-reporting was recommended and widely accepted. A dedicated working group for capacity-building could perform various functions, such as identifying needs and resources, with the United Nations Office for Disarmament Affairs (UNODA) potentially coordinating matchmaking between offers of and demands for capacity-building.

Many participants also agreed that **capacity-building is a cross-cutting issue and should be mainstreamed into all other working groups**, such as those on threats, international law and critical infrastructure protection. It was also suggested that the future mechanism should create synergies with other United Nations initiatives and initiatives of other stakeholders (including digital transformation initiatives) and should build on the achievements and consensus outcomes of previous programmes.

Finally, several participants proposed that the mechanism could develop guidelines for CBM implementation, share good practices from implementation of regional CBMs, and establish a platform for practitioners to interact and share experiences. Multiple references were made to the "Adopt a CBM" approach of the Organization for Security and Co-operation in Europe (OSCE), which encourages state ownership and greater collaboration in developing and implementing CBMs. Some participants suggested establishing a CBM working group on facilitating cooperation in the event of a serious ICT incident. This group could enhance the effectiveness of the Points of Contacts Directory, ensuring quick and coordinated responses in the event of major ICT incidents with spill-over effects. A proposal was also made to compile a list of regional CBMs to determine which ones could be transposed and operationalized at the global level via the new mechanism. The global Points of Contact Directory, adopted by the last annual progress report of the OEWG, was widely recognized as a useful and simple tool, and some participants called for its structure and implementation to remain straightforward. The role of regional organizations in the mechanism was emphasized, highlighting the need to maintain a link between global and regional confidence-building efforts. Finally, since there are divergent views and approaches on the topic of attribution, it was proposed that the **mechanism should leave room to discuss attribution in order to build confidence around public attribution practices**.

Table 4. Possible functions of the future mechanism

Threats:

- The mechanism could develop incident-reporting templates and protocols and a threat repository.
- State deliberations could be informed by practitioners, including from the private sector and academia.

Norms:

- The framework of responsible state behaviour could be strengthened through additional guidance, voluntary reporting and further development, where appropriate.
- There could be an organic link between the study of ICT threats and the discussion of norms.

International law:

- A dedicated working group could advance discussions on international law in state use of ICTs.
- Implementation and development of new rules could take place in parallel.

Capacity-building:

- The mechanism could support demand-driven capacity-building efforts aligned with OEWG principles.
- A working group could identify needs and resources, with a possible match-making role for offers of and requests for capacity-building.

Confidence-building measures:

- The mechanism could develop practical guidelines for CBM implementation and should share good practices.
- Cooperation in the event of serious ICT incidents could be facilitated and connected with regional efforts.
- Relevant regional CBMs could be adopted at the global level.

Overall, while many proposed functions were broadly acceptable to participants, there were **differences among states regarding prioritization and sequencing of specific activities**. Some states prioritize implementing existing norms and the operationalization of CBMs, while others advocated for developing new rules and norms. Some workshop participants suggested that implementation and the development of new rules could proceed in parallel, with the mechanism facilitating balanced discussions.

5. Summary of concluding plenary session

In the concluding plenary session, participants reflected on the significant progress made during the workshop. Many participants felt that the **workshop's alternation between plenary discussions and scenario-based deep dive discussions** in smaller working groups helped advance concrete discussions and, in the process, helped clarify where divergences still exist. Some participants observed that a similar model could also advance discussions in a future mechanism.

Many participants noted there was a **considerable convergence on the structure of the permanent mechanism, its need for cross-cutting discussions and its functions**. There was a notable convergence of views around the need to institutionalize cross-cutting consideration of the existing pillars of the framework, rather than maintaining divisions between norms, law, CBMs and capacity-building. Several participants expressed hope that the additional areas of convergence identified over the course of this workshop would be reflected in the upcoming annual progress report of the OEWG. Some participants cautioned that more discussions are needed but committed to working closely together to find the right balance between existing positions.

Overall, the workshop underscored significant convergence of views on establishing a single-track, action-oriented and flexible permanent mechanism on international aspects of ICT security. The discussions brought participants closer to consensus, demonstrating the **effectiveness of such dialogues in advancing discussions** on a future of regular institutional dialogue on ICT security.

