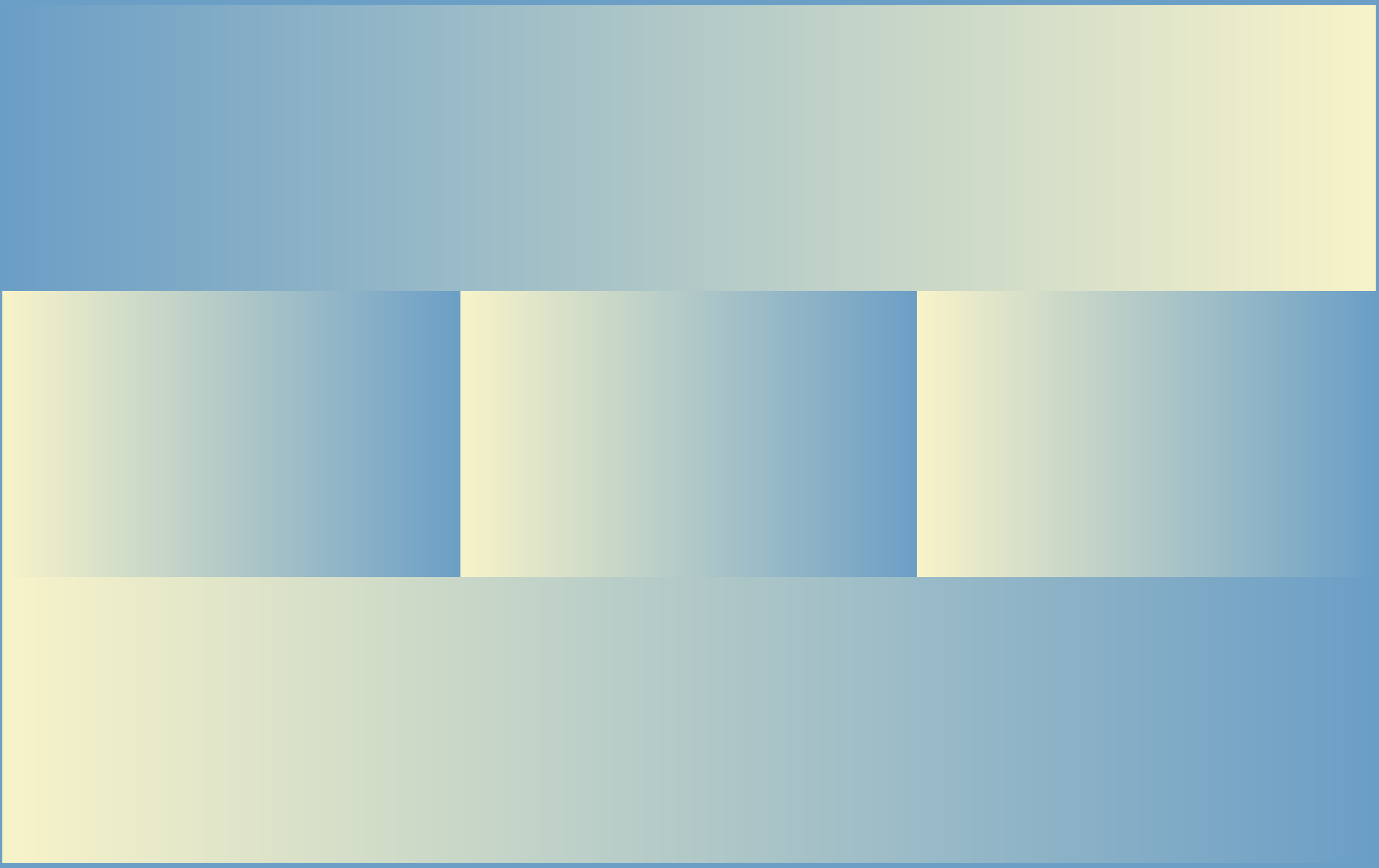


PERSPECTIVE

The UN’s New Global Mechanism on Cybersecurity

How Europe Can Advance Responsible State Behaviour in Cyberspace

Christina Rupp

March 06, 2026

Tech analysis and policy ideas for Europe

interface

Table of Contents

March 2026 will mark a milestone for international cybersecurity policy: all 193 UN Member States will convene in New York to launch the UN's first permanent Global Mechanism. Agreed at the final session of the second UN Open-ended Working Group (OEWG) in July 2025, the *Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs* (Global Mechanism) will begin its work with an organizational session on March 30-31, 2026.

While the length of the new format's title already reflects the political compromises underpinning it, the consensus reached represents a shared commitment to a single, sustained multilateral framework for cybersecurity after decades of ad hoc and time-limited processes. It also prevented a fragmentation of UN cybersecurity governance into competing parallel tracks, as had occurred with the concurrent Group of Governmental Experts (GGE) and OEWG processes underway in 2019-2021.

