EU CYBER DIRECT

POLICY BRIEF

THE PERMANENT TURN OF THE UN GLOBAL MECHANISM ON ICT SECURITY

Five Shifts in Cyber Diplomacy, and What They Will Require

Andrea Calderaro · July 2026

After two decades of ad hoc formats, Cyber Diplomacy has acquired a permanent institutional home under UN auspices. The UN Global Mechanism on Developments in the Field of ICTs in the Context of International Security held its first substantive session on 20–24 July 2026, closing out the temporary formats that preceded it: six cycles of the Group of Governmental Experts since 2004, and two cycles of the Open-Ended Working Group (OEWG), the second of which concluded in July 2025 with consensus on the Mechanism's establishment. The passing of the baton is surrounded by expectations that span the full spectrum, from those who suspect little will really change, to those who load the new body with responsibility for the future of multilateralism in cybersecurity itself. That a permanent institution was agreed by consensus at all, in a period when multilateral processes have more often fractured than consolidated, is itself an achievement worth registering before asking what it can deliver.

Its mandate is framed around a transition from negotiation to implementation, against a threat landscape in which emerging and disruptive technologies are outpacing traditional diplomatic processes. Whether that transition amounts to a genuine leap beyond what Cyber Diplomacy has achieved so far will only become clear over the coming months. But the Mechanism already carries several concrete novelties that could mark a discontinuity with the past, positioning it as the milestone in multilateral cybersecurity governance that the field has long had an appetite for.

IN THIS BRIEF

FIVE SHIFTS

1. Unlike the OEWG, which was built around a fixed mandate and a closing deadline, the Global Mechanism is permanent by design. **Permanence** cuts both ways. It makes the agenda versatile: where a time-bound process locks its priorities to the threat picture prevailing at the moment of its adoption, a standing forum can revise what it works on as technologies emerge, and can take up questions that did not exist when its mandate was written. It also retires a persistent distraction, since the temporariness of the OEWG repeatedly diverted work from substance to procedure, with delegations spending negotiating capital on what would succeed the process rather than on what the process should produce. But permanence removes, too, the artificial compression that forced states to converge on consensus text as a session expired, and that compression is precisely what produced the OEWG's outputs. Adaptive capacity is not the same as urgency: a standing body must find a substitute source of the latter if it is to keep pace with a threat landscape and a technological frontier that move faster than diplomatic cycles.
2. At the heart of the Mechanism sits a new **structure** built around two Dedicated Thematic Groups (DTGs), one on the concrete challenges of ICT security, the other on capacity building. They are meant to be informal spaces where states' perspectives and stakeholder expertise can flow in and real problems can be worked through. The curiosity is not only about how the DTGs will be structured, but about whether they will deliver to multilateralism the agility they have been tasked with providing.
3. **Stakeholder participation** has traditionally gone hand in hand with Cyber Diplomacy, and for well-established reasons: the field is unusual in that so much of the relevant expertise, and so much of the terrain itself, lies in non-state hands. The DTGs appear to be the first real attempt to build that recognition into the Mechanism's architecture. Yet what meaningful participation amounts to remains contested among Member States. During the first accreditation window, more than half of all applicants were vetoed, many of them stakeholders who have contributed to these processes for years. The signal is difficult to reconcile with the commitment, agreed by consensus, to engage stakeholders in a "systematic, sustained and substantive manner".
4. **Capacity Building** has accompanied most plenaries of the OEWG. The establishment of a dedicated thematic group signals how central the issue will be to the Mechanism's design. Looking ahead, the ambition should be to identify what is still most lacking, and whether capacity-building efforts should move beyond consolidating capacities among states to build them among stakeholders as well.
5. The OEWG did not have a mandate to address Artificial Intelligence or the broader, fast-changing landscape of **emerging and disruptive technologies**, an issue we should expect to take up space in the Mechanism. Partly because the permanent nature and versatile structure already highlighted were conceived precisely to accommodate it. But also because the Mechanism's first-biennium Chair co-chairs the newly launched Global Dialogue on AI Governance, placing cybersecurity and artificial intelligence governance, for the first time, under

EU CYBER DIRECT
euiss European Union Institute for Security Studies
Funded by the European Union

overlapping stewardship. Many of us might see that convergence as a real opportunity to bridge communities, knowledge, and processes that have developed in isolation from one another.