Endnotes

1 See, for example, OEWG 2021–2025, 2nd Annual Progress Report, A/78/265, 1 August 2023, https://undocs.org/A/78/265, paragraphs 55, 56, and 57.

2 "Other principles identified by States in their submissions included, inter alia, permanence, … States noted that the permanence of a programme of action structure would provide for institutional stability and save the General Assembly time and resources in negotiating new mandates." General Assembly, "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security", Report of the Secretary-General, A/78/76, 18 April 2023, https://undocs.org/A/78/76, paragraph 16.

3 "Given the fast pace of technology development and the constant emergency of new threats, the future mechanism should have broad mandate to cover different relevant aspects of international security related to the ICTs." OEWG 2021–2025, "Brazil's Views on the Future Regular Institutional Dialogue on Information and Communication Technology in the Context of International Security", Submission by Brazil, 23 April 2023, thttps://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Brazil-_EN--_website.pdf, paragraph 6.

4 "The aim of the future mechanism would be to continue to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment". OEWG 2021–2025, A/78/265, paragraph 55(b).

5 "The future mechanism would take as the foundation of its work the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports;" OEWG 2021–2025, A/78/265, paragraph 55(c).

6 "The permanent mechanism will be open-ended and action-oriented in nature". OEWG 2021–2025, "Draft Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security", Submission by the Chair, 1 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_1_May_2024_0.pdf, paragraph 1.

7 See, for example, OEWG 2021–2025, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the use of Information and Communications Technologies", Submitted by the Russian Federation on behalf of a group of states, 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.

8 "Some States expressed the desire for regular dialogue to prioritize implementation of existing commitments and recommendations, including developing guidance to support and monitor their implementation; coordinating and strengthening the effectiveness of capacity-building; and identifying and exchanging good practices. Other States expressed the desire for regular dialogue to prioritize the further development of existing commitments and elaboration of additional commitments, including the negotiation of a legally binding instrument and the institutional structures to support it." OEWG 2019–2021, Third Substantive Session, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf, paragraph 40.

9 "PoA could leverage existing and potential capacity-building efforts, increase their visibility and improve their coordination". OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

10 "States stated that the programme of action could offer an inclusive framework for further discussion on applicability of international law to the use of information and communications technologies by States and deepen common understandings on this topic, including through a dedicated workstream." Report of the Secretary-General, A/78/76, paragraph 29.

11 For example, the 2nd Annual Progress Report of the OEWG 2021–2025 outlines the purpose and objective of the future mechanism as an "open-ended action-oriented permanent mechanism … to further develop and implement the cumulative and evolving framework for responsible State behaviour in the use of ICTs and to strengthen the capacity of all States." OEWG 2021–2025, A/78/265, paragraph 55.

12 See, for example, OEWG 2021–2025, 'Proposal on the Structure of the Future Mechanism for Regular Institutional Dialogue on Cyber Issues', Submitted by a cross-regional group of states, 17 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_cross-regional_working_paper_-_Future_UN_cyber_mechanism_for_2025_onward-vf_0.pdf; and OEWG 2021–2025, "Working Paper for a Programme of Action (PoA) to Advance Responsible State Behavior in the Use of ICTs in the Context of International Security", Submitted by a group of states, 1 December 2023, https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

13 See Annex C in the 3rd Annual Progress Report of the OEWG 2021–2025 titled "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security." OEWG 2021–2025, A/79/214, Annex C.

14 For an overview see General Assembly, "Subsidiary Organs of the General Assembly", https://www.un.org/en/ga/about/subsidiary/index.shtml.

15 The 2nd Annual Progress Report of the OEWG 2021– 2025 acknowledges that several names were proposed: "Further to the recommendation in the 2021 OEWG report and in the first [Annual Progress Report] of the OEWG, States deepened discussions on the proposal to establish a Programme of Action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security. Other proposals were made for regular institutional dialogue, including a proposal for a future group, commission, committee or conference under the auspices of the United Nations." OEWG 2021–2025, A/78/265, paragraph 52(c).