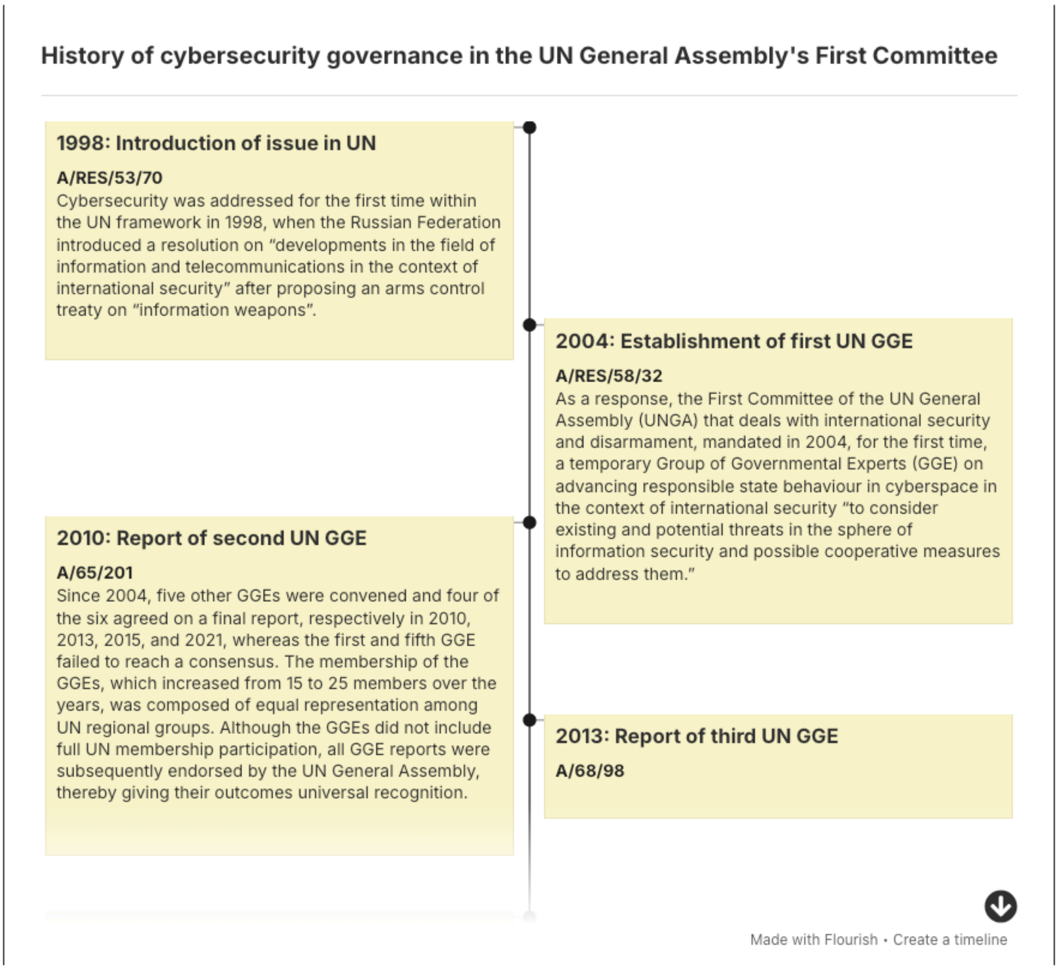
Yet, how the forum's defining new feature – the creation of dedicated thematic working groups (DTGs), aimed at providing a space to accelerate the implementation of the outcomes of more than two decades of UN discussions – will operate in practice and how their work will connect with other components of the process remains largely unsettled and highly contested among states. While this may seem like a technicality or a mere procedural concern, how these groups are set up will determine whether the mechanism can deliver meaningful practical progress in the long term. For Europe, these early stages offer a unique opportunity to shape the mechanism, advance its priorities, and influence global cybersecurity discussions for years to come.

How cybersecurity became a UN issue

To understand today's debates and the divergences among states, it is necessary to examine how cybersecurity – or, in UN terminology, the security of and in the use of information and communications technologies – has been discussed within the UN over the past two and a half decades. While the issue gradually gained prominence on the UN agenda, the process was far from linear and marked by political divergences.[1] The timeline below (Figure 1) provides a historical overview

[1] For further information, see, for example, Ruhl et al. (2020): Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. For a personal account (from the U.S. perspective) on these developments, see Michele Markoff (2025): The Origins of Cyber Diplomacy: Great Power Cyber Competition and Rapprochement in the United Nations 1998–2021, in: Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis (eds.): A Handbook for the Practice of Cyber Diplomacy.

of key milestones in UN cybersecurity governance in the UN General Assembly’s First Committee[2] :



History of cybersecurity governance in the UN General Assembly's First Committee

1998: Introduction of issue in UN

A/RES/53/70

Cybersecurity was addressed for the first time within the UN framework in 1998, when the Russian Federation introduced a resolution on “developments in the field of information and telecommunications in the context of international security” after proposing an arms control treaty on “information weapons”.

2004: Establishment of first UN GGE

A/RES/58/32

As a response, the First Committee of the UN General Assembly (UNGA) that deals with international security and disarmament, mandated in 2004, for the first time, a temporary Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security “to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them.”

2010: Report of second UN GGE

A/65/201

Since 2004, five other GGEs were convened and four of the six agreed on a final report, respectively in 2010, 2013, 2015, and 2021, whereas the first and fifth GGE failed to reach a consensus. The membership of the GGEs, which increased from 15 to 25 members over the years, was composed of equal representation among UN regional groups. Although the GGEs did not include full UN membership participation, all GGE reports were subsequently endorsed by the UN General Assembly, thereby giving their outcomes universal recognition.