One thread runs through these five elements. Permanence will compound whatever inequalities the process fails to correct; the thematic groups, stakeholder access and capacity building all turn on who is able to contribute; and the convergence with AI governance risks reproducing the same divide in a second room. The test is not whether the Mechanism admits more actors, but whether those admitted can contribute substantively, and whether the delegations receiving that contribution are equipped to absorb it. Access is the easy part. Accountability is what access is for, and it is the standard against which each of these elements is assessed below.

The safe bet is that little has changed. A permanent process, on this reading, is a temporary one without an end date. But the features set out above point elsewhere. So what should we realistically expect from this new phase, and what will determine whether the Mechanism delivers more than institutional continuity?

SHIFT 01

Permanence: what it changes, and what it does not

Permanence, the first of these novel elements, resolves less than it promises. The Global Mechanism inherits the entire normative acquis of the GGE and OEWG era: the framework of responsible state behaviour, eleven voluntary norms, the applicability of international law to cyberspace, and confidence-building measures including the Points of Contact directory. It also inherits, intact, the divides that shaped two decades of negotiation. The fault line between states that consider the existing framework sufficient and in need of implementation, and those that continue to advocate new legally binding obligations, has not been bridged. It has been transferred into a permanent venue, together with a consensus rule that grants any state a de facto veto. The March 2026 organisational session offered a preview: even procedural questions, such as who appoints the co-facilitators of the thematic groups and how their agendas are set, proved contested. The first substantive session in July 2026 confirmed as much. The appointment of the thematic groups' co-facilitators divided delegations not over the individuals but over what a state-led process requires when a standing body has to take organisational decisions between plenaries, a category of dispute a time-bound process could always defer because its organisational choices expired with its mandate. Permanence removes the deadline. It does not remove the disagreement.

> "Permanence shifts expectations toward concrete implementation, rather than diverting negotiation into what should come next.

What permanence does change is the tempo and the horizon. The Mechanism will operate in five-year cycles, with annual plenaries and thematic group meetings in years one to four, followed by a review conference in year five, the chairmanship rotating on a two-year cycle within it. That review conference is a revision point, not a sunset clause. What falls due in

EU CYBER DIRECT
euiss European Union Institute for Security Studies
Funded by the European Union

year five is how the Mechanism works, not whether it continues. Permanence attaches to the institution. The architecture described here is the first cycle's configuration of it, and the review conference is where that configuration can be reopened. UN Cyber Diplomacy now has a calendar rather than a countdown, and the first session has already begun filling it in: the provisional agendas for both the 2026 and 2027 plenaries were adopted by consensus, which makes the forward schedule an agreed programme two years deep rather than a design feature on paper. That creates something the field has never had: a predictable rhythm of accountability checkpoints against which progress can be measured, rather than a perpetual renegotiation of the process itself, and an institutional memory through which positions, commitments, and capacity gaps can be tracked across cycles rather than dissolving with each mandate. This is also where the substitute for the OEWG's deadline pressure will have to come from: not the artificial urgency of an expiring mandate, but the recurring obligation to demonstrate, at fixed intervals, what has been implemented since the last checkpoint. Whether a review conference four years out disciplines negotiators as effectively as a session closing on Friday is the open question of the first cycle.

It also removes an alibi. When a process expires, disappointing outcomes can always be attributed to the clock. A standing body cannot make that argument twice. Expectations should therefore be calibrated toward implementation rather than norm production. The most plausible near-term deliverables are unglamorous but consequential: operationalising the Points of Contact directory into a functioning crisis-communication tool, developing shared understandings of how existing norms apply to concrete threats such as ransomware and attacks on critical infrastructure, and constructing a more systematic architecture for capacity building. It is against this agenda, not against treaty-making ambitions, that the Mechanism's first cycle should be judged.

SHIFT 02

The Dedicated Thematic Groups: agility by design?

If permanence changes the tempo, the structure is what will determine whether the Mechanism can use it. Alongside the annual plenary, the Mechanism establishes two Dedicated Thematic Groups, one addressing specific challenges in the cyber domain, the other focused on capacity building, scheduled to meet for the first time on 7–11 December 2026. The DTGs are designed to enable more focused, technically informed discussions than plenary diplomacy allows, feeding their outcomes back into the formal track. This is the agility the Mechanism has been tasked with delivering, and the place where the review-conference rhythm has to translate into working tempo. Whether those outcomes genuinely shape plenary decisions, or are merely noted and set aside, will be an early test of whether the two-track design feeds the plenary or simply echoes it.

The significance of this design should not be understated. By creating a standing venue in which expert briefings and stakeholder insights are expected to inform deliberations, the DTGs represent the formalisation of a demand for expertise that multilateralism in the cyber domain has long expressed only informally. States have conceded, in institutional form, what practitioners have always known: cyberspace cannot be governed at arm's length from those who build and defend it.