16 For example, a working paper by a group of states proposes that a future RID could include "sharing national views, including regional, sub-regional as well as national statements on how international law applies in the use of ICTs, dedicated meetings, expert briefings, scenario-based discussions, and capacity building on international law via dedicated thematic working groups and/or technical meetings". OEWG 2021–2025, "Programme of Action (PoA) and International Law", Working Paper by Chile, Estonia, Fiji, Japan and the United Kingdom, 14 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PoA_and_International_Law_OEWG_Working_Paper_May_2024.pdf, p. 2.

17 It would be an open, inclusive, transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environment." OEWG 2021–2025, A/78/265, paragraph 55(d).

18 "States also expressed the desire for the international community to ultimately return to a single consensus-based process under UN auspices," OEWG 2019–2021, Third Substantive Session, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf, paragraph 43.

19 For example, according to a concept paper, it may be "useful to enable interaction of the permanent OEWG with relevant regional organizations and associations". OEWG 2021–2025, Concept paper submitted by a group of states, p. 3.

20 "The mechanism should be permanent and flexible, fit to adapt its work in the face of new technological developments and emerging threats." OEWG 2021–2025, Submission by Brazil, paragraph 5.

21 "It would be a single-track, State-led, permanent mechanism under the auspices of the United Nations." OEWG 2021–2025, A/78/265, paragraph 55(a).

22 For example, a concept paper calls for "avoiding duplication of international efforts aimed at ensuring security of and in the use of ICTs within different negotiating platforms"; and a working paper states that "the PoA would act as complementary and coordinated with other relevant UN processes [and] is not intended, nor designed to duplicate or replace any other negotiation format." OEWG 2021–2025, Concept paper submitted by a group of states, p. 2; OEWG 2021–2025, "Working Paper for a Programme of Action (PoA)", p. 4.

23 "Regarding the dedicated trust fund, several States reflected on examples provided by existing mechanisms under the United Nations in the area of arms control, such as the United Nations Trust Facility Supporting Cooperation on Arms Regulation and the Saving Lives Entity fund. States noted other existing funding structures such as the World Bank Cybersecurity Multi-Donor Trust Fund and those at the regional and subregional levels." Report of the Secretary-General, A/78/76, paragraph 20.

24 For example, a concept paper states that "the work of the future permanent OEWG should be based on the following principles: … compliance with the principles of the UN Charter (sovereign equality of States, non-use of force or threat of force, peaceful settlement of international disputes)". OEWG 2021–2025, Concept paper submitted by a group of states, p. 2.

25 "Many States emphasized that capacity-building should represent a central programme of action function. A number of States recalled the consensus guidelines for capacity-building agreed in the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." Report of the Secretary-General, A/78/76, paragraph 31.

26 "States in a position to do so to continue to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant UN processes." OEWG 2021–2025, A/78/265, paragraph 36.

27 "States identified various functions and activities under a future programme of action, including those related to exchange of information, inter alia, on existing and potential threats and how to address them." Report of the Secretary-General, A/78/76, paragraph 27. Related proposals were made by Kenya for a threat repository and by India for a global cyber security portal. OEWG, 2021–2025, "Draft Working Paper on the Establishment of a Threat Repository within the United Nations", Submitted by Kenya, 18 July 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated18July23Kenya_Draft_Working_Paper_Threat_Repository.pdf; OEWG, 2021–2025, "Global Cyber Security Cooperation Portal", Submitted by India, 12 December 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/GCSCP-final-3.pdf.

28 For example, a concept paper references "practical implementation of the agreements reached by the OEWG 2021–2025"; and a cross-regional group proposes that the mechanism would "be rooted in the implementation of the framework". OEWG 2021–2025, Concept paper submitted by a group of states, p. 1; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

29 For example, a concept paper references "development of a common understanding of how international law applies in the use of ICTs and how the existing norms could be adapted to the specifics of information space"; and a working paper proposes dedicated meetings on international law. OEWG 2021–2025, Concept paper submitted by a group of states, p. 1; OEWG 2021–2025, "Programme of Action (PoA) and International Law".