2013: Report of third UN GGE

A/68/98

Made with Flourish • Create a timeline

For a complete presentation of this graph, please see the online version of this publication. https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity

Figure 1: History of cybersecurity governance in the UN General Assembly’s First Committee (to see the table in a new tab, click here)

Over time, discussions by states in these various groups have led to the creation and continuous development of a so-called framework of responsible state behavior, which aims to set rules and shared expectations for how states should (not) act through political norms and international law, prevent conflict escalation through confidence-building measures (CBMs), and strengthen resilience by capacity-building activities.[3]

[2] In addition to the First Committee, discussions on cybercrime take place in the UN General Assembly’s Third Committee, which has negotiated the UN Convention on Cybercrime. Cybersecurity has also increasingly featured on the Security Council’s agenda in recent years. On the latter, see, for example, Allison Pytlak (2024): Addressing International Cyber Peace and Security - What Role for the UN Security Council?, Stimson Center and Security Council Report (n.d.): Technologies.

[3] Although the GGEs did not include full UN membership participation, all GGE reports were subsequently endorsed by the UN

Most notably, states have

- 2013: Affirmed for the first time that **international law**, including the UN Charter, applies to cyberspace,[4] subsequently, in 2021, also specifically affirming "that international humanitarian law applies only in situations of armed conflict",[5]
- 2015: Agreed on 11 voluntary, non-binding **norms for responsible state behaviour** in cyberspace,[6] later, in 2021, adding another layer on ways for their implementation and forms of expected behavior in accordance,[7]
- 2021: Adopted ten principles on **cyber capacity-building** (CCB) by which states should be guided by in relation to State use of ICTs in the context of international security,[8]
- 2022-2024: Developed a set of eight universal **cyber CBMs**, encompassing inter alia a global Points of Contact (PoC) network of technical and diplomatic PoCs.[9]

These elements have formed the four pillars of the framework, which also structured the agenda of the sessions. Over the years, the exchanges of states have also encapsulated a catalogue of both **existing and potential threats**, producing a substantive overview of potential risks to international peace and security. Most recently, in 2025, states have implicitly elevated the discussion of existing and potential threats to the status of a fifth pillar of the framework.[10]

Institutionalizing UN cybersecurity discussions: The Global Mechanism

Amid growing interest and the rising implications of cybersecurity for international security, states have been discussing since 2019 how to move beyond temporary groupings and institutionalize these discussions through a permanent forum with a dedicated body within the UN. Various proposals were made over the years, including the France-led and EU-backed Program of Action (PoA) proposing a combination of plenary meetings and working groups,[11] Russia et al.'s permanent

General Assembly, thereby giving their outcomes universal recognition.

[4] United Nations General Assembly (2013): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98).

[5] United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

[6] United Nations General Assembly (2015): 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).

[7] United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

[8] United Nations General Assembly (2021): Open-ended working group on developments in the field of information and telecommunications in the context of international security - Final Substantive Report.

[9] United Nations General Assembly (2023): Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/78/265) and United Nations General Assembly (2024): Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/79/214).

[10] United Nations General Assembly (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257).

[11] France, Egypt et al. (2020): The future of discussions on ICTs and cyberspace at the UN, France, Egypt et al. (2021): Working paper for a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security, United Nations General Assembly (2022): Programme of action to advance responsible State behaviour in the use of

OEWG,[12] and China's later proposition of a somewhat hybrid model seeking to combine substantive and dedicated plenary sessions.[13]

Even though much of this may seem procedural in nature, at the heart of these proposals lies a political rather than a merely procedural question. The differing preferences expressed by states are not merely technical disagreements about format or process. Rather, they reflect broader national positions and divergent views on the body's overall purpose and the level of substantive progress it should seek to achieve.

In plenary sessions, the combination of broad agenda items and wide-ranging interventions make it difficult to examine specific or more technical issues in detail. As a result, plenary debates oftentimes remain high-level rather than issue focused. For these reasons, the proposal for a permanent UN OEWG, favoring exclusive plenary sessions and opposing thematic groups, was unacceptable to many, with divergences centering on whether to continue past practices or move into an "implementation phase," enabling forums for more substantive, issue-driven dialogues.

During the negotiations on a permanent mechanism within the second UN OEWG, states eventually agreed in July 2024 that the new mechanism would include working groups – so-called dedicated thematic groups (DTGs) – in addition to plenary sessions as one of the forum's institutional layers.[14] The Global Mechanism will operate in five-year cycles, with formal plenary sessions and informal DTGs in years one to four, followed by a review conference in year five that will shape how the mechanism continues its deliberations from year six onward. Plenary sessions will continue discussions along the five pillars of the UN framework – threats, norms, international law, confidence-building measures, and capacity-building – serving as agenda items for state statements. The DTGs will take place in hybrid format and will thus be informal meetings in line with UN practice, with formal decision-making remaining the prerogative of the plenary. To this end, the DTGs are envisioned to provide recommendations to the plenary sessions.

information and communications technologies in the context of international security (A/RES/77/37), United Nations General Assembly (2023): 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), France et al. (2024): Cross-regional working paper - Proposal on the structure of the future mechanism for regular institutional dialogue on cyber issues, France (2024): Presentation on a proposal for the structure of the future mechanism on regular institutional dialogue, France (2025): Working Paper - Action-oriented thematic groups to advance responsible State behaviour in cyberspace, and France (2025): Working Paper - Bridging the consensus gap through a compromise: updated proposal for action-oriented thematic groups. See also Allison Pytlak (2022): Advancing a Cyber Programme of Action: Options and Priorities, Women's International League for Peace and Freedom.