The legitimacy of state-led cyber governance depends on structured access to knowledge that states do not themselves possess.

> The DTGs formalise the role of non-governmental expertise in cybersecurity multilateralism.

Informality, however, is a double-edged instrument. It is what allows the groups to move faster and speak more technically than the plenary. It is also what leaves them without the authority to settle anything. And on the evidence of the opening week, it is undefined. Delegations divided at once over what informality licenses: whether sitting outside the formal track allows the groups to convene a wider range of experts than plenary accreditation permits, or whether uniform modalities must apply across every format lest differentiated rules dilute the groups' intergovernmental character and cast doubt on the standing of what they produce. Both readings are available because the term was never defined, and the one that prevails will decide how much expertise the groups can actually convene, and prevails only until the review conference, which makes the practice established in this cycle the baseline the next one inherits. A structure designed to be agile can just as easily become the place where difficult questions are parked. Which of the two the DTGs turn out to be depends less on their design than on who is permitted to populate them.

SHIFT 03

What stakeholders can contribute, and on what conditions

If the DTGs are the venue, what would stakeholders actually bring into them? In this domain the answer is unusually concrete: the organisations applying for accreditation are not commentators on the terrain under negotiation, they operate it. Incident responders, network operators, standards bodies, threat intelligence teams, and the scientific community documenting how these threats harm people hold the knowledge base on which any serious discussion of ransomware, critical infrastructure protection, or the security implications of emerging technologies has to draw.

Contribution, however, is not the same as presence. Stakeholder influence during the OEWG years was real but invisible, and invisible influence is fragile: it rests on individual relationships, cannot be evaluated by anyone, and disappears when the people who cultivated it move on. What the DTGs make possible for the first time is contribution that is **timed, targeted, and traceable**.

> Without accountability building beyond states, participation is a formality that legitimises outcomes shaped by a few.

Each word carries a requirement. **Timed** means input arrives while a text is being drafted, not after positions have hardened around whatever the most cautious states will accept. **Targeted** means delegations put specific questions to stakeholders

EU CYBER DIRECT
euiss European Union Institute for Security Studies
Funded by the European Union

where outside insight is genuinely needed, replacing ritual general statements with exchange that has a purpose. **Traceable** means the use of expertise is recorded in plenary statements and DTG reporting, so that a contribution can be evaluated rather than merely performed. None of the three is guaranteed by the modalities. All three are within the gift of the states that designed them.

The modalities themselves remain contested. Some delegations read the July 2025 consensus as providing for stakeholder participation throughout DTG discussions. Others insist that expert briefings are a possibility rather than a standard feature. And the first accreditation window sends a discordant signal: of 92 applicants, 50 were blocked, a single objection sufficing and no reason required. Many of those excluded are precisely the operators and researchers described above. The exclusions did not pass unremarked at the first substantive session, and the Chair's consultations with the objecting states left their positions unchanged. Set against the case for transparency is the argument that the non-objection procedure was itself agreed by consensus. What the exchange clarified is the stake: not whether states may object, but whether a permanent process is well served by a veto that carries no obligation to give reasons. The result is an architecture that is, in practice, two-tiered: the thematic groups open to outside expertise while the plenary, where text is agreed, is not.

Two risks follow from the same asymmetry. Engagement will gravitate toward the capacity-building DTG, where the stakeholder mandate feels natural, leaving the group on politically sensitive challenges harder to access. And in a deteriorating geopolitical climate, stakeholders may be instrumentalised rather than consulted, invoked as evidence of openness precisely as consensus becomes harder to reach. Neither is an argument against the design. Both are arguments for using it deliberately.

SHIFT 04

From Capacity Building to Cyber Accountability Building

Using the design deliberately, however, requires more than goodwill, and the Mechanism has given the reason an institutional home. Of the two Dedicated Thematic Groups, one is devoted entirely to capacity building, which means the question of who can contribute is not an ambient concern of the process but a standing item on its agenda. That is fortunate, because formalising the demand for expertise does nothing to guarantee its supply. Even if every one of the 50 blocked organisations were admitted tomorrow, the harder question would remain: admitted to do what, and with what capacity to do it? This is where capacity building stops being a matter of access and becomes a matter of accountability. Timed, targeted, and traceable contribution presupposes someone able to supply it and someone able to receive it. The modalities can guarantee neither. I have argued elsewhere[1] that supply and reception are the conditions this process has never met.