30 For example, a concept paper references "development and implementation of confidence-building measures and mechanisms for practical cooperation between States, including through established channels of interaction between authorized agencies/bodies and the global intergovernmental directory of points of contact"; a cross-regional group references referencing "practical initiatives and confidence-building measures to support the implementation"; and the OEWG Chair proposed confidence-building measures [and] further development and operationalization of the Global Points of Contact Directory" as a part of the future mechanism's scope. OEWG 2021–2025, Concept paper submitted by a group of states, p. 1; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 3; OEWG 2021–2025, "Draft Elements", paragraph 8.

31 "A number of States underscored that capacity-building, including financial and technical assistance, should be a fundamental component of the scope of the programme of action and should support States' ability to implement their commitments." Report of the Secretary-General, A/78/76, paragraph 10.

32 For example, a concept paper references "further development of legally binding rules, norms and principles of responsible behavior of States", and a cross-regional group calls for a "review of the normative framework for responsible State behavior, including its further development if necessary" within the future mechanism. OEWG 2021–2025, Concept paper submitted by a group of states, p. 1; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 1.

33 "Precise mapping of the needs and challenges States face through progress reports". OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

34 "Topics could include . . . critical infrastructure protection, cyber incident response and cooperation among States, cyber threats assessments." OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

35 "Reporting best practices, identifying challenges or conducting practical initiatives will contribute to inform needs-based and strategic decision-making by Member States at RevCons and plenary discussions". OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

36 "States could be given opportunities for voluntary national reporting of their efforts to implement the cumulative and evolving framework for responsible State behaviour in the use of ICTs." OEWG 2021–2025, "Draft Elements", paragraph 16.

37 "A number of States referenced the need for the programme of action to identify gaps in the existing normative framework and consider actionable recommendations to support implementation efforts." Report of the Secretary-General, A/78/76, paragraph 28.

38 "The PoA could leverage existing and potential capacity-building efforts, increase their visibility and improve their coordination, as well as support the mobilization of resources and assist with pairing available resources with requests for capacity-building support and technical assistance." OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

39 For example, a concept paper proposes "further development of legally binding rules, norms and principles of responsible behavior of States and creation of effective mechanisms for their implementation, as elements of a future universal treaty on ensuring international information security"; and a cross-regional group states that "the PoA would also provide a venue to consider the need for additional voluntary, non-binding norms or additional legally binding obligations, as necessary." OEWG 2021–2025, Concept paper submitted by a group of states, p. 1; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2.

40 "The normative role should continue to be performed by the UN General Assembly – as it has up to today, by adopting the reports of the GGEs and of the OEWGs." OEWG 2021–2025, Submission by Brazil, paragraph 11.

41 See for example OEWG 2021-2025, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security", Submitted by Russian Federation on behalf of a group of states, 19 June, 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.

42 The possibility of merging existing proposals has been noted by states. For example, the Chair's summary of the third session of the OEWG 2021–2025 notes that "it was suggested that different formats could be complementary or could be merged in order to capitalize on the unique features of each and reduce duplication of efforts." OEWG 2019–2021, A/AC.290/2021/CRP.3, paragraph 43.

43 For example, a concept paper proposes holding "hold two substantive sessions per year at the UN Headquarters in New York"; a cross-regional group references "open-ended discussions similar to the format of other UN forums, like the current OEWG on ICT security"; and the OEWG Chair proposed "two substantive sessions to be convened per year, with each substantive session lasting for one week". OEWG 2021–2025, Concept paper submitted by a group of states, p. 2; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2; OEWG 2021–2025, "Draft Elements", paragraph 9.

44 "The open-ended action-oriented permanent mechanism will include a dedicated thematic group on capacity-building and international law". OEWG 2021–2025, "Draft Elements", paragraph 13.

45 For example, a cross-regional group references topics for working groups such as "critical infrastructure protection, cyber incident response and cooperation among States, and cyber threats assessments". OEWG 2021–2025, Proposal by a cross-regional group of states, footnote 4.