[12] Russia et al. (2023): Concept paper of the Russian Federation on establishing under the auspices of the United Nations a regular institutional dialogue for all the UN Member States on security of and in the use of information and communications technologies and Russia et al. (2023): Concept paper on a permanent decision-making Open-ended Working Group on security of and in the use of information and communications technologies.

[13] China (2025): China's Proposal for the Future UN Permanent Mechanism on ICT Security in the Context of International Security.

[14] United Nations General Assembly (2024): Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/79/214), Annex C. In addition to these formats, states can also convene in dedicated intersessional or consultative meetings with stakeholders, both at the discretion of the Mechanism's Chair.

Even after states agreed to include working groups as a component of the new mechanism, divergent views persisted during the second UN OEWG's final year over which themes to prioritize and how many working groups to establish. Broadly, positions fell into three approaches:

- ***Pillar-based approach:*** Russia and several others supported one group per pillar,[15] though critics warned that this could duplicate plenary debates following the same pillar-based structure and limit progress to familiar, high-level exchanges.
- ***Selective pillar focus:*** Some states, including the African Group, favored dedicated groups on selected pillars, such as international law or capacity-building.[16] During the final stages of negotiations, the UN OEWG Chair proposed groups on these two pillars as a compromise alongside a group on "resilience and stability" [author's summary].[17] The African Group supported this approach in part due to resource considerations, noting that "focus on three dedicated thematic groups will assist with greater efficiency."[18] Other delegations opposed elevating certain pillars over others, arguing that "all five pillars of the mandate of the FPM [Future Permanent Mechanism] [sh]ould be treated equally during the discussions."[19] Separately, there were concerns that a dedicated group on international law could provide a platform for Russia and like-minded states to advance its proposal for a convention on international information security – an initiative which is strongly opposed by the EU and other like-minded states.
- ***Challenge-based approach:*** The EU and its like-minded partners proposed organizing work around three cross-cutting challenges to move beyond pillar-by-pillar discussions and explore connections and synergies for implementation, drawing on the framework in a holistic way: (1) "build[ing] resilience of cyber ecosystems and critical infrastructure" (resilience), (2) "cooperat[ing] in the management of ICT-related incidents" (cooperation), (3) "increase[ing] stability in cyberspace" (stability).[20] For some states, however, this proposal did not sufficiently clarify how these themes related to the existing pillars or how boundaries between them would precisely be drawn.

A compromise with many open questions

Although a compromise, many structural elements of the Global Mechanism closely reflect the initial PoA proposal, marking a notable success for the "Western" camp. Due to persistent differences in views, however, states were unable to agree on any

[15] Russia et al. (2025): LMG Joint Paper of the Group of Like-Minded States.

[16] For proponents of a DTG on capacity-building, see, for example, Argentina et al. (2025): Working Paper: Strengthening Capacity-Building within the Framework of a Future United Nations Mechanism on the Use of ICTs in the Context of International Security and Argentina et al. (2025): Working Paper: Strengthening Strategic Dialogue on CapacityBuilding and Its Inclusion in the Future Permanent Mechanism.

[17] Chair Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (2025): Draft Final Report of the Open-ended Working group on security of and in the use of information and communications technologies 2021–2025, submitted to the 80th session of the General Assembly pursuant to General Assembly Resolution 75/240, Annex III.

[18] Representative of Nigeria on behalf of African Group (2025): Open-ended working group on Information and Communication Technology (ICT) - Eleventh Substantive Session, 4th meeting.

[19] Russia et al. (2025): LMG Joint Paper of the Group of Like-Minded States and Russia et al. (2025): Joint Statement of the Group of Like-Minded States.

[20] France (2025): Working Paper - Action-oriented thematic groups to advance responsible State behaviour in cyberspace.

of the three approaches proposed for defining the number and scope of the DTGs. They ultimately settled on establishing two DTGs for the first four years, leaving open the possibility of creating additional ad hoc groups by consensus. **DTG 1** will focus on "addressing **specific challenges** in the sphere of ICT security in the context of international security," essentially merging the three groups proposed by the EU into one, whereas **DTG 2** will focus on a single pillar, namely "accelerating ***ICT security capacity-building***."[21]

While this outcome avoided deadlock, it left several critical issues to be resolved at the earliest at the upcoming March organizational session. Beyond the significance of selecting the Mechanism's Chair for the first two years, a number of additional decisions will be crucial. These open questions include appointing states as DTG co-facilitators, defining the specific agenda items and thematic focus of each group, determining the nature and status of recommendations to be forwarded by the DTGs to the plenary, and clarifying how non-governmental experts will be engaged in the DTGs to ensure practical value. At the same time, the designation of a Chair and the co-facilitators will be particularly important given the considerable influence their positions hold in shaping discussions and potential outcomes.

These decisions matter especially because the Mechanism inherits a mixed UN track record on cybersecurity: while states have reached important political agreements, their implementation has often lagged due to capacity gaps, persistent substantive disagreements, and rising geopolitical tensions. Turning agreed language into practice has repeatedly proven challenging. This is illustrated, for example, by persistent divisions over whether to prioritize the implementation of existing commitments vs. the elaboration of new norms, as well as by referencing, at a minimum, OEWG discussions on international humanitarian law. A further example is the inability of the past UN OEWG to substantively engage with and agree on a norms implementation checklist[22] tabled by the Group's Chair. Against this backdrop, the DTGs – precisely because of their informal nature – are widely seen as the main opportunity to move beyond restating national positions toward deeper exchanges that can help translate past consensus language into concrete policy action.

[21] United Nations General Assembly (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257).

[22] See, for example, Chair Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (2025): Zero Draft - Final Report of the Open-ended Working group on security of and in the use of information and communications technologies 2021–2025, submitted to the 80th session of the General Assembly pursuant to General Assembly Resolution 75/240, Annex I.

Preparing for the Mechanism's launch

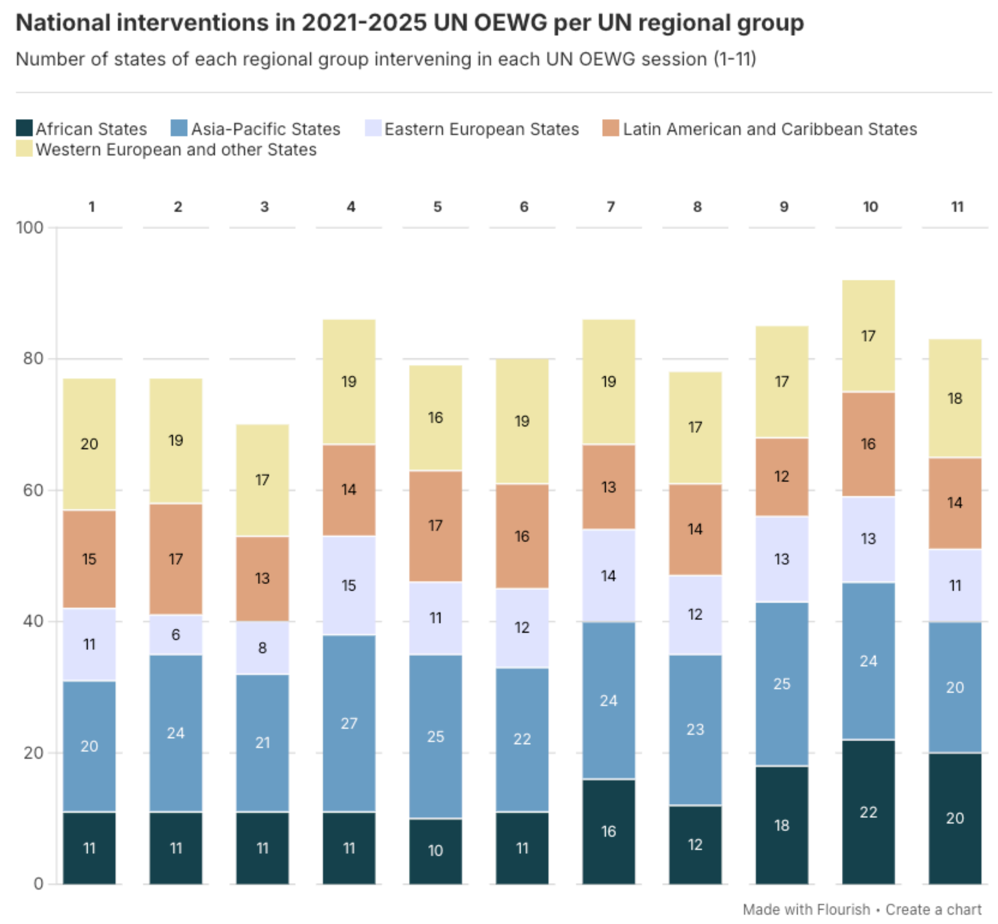
The organizational session of the mechanism will be the first opportunity to address and ideally resolve these open questions. As the organizational session agreements – or a lack thereof – will set the stage for how the permanent mechanism operates, the weeks leading up to the March 30–31 meeting will be critical and require extensive preparatory work. States must define clear priorities, identify potential agenda items, and set realistic expectations for what the DTGs can achieve. But setting priorities is not enough. States must also engage with partners and states across all regions to explore positions, identify common denominators, and build support for concrete ideas.

Since (at least) November 2025, EU Member States have been deliberating an internal coordinated EU position on the Global Mechanism to guide the region's negotiation and outreach strategy.[23] In forming this position and exchanging with other regions, European cyber diplomats should view the DTGs not just as spaces for deliberation, but as catalysts for action beyond the UN system – particularly in today's geopolitical context, where multilateral organizations are under increasing pressure and achieving universal consensus on international security issues is becoming progressively difficult.

Past UN cybersecurity working groups demonstrate that the value of these forums extends beyond formal agreements – the process itself is also a key product. They have helped states develop and articulate national positions, share experiences, and build trust, often triggering follow-up actions such as domestic policy changes and initiatives,[24] new partnerships, and targeted assistance measures. Developments in the OEWG II further showed slowly but steady rising global engagement on cybersecurity: more delegations are participating in discussions and geographic diversity has increased overall, with a particularly notable rise in interventions from the African Group in the OEWG's last sessions as Figure 2 illustrates.

[23] Council of the European Union (2025): Notice of Meeting and Provisional Agenda - Horizontal Working Party on Cyber Issues (CM 5133/25).

[24] Evidenced, for example, by the growing number of national and regional position papers on the applicability of international law developed during and since the last OEWG. See also, commentary by Talita Dias in: Allison Pytlak, Christina Rupp, Eugene EG Tan, Louise Marie Hurel, Talita Dias and Valentin Weber (2025): The Rules of the Road in Cyberspace, 10 Years Later, Royal United Services Institute for Defence and Security Studies and commentary by Nemanja Malisevic in: GIP Digital Watch Observatory (2025): Breaking down the OEWG's legacy: Hits, misses, and unfinished business.



For a complete presentation of this graph, please see the online version of this publication.
https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity

Figure 2: National interventions in 2021-2025 UN OEWG per UN regional group (the figure does not account for the interventions made by the EU, to see the table in a new tab, click here)

Hence, European policymakers should prioritize DTG focus areas where long-standing UN consensus aligns with EU policy priorities. They should focus on issue-areas where they are – as a byproduct – interested in raising awareness of their own approaches, stimulate discussions in other states, and have the political backing to potentially engage in new partnerships and provide capacity-building support on these issues.

In addition, Europe should draw lessons from its past negotiation approaches, particularly the PoA proposal. Although many of its initial elements were ultimately reflected in the overall compromise, the EU's challenge-based proposals for the DTGs struggled to gain widespread traction. Beyond political preferences and sensitivities, which clearly played a significant role, one reason was their lack of clear links to established pillars and agreed language. This left some states – especially those only recently accustomed to the pillar-based structure that has framed UN discussions for the past decade – uncertain about how these issue-based discussions precisely connected to prior deliberations. Especially since DTG discussions are mandated to "draw[...] on the five pillars of the framework,"[25] future EU input should explicitly link its proposed focus areas to the pillars to mitigate these concerns and demonstrate how issue-focused discussions can reinforce existing frameworks, thereby helping to secure buy-in from other states.

A European strategy for the DTGs

The current modalities foresee only a week for all meetings of DTG 1 and 2 per year, while any additional sessions remain subject to the discretion of the Global Mechanism's Chair and the DTG co-facilitators. In light of these constraints, ensuring a clear and focused mandate for DTG 1 will be particularly important – arguably even more so than for DTG 2, whose scope is already more narrowly circumscribed around a specific topic.

Addressing the considerations outlined above and overlaying priorities from 25 years of UN discussions, alongside issues voiced by states from various regions, helps identify potential strategic focus areas for the EU. Building on this analysis, two areas illustrate how these connections could be made: **critical infrastructure protection** for DTG 1 and **prevention, detection, and response capacities** for DTG 2.

DTG 1: Critical infrastructure protection (Year 1-2)

For the first two years of DTG 1, European Member States could aim for focusing on critical infrastructure protection. This would build upon the international community's "express[ion of] serious concern regarding the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII),"[26] as well as the consistently high number of national statements addressing this matter. It would also permit the EU to draw on the challenges identified in the PoA proposal, where critical infrastructure was included as a potential focus in the proposed group on resilience.[27] This approach would allow the EU to build upon its past proposals rather than deviate from them, giving

[25] United Nations General Assembly (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257), Annex I.

[26] For example, United Nations General Assembly (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257).

[27] France (2025): Working Paper - Action-oriented thematic groups to advance responsible State behaviour in cyberspace.

them renewed momentum.

Emphasizing critical infrastructure protection provides an opportunity to follow up on UN discussions on threats, capacity-building, and confidence-building, while also exploring how these challenges relate to various UN cyber norms and what states can do to accelerate their implementation. Based on past UN consensus documents, non-exhaustive guiding questions for discussion may include the following, each linked to examples of relevant framework pillars whose implementation it may support [indicated in brackets]:

- Which ICT-related threats are the most significant for critical infrastructure and what cooperative measures are available to address them? How can states cooperate in the management of cross-border interdependencies of critical infrastructure? [→ *connection to threats and norms, especially norms A and G*]
- How can states protect critical infrastructure from threats such as ransomware and other malicious ICT activities, and what best practices and lessons learned regarding preventive or risk-reduction measures can they share with each other to reduce the likelihood or impact of incidents? [→ *connection to threats, norms, especially norm G, and CBMs, especially CBM 7*]
- How have states responded to requests for assistance from other states whose critical infrastructure has been targeted by malicious ICT acts? What types of assistance have been most needed, and what practical challenges or prerequisites affect effective cooperation? [→ *connection to norms, especially norm H*]
- What steps have states taken, or could take, to comply with norms prohibiting ICT activity that intentionally damages or impairs critical infrastructure or harms the systems of another state's authorized computer emergency response teams (CERTs)? [→ *connection to norms, especially norms F and K*]
- What role does international law play in guiding the protection of critical infrastructure, even without a universal definition of critical infrastructure? Which international law provisions do states consider relevant, if so? [→ *connection to international law*]
- How can states strengthen capacity to implement protective measures, what gaps exist and what capacity-building activities are specifically needed? [→ connection to *capacity-building and norms, especially norm G*]
- How can states, through public-private partnerships with private operators and other stakeholders, strengthen confidence-building, implement protective measures, and ensure effective incident response? [→ *connection to CBMs, especially CBMs 7 and 8*]

In contributing to this discussion, the EU and its Member States could share lessons from its horizontal frameworks in place – such as the NIS 2 Directive and the Critical Entities Resilience (CER) Directive – as well as sector-specific rules in areas including energy, financial services, and civil aviation,[28] and provide insights into

[28] For example, Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (2024/1366), Regulation on digital operational resilience for the financial sector (2022/2554, DORA), or Commission Implementing Regulation laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (2019/1583).

designation criteria for critical sectors. Substantively, the EU could outline key critical infrastructure protection-related obligations for Member States, including national cybersecurity strategies, cyber crisis management arrangements, coordinated vulnerability disclosure (CVD) policies, and supervisory and enforcement capacities. In addition, it could highlight requirements for critical entities themselves, such as risk management and incident reporting, and demonstrate how these requirements are implemented in practice. EU Member States could also share information on Union-level coordination and information-sharing mechanisms in place, including crisis management blueprints.[29] EU contributions along these lines would enable the Union to showcase its approach, exchange lessons learned, and encourage strengthened action internationally. At the same time, they could position the EU as a practical point of contact for partners seeking to better understand the Union's frameworks and experience, thereby creating opportunities for follow-up dialogue and sustained cooperation.

Building on the outputs of discussions in years one and two, for DTG 1 years three and four, UN Member States could either choose to extend ongoing discussions on critical infrastructure protection or select a new focus area where measurable progress can be achieved. In the latter case, EU Member States could propose that the group focus on another challenge previously included in the PoA proposal, such as supply chain security or fostering effective mechanisms for the peaceful settlement of disputes.

DTG 2: Prevention, detection, and response capacity-building (Year 1-4)

Unlike DTG 1, whose scope requires careful tailoring to avoid duplication with plenary discussions, DTG 2 has a more defined focus on building specific cybersecurity capacities from the outset. In this regard, it is important to highlight that many states have emphasized in OEWG discussions that the UN should not be the forum for general debates on cybersecurity capacity-building. Rather, discussions on capacity-building should focus on strengthening capacities that accelerate the implementation of the framework for responsible state behavior.

[29] Examples the EU could draw on include information-sharing and cooperation arrangements under the CER and NIS Directive, specifically the Critical Entities Resilience Group and the NIS Cooperation Group, the latter of which, inter alia, covers workstreams on energy, health, and aviation. In terms of crisis management, the EU has both cyber and critical infrastructure-specific relevant crisis blueprints in place, designed to enable coordinated responses to significant incidents when needed (Council of the EU (2025): Council Recommendation on an EU blueprint for cyber crisis management (C/2025/3445) and Council of the EU (2024): Council Recommendation on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance (C/2024/4371).

In recent years, capacity-building discussions have repeatedly centered on the triad of prevention, detection, and response capacities, as reflected in UN consensus language since 2021. States have underscored that "a lack of awareness and adequate capacities to detect, defend against, or respond to malicious ICT activities may make them more vulnerable,"[30] a point that has been reiterated in subsequent reports since. They have also earlier identified "building or enhancing the technical, legal, and policy capacities of States to detect, investigate, and resolve ICT incidents"[31] as one of the recommended areas for international capacity-building. Yet, there has so far been no elaboration on what these capacities entail and how they can contribute to advancing responsible state behavior in cyberspace.

Structuring DTG 2 along these lines by dedicating each year to one capacity area – for example, year one: prevention capacities, year two: detection capacities, year three: response capacities, and year four: integrated discussion across all three capacity areas – would allow for systematic exploration and synergy-building. It would also enable compatibility with existing technical and operational efforts, allowing the group to draw on established guidelines and standards, which facilitates leveraging synergies and making discussions concrete and accessible.[32]

Taking detection as an example, detection capacities help states implement nine of the eleven UN cyber norms,[33] relate to due diligence under international law, and are referenced in two of the eight global CBMs.[34] Against this backdrop, non-exhaustive guiding questions for discussion in DTG 2 during the year potentially dedicated to detection capacities could include the following, each linked to examples of relevant framework pillars whose implementation it may support [indicated in brackets]:

- What capabilities do states consider essential for detecting cybersecurity threats, and which governmental structures, responsibilities, and mechanisms can support the development of these capacities? [→ *connection to capacity-building and norms, especially norm B*]
- From the perspective of states, which gaps currently exist in detection capacities, and which capacity-building initiatives are most valuable to address these needs effectively? How can the catalogue of CCB principles be applied to guide activities aimed at enhancing these capacities? [→ *connection to capacity-building*]

[30] Included for the first time in United Nations (2021): Open-ended working group on developments in the field of information and telecommunications in the context of international security.

[31] United Nations (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

[32] For example, U.S. National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0 and U.S. National Institute of Standards and Technology (n.d.): Cybersecurity Framework or Federal Office for Information Security (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen for a detection capacity-specific example.

[33] Christina Rupp (2025): Signals in the Noise: Building Governmental Capabilities to Detect Cybersecurity Threats, interface.

[34] Importantly, however, working through this example also highlights the limitations of CCB discussions in a UN context. Elevating detection capabilities to a dedicated agenda item in UN processes should not lead to assigning the UN a more operational role in the cyber domain, such as creating pathways for the direct exchange of indicators of compromise (IoCs) or other forms of cyber threat intelligence (CTI). Not only would this risk duplicating existing efforts, it would also be less effective. This is because information-sharing works best in settings comprising far fewer than 193 members.

- How can detection capacities help states identify and understand existing and emerging ICT threats, including those involving AI and other emerging technologies? [→ *connection to threats*]
- How can detection capacities support states in considering all relevant information in the case of ICT incidents, ensuring supply chain integrity, or encouraging responsible vulnerability reporting and mitigation sharing? [→ *connection to norms, especially norms B, I, and J*]
- How can detection capacities help states in fulfilling international law obligations, such as, for example, identifying internationally wrongful acts in the context of the principle of due diligence? [→ *connection to international law and norms, especially norm C*]
- How can the Points of Contact (PoC) directory contribute to facilitating the detection of urgent or significant ICT incidents? [→ *connection to CBMs, especially CBM 1*]
- What examples exist of public-private collaboration to strengthen detection capacities? How can states maximize the value of detection capacities through cooperation and information exchange with other actors both within and beyond their jurisdiction? [→ connection to *CBMs, especially CBM 5 and 8, and capacity-building*]

Accordingly, EU Member States could leverage DTG 2 as a catalyst to engage other delegations. This would be particularly in the EU's interest, as the Union's recent International Digital Strategy explicitly identifies strengthening partners' capacities to detect, prepare for, and respond to cybersecurity threats and incidents as a direct investment in the EU's own security,[35] which aligns well with the suggested potential scoping for years one to three.