1 Calderaro, Andrea. *Cyber Accountability Building*. CyberDirect. European Union Institute for Security Studies / Stimson Center, 2024. eucyberdirect.eu/research/cyber-accountability-building

EU CYBER DIRECT
euiss European Union Institute for Security Studies
Funded by the European Union

> Accountability can only be achieved when all actors engaged in the transnational governance of the cyber domain are equally capable of negotiating the rules and commitments to which they must be accountable.

That capability has a second half. Delegations must themselves be legitimised through domestic accountability mechanisms connecting them to the industry and civil society actors with whom states share responsibility for the protection of digital infrastructure. Inclusivity, in this sense, does not merely consist of waiving restrictions to negotiating platforms: it requires that representatives from all regions have the capacity to contribute substantively. A seat at the table is not the same as a voice in the text. Without such capacity, participation remains a formality that legitimises outcomes shaped by a limited number of actors. This is why the capacity building narrative itself needs amending: from building capacity to participate, to building the conditions under which participation carries accountability. **Cyber Accountability Building**, rather than cyber capacity building.

The Global Mechanism will be tested against this standard on three fronts. The first is the one capacity building has always addressed: the more even distribution of statements achieved over the second OEWG cycle must be consolidated, since a permanent process demands sustained, not episodic, participation from delegations across Africa, Asia, and Latin America. Permanence, here, is not neutral: it accumulates whatever the process fails to correct, and capacity inequalities will now compound over five-year cycles rather than resetting with each mandate.

The second front is new, and the DTGs create it. Contribution that is timed and targeted is a skill before it is a right. Translating technical knowledge into policy-relevant language, judging when in a drafting cycle to intervene, and demonstrating concrete value to a delegation are capacities in their own right, and they are unevenly distributed. Capacity building has spent a decade narrowing a gap between states. The DTGs are about to open the same gap between stakeholders. Without deliberate intervention, the expertise flowing into the Mechanism will come predominantly from well-resourced organisations headquartered in Europe and North America, reproducing within the multistakeholder channel the very asymmetries that cyber capacity building was created to redress.

The third front is the receiving end, and it is the most neglected. Many delegations lack structured channels for engaging domestic stakeholders, arriving in New York, Geneva, or at any other negotiating table without the means to absorb, validate, or represent the expertise available within their own national ecosystems. They negotiate the governance of infrastructure they neither own nor operate. Expertise that cannot be received is no more useful than expertise that cannot be sent. Some of this surfaced at the first session in the guise of housekeeping: requests for simultaneous interpretation, and for clear rules and timelines coordinating the two thematic groups. These read as procedural minor business. They are nothing of the kind. A delegation that cannot follow a technical exchange in its working language, or that cannot cover two parallel groups with the staff it has, has

been formally included and practically excluded. Accountability is decided in details of this order at least as often as in modalities.

Responsibility on all three fronts should rest with Member States. The Global Mechanism is an intergovernmental process: states designed its architecture, control access to it, and are the guarantors of its legitimacy. Having formalised the demand for expertise, they cannot rely on donors and foundations alone to ensure it can materialise.

Framed this way, the capacity building DTG carries an unusual responsibility. It is the only body within the Mechanism whose work determines whether the other one can function: the group on concrete cyber challenges depends on expertise that the group on capacity building is charged with cultivating. Rather than treating capacity building as a portfolio of programmes delivered to states, its first agenda should ask what conditions would allow the expertise the other DTG needs to reach it, and who is currently unable to supply or receive it. A group that builds capacity everywhere except in the process it belongs to has misread its own mandate.

That work, moreover, is not done in the room. The two OEWG cycles taught a quieter lesson: the decisive exchanges often happen between sessions, in a community that stays engaged across the year rather than assembling only when the plenary meets. Consultations conducted over the past year point in the same direction. The expertise the DTGs need cannot materialise in the dedicated sessions if it has not been cultivated in the months in between. An off-cycle community that tracks the agenda, tests positions, and briefs itself continuously is what allows stakeholders to arrive already fluent and delegations to arrive already connected. Without it, participation reverts to episodic presence, the very formality that accountability is meant to replace.

SHIFT 05

AI and cyber: convergence, or parallel tracks?

The case for permanence was, at bottom, a case about pace: a standing institution was meant to let multilateralism keep step with a technological landscape that ad hoc formats could no longer track. For much of the OEWG era, however, the conversation was held within a fairly narrow frame, treating ICT security as a domain largely separable from the wider digital and technological agenda. That separation is no longer tenable. Artificial intelligence is already reshaping the very threat landscape the Mechanism exists to address, lowering the cost of offensive operations, accelerating the tempo of intrusion and defence, and introducing forms of autonomy that strain norms written for human-directed conduct. A permanent process unable to absorb this shift would inherit the OEWG's frame at precisely the moment that frame stopped holding.

Here the Mechanism enjoys an unusual, and possibly fleeting, advantage. Its first-biennium Chair also co-chairs the Global Dialogue on AI Governance, the track born of the Global Digital Compact, whose inaugural session concluded in Geneva on 6–7 July 2026. For the first time, the security of ICTs and the governance of AI sit within a single line of sight, bringing together two processes that have too often run on separate tracks while addressing overlapping communities, knowledge, and risks.

> Permanence is what allows a fast-moving technological landscape to enter the Mechanism's agenda at the pace it changes.

The opportunity is genuine, but so is the default. A shared chair creates the opportunity. It does not by itself supply a theory of convergence. Left to institutional gravity, the two conversations will simply run in parallel under one chairmanship rather than genuinely informing one another. Building the bridge requires deliberate design: drawing on a shared pool of technical expertise, cross-referencing agendas where cyber and AI risks intersect, and, above all, treating capacity building as a single problem across both tracks. The AI Dialogue's own emphasis on bridging AI divides mirrors, almost exactly, the accountability asymmetries traced above in Cyber Diplomacy. To address the same divide twice, in two rooms, would squander the one structural connection the current chairmanship makes available.

The way forward: two halves of one agenda

The two sets of commitments below are halves of a single agenda. Pursued separately they cancel out: funding and platforms without organised interlocutors produce empty channels, and well-prepared stakeholders without traceable routes into the text produce influence that vanishes again.

> Participation without organisation does not travel far in a multilateral-driven setting.

Ahead of the December DTGs, Member States should commit to an agenda of accountability-oriented capacity building on two fronts:

1. **Supply and reception.** Establish and resource national multistakeholder platforms, so that delegations arrive informed by their domestic cybersecurity ecosystems and stakeholders have a predictable channel into national positions, and create funding lines within existing cyber capacity building portfolios that complement state-led programming by reaching civil society, local industry and the technical community directly, particularly in the Global South.
2. **The discipline of the channel itself.** Following the three requirements set out above: make contribution targeted by structuring speaking opportunities around specific questions rather than ritual general statements; make it traceable by acknowledging stakeholder input in plenary statements and DTG reporting; and keep access neutral through criteria-based, regionally balanced selection of expert briefers and a transparent record of accreditation objections with reasons given, so that this year's exclusions do not become next year's default.

That agenda will only deliver if stakeholders' expertise meets it with a comparable discipline. Participation without organisation does not travel far in a multilateral-driven setting. Stakeholders should organise regionally and thematically ahead of each DTG cycle, arriving with coordinated recommendations rather than a plurality of individual interventions delegations have no way to weigh. They should take states' priorities and constraints as seriously as they expect delegations to learn from their expertise, since input pitched to a question no delegation is asking rarely reaches the text.

One commitment belongs to both. A standing community should be sustained between plenaries: an off-cycle space in which stakeholders and delegations track the agenda together, maintain contact through the intersessional period, and hold themselves accountable for staying regionally balanced rather than settling into the same circle of repeat participants. It is what allows the expertise the DTGs require to arrive already formed rather than assembled in the room, and what keeps the connection between the cyber and AI governance tracks alive as a working relationship rather than a shared chairmanship.

The Global Mechanism's permanence will shape the future of Cyber Diplomacy only if it creates more than institutional continuity. Its first cycle will show whether thematic expertise can shape political outcomes, whether access can produce accountability, and whether cyber and AI governance can address shared inequalities rather than reproduce them in parallel. The architecture now exists. Whether it delivers depends on whether states and stakeholders alike bring that discipline to it.

IMPRINT

ABOUT THE AUTHOR

Andrea Calderaro is Director of EU Cyber Direct – EU Cyber Diplomacy Initiative, at the European Union Institute for Security Studies (EUISS). Contact: Andrea.Calderaro@iss.europa.eu

HOW TO CITE THIS PUBLICATION

Calderaro, Andrea. *The Permanent Turn of the UN Global Mechanism in Cybersecurity: Five Shifts in Cyber Diplomacy, and What They Will Require*. Brussels: EU Cyber Direct, European Union Institute for Security Studies, 2026.

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

www.eucyberdirect.eu @EUCyberDirect