46 For example, a concept paper suggests "UN Member States may decide to create subsidiary subgroups for more detailed, in-depth consideration of specific aspects of the mandate"; a cross-regional group proposes "Open-ended technical meetings and/or implementation working groups on specific areas could be mandated by Member States in plenary discussions"; and a Report of the Secretary-General recalls that "a number of States called for the creation of technical work-streams, working groups on specific topics and other forms of intersessional consultative meetings". OEWG 2021–2025, Concept paper submitted by a group of states, p. 3; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2; and Report of the Secretary-General, A/78/76, paragraph 37.

47 "A number of States noted that the Office for Disarmament Affairs would be the most appropriate entity to serve as secretariat for the programme of action." Report of the Secretary-General, A/78/76, paragraph 39.

48 For example, a cross-regional group proposes review conferences to "(i) assess the evolving cyber threat landscape, the results of the PoA's initiatives and meetings; (ii) update the Framework as necessary; (iii) provide strategic direction and mandates for the PoA's future plenaries, technical meetings, and other initiatives, including to develop new practical initiatives"; and the OEWG Chair proposed "the effective operation of the open-ended action-oriented permanent mechanism to be reviewed every four years". OEWG 2021–2025, Proposal by a cross-regional group of states, p. 2; OEWG 2021–2025, "Draft Elements", paragraph 21.

49 "Some supported annual meetings, while others noted the possibility of biennial meetings. Other States expressed flexibility regarding the frequency of such meetings. With regard to location, several States supported the holding of follow-up meetings in New York, with a few noting the possibility of holding meetings at alternative locations such as Geneva." Report of the Secretary-General, A/78/76, paragraph 35.

50 "A number of States reflected on the possibility of review conferences. Proposed frequencies ranged from every third or fourth year to every six years." Report of the Secretary-General, A/78/76, paragraph 36.

51 See OEWG 2021–2025, Proposal by a cross-regional group of states.

52 See OEWG 2021–2025, Concept paper submitted by a group of states.

53 For example, a concept paper proposes "a bureau composed by the chair, two vice-chairs, a rapporteur and, if needed, by chairs of subgroups (in the status of vice-chairs) … approved by consensus of States once in two years basing on fair geographic representation and rotation among regional groups"; and the OEWG Chair proposed "the Chair of the permanent mechanism to be appointed for a period of two years, on the basis of equitable geographical representation". OEWG 2021–2025, Concept paper submitted by a group of states, p. 3; OEWG 2021–2025, "Draft Elements", paragraph 18(c).

54 "The view was expressed that technical working groups could be convened in a hybrid or virtual format to allow for the broadest participation of experts. Suggested topics of focus for potential working groups included applicability of international law, implementation of specific norms of responsible State behaviour and the elaboration of new norms, rules and principles, including legally binding obligations or instruments, as appropriate. It was also suggested that the working groups could address thematic topics such as critical infrastructure protection." Report of the Secretary-General, A/78/76, paragraph 37.

55 "It would be a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee of the United Nations General Assembly." OEWG 2021–2025, A/78/265, paragraph 36.

56 “There is broad agreement that consensus decision-making and inclusivity, in particular, are critical elements of regular institutional dialogue in this area.” Report of the Secretary-General, A/78/76, paragraph 46.

57 “Other interested parties, including businesses, non-governmental organizations and academia could contribute to any future regular institutional dialogue, as appropriate.” OEWG 2021–2025, A/78/265, paragraph 57.

58 “Many States noted the value of inclusive participation of non-governmental stakeholders, including civil society, the private sector, academia and the technical community, and called for specific modalities for their participation.” Report of the Secretary-General, A/78/76, paragraph 40.

59 For example, a concept paper proposes “participation of non-state actors (non-governmental organizations, businesses and academia) in the work of the permanent OEWG should be strictly consultative and informal [where] accredited (agreed by States) non-state actors should be allowed to participate in the official events as observers”; and a cross-regional group states that “the PoA would enable engagement and collaboration with relevant stakeholders”. OEWG 2021–2025, Concept paper submitted by a group of states, p. 3; OEWG 2021–2025, Proposal by a cross-regional group of states, p. 3.

60 “States in a position to do so to continue to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant UN processes.” OEWG 2021–2025, A/78/265, paragraph 36.

61 “States recognized 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.” OEWG 2021–2025, A/78/265, paragraph 56.