As contributions to the discussions, the EU could draw on its experience in strengthening detection, prevention, and response capacities. Under the NIS 2 Directive, each Member State is required, among other obligations, to establish or designate one or more national CSIRTs capable of preventing, detecting, responding to, and mitigating cybersecurity threats. More recently, the EU has adopted the Cyber Solidarity Act, which aims to reinforce these capacities. This includes the establishment of a Cybersecurity Alert System, composed of national and cross-border cyber hubs, to enhance coordinated detection, situational awareness, and the analysis of cyber threats and incidents. Beyond public sector capacities, the EU is also increasingly placing obligations on specific entities to strengthen their related cybersecurity posture. For instance, the Digital Operational Resilience Act (DORA) requires financial entities to implement measures for detecting potentially adverse activities and to regularly test their resilience measures.

By contributing its experience in establishing and implementing these rules, the EU could share lessons learned while gaining insight into how other states develop these capacities and the challenges they face. This can not only inform potential targeted

[35] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025): An International Digital Strategy for the European Union (JOIN(2025) 140 final).

follow-up measures but also support more focused discussions on how such capacities help implement the framework for responsible state behavior, while allowing the EU to demonstrate how it already operationalizes key elements of the framework through existing law and policies.

DTGs as the Global Mechanism’s driving force

At the same time, it should be recognized that the DTGs do not operate in isolation. While essential for substantive progress, they remain informal components within a broader institutional architecture that includes plenary sessions equipped with the mechanism’s formal decision-making power. Within this framework, DTGs can serve as facilitators of substance and continuity. For example, the DTG co-facilitators could be mandated to provide annual written summaries in their respective capacities. These summaries could then be transmitted to the plenary and progressively inform progress reports negotiated and adopted by states in plenary sessions – possibly at the end of years two and four – and be taken into account when negotiating the review conference report at the end of year five.

To generate recommendations and implementation insights that the plenary can formalize, the primary role of the DTGs should be to identify practical implementation steps by fostering interactive discussions that examine existing practices, identify gaps and challenges, and map pathways for cooperation. Discussions should aim for cross-cutting, interactive exchanges across pillars, while remaining attentive to how their outcomes feed back into the plenary’s pillar-based reporting structure. Co-facilitators could therefore encourage states to clearly link each identified implementation step to specific elements of the framework – whether a particular norm, a rule of international law, a confidence-building measure, or a capacity-building principle – and to assess these steps against the list of identified existing and emerging ICT threats to international peace and security.

To invigorate discussions and bridge technical, legal, political, and diplomatic communities, DTGs should make full use of expert participation as foreseen in their modalities. Meetings could combine expert briefings from governmental experts with interactive exchanges involving non-governmental practitioners, researchers, and other stakeholders. From a European perspective, this creates opportunities to involve actors such as the European Union Agency for Cybersecurity (ENISA) for technical briefings. ENISA, inter alia, supports EU Member States in implementing EU policies, including those related to critical infrastructure protection, and in building prevention, detection, and response capacities. On this basis, it would be well-positioned to share best practices and lessons learned from supporting states with varying levels of cyber maturity, as well as practical insights into implementation challenges.

Expert contributions like these – whether delivered through briefings or written inputs responding to specific questions – can shed light on how national and regional policies align with and operationalize the UN framework, identify persistent gaps, and propose concrete improvements. Through such formats, DTGs can function as dynamic gears within the broader mechanism, ensuring that technical expertise meaningfully informs diplomatic progress.

Turning frameworks into practice

The DTGs offer a timely opportunity to place the operationalization of the framework for responsible state behavior at the center, translating its components into practical, on-the-ground implementation. As this implementation process operates at the intersection of foreign and domestic policy, it requires states to develop and apply national instruments while feeding lessons from national and regional implementation back into global discussions. Recognizing this, the EU should use the Global Mechanism’s launch as an opportunity to link UN and EU frameworks to create practical synergies. Potential DTG focus areas, such as critical infrastructure protection (DTG 1) and prevention, detection, and response capacity-building (DTG 2), illustrate how these connections could be made in practice.

This approach would raise awareness of the EU’s cybersecurity policy acquis[36] internationally while strengthening internal understanding of the UN framework’s components by connecting them to EU policies through clear, practical examples. By shaping the DTGs from the design phase and strategically leveraging the Mechanism as a catalyst for interregional partnerships, the EU and its Member States can not only contribute to maximizing the Global Mechanism’s impact and practical value beyond its predecessors, but also lay the groundwork for follow-up actions in the Union’s external engagement, for example, through targeted capacity-building activities or bilateral, multilateral, or interregional exchanges on specific issues.

[36] Christina Rupp (2025): EU Cybersecurity Policy Directory, interface.

Author

Christina Rupp
Lead International Cybersecurity Policy
crupp@interface-eu.org
+49308145037880

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com