62 For example, Brazil noted the need for “modalities/methods of work [to] avoid stagnation of the process (e.g., possibility of [use of the consensus rule as] a de facto veto power), as experienced, for example, by the Programme of Action on small arms and light weapons for a long period.” OEWG 2021–2025, Submission by Brazil, paragraphs 5, 19.

63 “Several States called for the international conference to provide for the participation of stakeholders and make decisions on the basis of consensus, at least on matters of substance.” Report of the Secretary-General, A/78/76, paragraph 25.

64 For example, a concept paper states that “participation of non-state actors (non-governmental organizations, businesses and academia) in the work of the permanent OEWG should be strictly consultative and informal – for example, within intersessional meetings held once a year.” OEWG 2021–2025, Concept paper submitted by a group of states, p. 3.

65 For example, a cross-regional group states that “the PoA would enable engagement and collaboration with relevant stakeholders”. OEWG 2021–2025, Proposal by a cross-regional group of states, p. 3.

66 3rd Annual Progress Report of the OEWG 2021–2025, “Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security.” OEWG 2021–2025, A/79/214, Annex C.

References

General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, https://undocs.org/A/70/174.

General Assembly, ''Developments in the Field of Information and Telecommunications in the Context of International Security", Resolution A/RES/75/240, 31 December 2020, https://undocs.org/A/RES/75/240.

General Assembly, "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security", Report of the Secretary-General, A/78/76, 18 April 2023, https://undocs.org/A/78/76.

General Assembly, Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816, 18 March 2021, https://undocs.org/A/75/816.

General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, https://undocs.org/A/76/135.

General Assembly, First Annual Progress Report of the Open-Ended Working Group on Security of and in the use of Information and Communications Technologies 2021–2025, A/77/275, 8 August 2022, https://undocs.org/A/77/275.

General Assembly, Second Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, 1 August 2023, https://undocs.org/A/78/265.

General Assembly, Third Annual Progress Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Annex C titled "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security," A/79/214, 22 July 2024, https://documents.un.org/doc/undoc/gen/n24/217/49/pdf/n2421749.pdf.

General Assembly, "Subsidiary Organs of the General Assembly", https://www.un.org/en/ga/about/subsidiary/index.shtml.

OEWG 2019–2021, Third Substantive Session, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

OEWG 2021–2025, "Brazil's Views on the Future Regular Institutional Dialogue on Information and Communication Technology in the Context of International Security", Submission by Brazil, 23 April 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Brazil-_EN--_website.pdf.

OEWG 2021–2025, "Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the use of Information and Communications Technologies", Submitted by the Russian Federation on behalf of a group of states, 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.

OEWG 2021–2025, "Draft Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security", Submitted by the Chair, 1 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_1_May_2024_0.pdf.

OEWG 2021–2025, "[DRAFT] Rev.2 Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security", Submitted by the Chair, 18 June 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_18_June_2024.pdf.

OEWG, 2021–2025, "Draft Working Paper on the Establishment of a Threat Repository within the United Nations", Submitted by Kenya, 18 July 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Updated18July23Kenya_Draft_Working_Paper_Threat_Repository.pdf.

OEWG, 2021–2025, "Global Cyber Security Cooperation Portal", Submitted by India, 12 December 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/GCSCP-final-3.pdf.

OEWG 2021–2025, "Programme of Action (PoA) and International Law", Working Paper by Chile, Estonia, Fiji, Japan and the United Kingdom, 14 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PoA_and_International_Law_OEWG_Working_Paper_May_2024.pdf.

OEWG 2021–2025, "Proposal on the Structure of the Future Mechanism for Regular Institutional Dialogue on Cyber Issues", Submitted by a cross-regional group of states, 17 May 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_cross-regional_working_paper_-_Future_UN_cyber_mechanism_for_2025_onward-vf_0.pdf.

OEWG 2021–2025, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security", Submitted by a Russian Federation on behalf of a group of states, 29 June 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.

OEWG 2021–2025, "Working Paper for a Programme of Action (PoA) to Advance Responsible State Behavior in the Use of ICTs in the Context of International Security", Submitted by a group of states, 1 December 2023, https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG