ENSURED

Shaping cooperation
for a world in transition

policy brief

Building Consensus Amid Growing Rivalry:

Taking Stock of UN Cyberspace Governance

Author: Federica Marconi (Istituto Affari Internazionali) and Ettore Greco (Istituto Affari Internazionali)

December 2025

Abstract

Despite growing fragmentation and mounting challenges to multilateralism, states still agree on the need for a global governance framework for cyberspace – an inherently transnational domain. Two UN initiatives have been working on drafting and implementing such frameworks: (1) the UN Open-Ended Working Group (OEWG) on the Security of and in the Use of Information and Communications Technologies and (2) the Internet Governance Forum (IGF), established via the World Summit on the Information Society (WSIS). Although both mandates were initially set to conclude in 2025, recent discussions on their renewal and broader way forward have shown an emerging consensus on the need to strengthen these fora and grant them a more stable place within the UN system. However, deeply divergent national interests and approaches may hinder meaningful progress, preventing coherent and actionable outcomes. This policy brief offers recommendations to strengthen the two instruments to ensure a robust, effective, and democratic global cyber governance.

Citation Recommendation

Marconi, Federica, and Ettore Greco. 2025. "Building Consensus Amid Growing Rivalry: Taking Stock of UN Cyberspace Governance." *ENSURED Policy Brief 8* (December): 1–9. https://www.ensuredeurope.eu.

Introduction

Cyberspace – as both a virtual and physical domain – has become a critical topic in global governance. By its very nature, cyberspace is dematerialised, transnational, and cuts across sectors, posing unique challenges to state actors. While joint efforts are necessary to regulate cyberspace globally, cyberspace governance has increasingly become a domain of state rivalry, with national interests driving regulatory processes to assert power in a competitive geopolitical and economic landscape. Furthermore, debates on the governance of cyberspace are highly sensitive, as they touch upon the core of state authority.

Although efforts to regulate cyberspace are unfolding at multiple levels, the United Nations (UN) framework has emerged as a key platform for facilitating intergovernmental negotiations and broader stakeholder engagement. Within the UN system, two main mechanisms – whose mandates are both set to end in 2025 – have been established: (1) the Open-Ended Working Group (OEWG) on the Security of and in the Use of Information and Communications Technologies and (2) the Internet Governance Forum (IGF). This policy brief examines these two mechanisms, offering an overall assessment of their outcomes so far. In particular, this brief explores the tension between safeguarding state prerogatives and advancing shared governance frameworks, as well as ongoing debates on the future of cyberspace governance.

Cyberspace governance has increasingly become a domain of state rivalry.

The OEWG and the IGF: UN Initiatives for Cyberspace Regulation

Early discussions on cyberspace regulation started in the late 1980s. The growing reliance on digital and technological infrastructures brought new issues to the fore, prompting the establishment of multilateral initiatives to address emerging concerns, including the OEWG and IGF. These mechanisms illustrate how the UN system has attempted to reconcile two interrelated challenges: the first is establishing mechanisms that are both robust enough to deliver effective and coordinated outcomes in such a security-sensitive domain, while also remaining flexible and inclusive enough to accommodate cyberspace's constantly evolving and cross-cutting nature. The second challenge is navigating the growing competition among states with diverging interests and power asymmetries, shaping both the process and the substance of international discussions on cyberspace.

The OEWG

In 1998, Russia proposed that discussions on the military use of information and communication technologies (ICT) be added to the UN agenda, as part of a broader conversation on international security. Russia's proposal reflected its growing concerns over the United States' (US) cyber warfare capabilities. To address these concerns, a Group of Governmental Experts (GGE) was established under the auspices of the UN, becoming the primary forum for interstate dialogue on developing a rules-based environment for cyberspace and applying international law to state behaviour. Between 2004 and 2017, five GGE cycles took place (2004-2005; 2009-2010; 2012-2013; 2014-2015, 2016-2017). In 2018, divergences among GGE members prompted Russia and several other UN member states to break off and propose their own resolution to the UN General Assembly, which resulted in the establishment of the OEWG in parallel to the GGE process (supported strongly by the US). From 2019 to 2021, the first OEWG (whose mandate was then renewed until the end of 2025) ran alongside the sixth and final GGE.

While democratic, the OEWG's broad platform has made reaching consensus among its diverse membership difficult.

The OEWG is a multilateral negotiation forum designed to be more open and representative than the GGE, which was widely criticised for its restricted access and state-centric nature. All 193 UN member states participate in the OEWG; non-state actors (NSAs) may provide inputs, although decision-making power only rests with states. While more democratic, this broader platform for engagement has made reaching consensus among its diverse membership difficult.

Russia views the OEWG as a results-oriented mechanism and advocates for a legally binding international treaty to regulate state behaviour in cyberspace. Together with China, it opposes informal or purely voluntary approaches, as well as the application of international humanitarian law, seeking instead to enshrine states' rights to cyber sovereignty through a new binding treaty. By contrast, the US, the EU and other Western democracies emphasise the adequacy of existing international law and promote voluntary, non-binding norms of responsible state behaviour. This divergence has characterised the entire regulatory process; as a result, some of the most contentious cyberspace issues remain unresolved.

The IGF

The IGF was established by the UN as one of the key outcomes of the World Summit on the Information Society (WSIS). Opening with summits in Geneva (2003) and Tunis (2005), WSIS is an ongoing process that aims to create an evolving multi-stakeholder platform that addresses the issues raised by ICTs. A first review of the WSIS framework took place in 2015, with the second expected by the end of 2025.

The IGF, as a product of WSIS, is a unique multi-stakeholder format that promotes openness, transparency, inclusion, and bottom-up decision-making. Unlike the GGE and the OEWG, which are state-led and intergovernmental in nature, the IGF brings together governments, the private sector, civil society organisations (CSOs), and the technical community on an equal footing.

The IGF's primary objective is to facilitate dialogue, foster partnerships, and promote the exchange of best practices to inform developments in cyber policy at the national, regional, and international levels. Importantly, the IGF does not adopt formal resolutions or promote binding treaties. Instead, its outputs serve as soft governance tools, shaping debates, influencing policy agendas, and contributing to the gradual emergence of more coherent and harmonised regulatory frameworks through its open and participatory approach.

The IGF's primary objective is to facilitate dialogue to inform cyber policy.

Achievements of the OEWG and IGF: A Mixed Picture

To date, the outcomes of these UN initiatives have been mixed, reflecting both structural limitations and persistent geopolitical tensions that hinder the development of effective global governance frameworks for cyberspace.

Building on the findings of the GGE, the OEWG has managed some tangible progress: it allows all interested UN member states to participate in negotiations and has taken steps to develop a common understanding of international law for cyberspace. Notably, the 2015 GGE report affirmed the full applicability of the UN Charter and recommended 11 voluntary, non-binding norms for responsible state behaviour – principles further reaffirmed by the final GGE consensus report in 2021.

However, at times, further progress was impeded by internal challenges. For example, the OEWG's consensus rule (i.e., any initiative must be approved by all 193 UN member states) has slowed down its ability to establish clear rules on cyberspace. Questions about the OEWG's openness and democratic character also remain. Unresolved and contentious issues are deferred to the Chair's Summary, a document that is not subject to member-state approval. Moreover, smaller participating countries often lack the resources and expertise to exert influence comparable to that of larger states.

The participation of NSAs also remains a point of contention, with Russia and China stressing the state-centric nature of UN negotiations, arguing that non-governmental stakeholders should have only a limited role, and often portraying them as proxies for states' interests. In contrast, the US and EU, as well as other like-minded countries, have championed a more inclusive approach, emphasising the essential expertise and technical knowledge that NSAs bring to ICT security discussions. This divide is also evident in the veto power that each state holds to block NSA accreditation requests. Even when non-governmental stakeholders are admitted, their participation is generally restricted to intersessional consultations.

Turning to the IGF's track record so far, the picture is similarly mixed. The IGF has helped build consensus around the idea that the internet requires mechanisms for regulation, coordination, and cooperation, and that these mechanisms should be multilateral, transparent, and democratic. The IGF has also successfully promoted accessibility and transparency in its workings. In this regard, it is widely regarded as a successful, future-proof multi-stakeholder model. Its added value lies in the capacity to foster new networks and partnerships, promote the exchange of best practices at the national, regional, and global levels, and build a shared understanding of key issues related to ICTs.

On the other hand, however, its role is somewhat limited due to its lack of a negotiating status and its inability to produce binding outcomes. Its operational effectiveness is further constricted by financial constraints, as it relies entirely on stakeholder contributions rather than on direct UN funding.

The OWEG and IGF have only achieved consensus on non-binding elements – the most sensitive issues remain unresolved.

Overall, both instruments have only been able to achieve consensus on non-binding elements with limited practical impact – the most sensitive issues remain unresolved. That being said, when looking at soft influence, the IGF has been quite impactful: thanks to its open and inclusive nature, the IGF has successfully fostered a shared understanding of critical issues and encouraged the exchange of best practices among diverse stakeholders. This process helps governments integrate insights gained through dialogue into their national policies, thereby increasing the likelihood of more convergent approaches to digital governance over time.

Next Steps, Future Trajectories

The Final Report of the OEWG (2021-2025) was adopted by consensus in July 2025, charting the UN's next steps in cyberspace governance. The report's main achievement was the establishment of a Global Mechanism on developments in the field of ICTs. This new single-track mechanism, conceived as a subsidiary body of the UN General Assembly (UNGA), is a major step forward, replacing ad hoc GGEs and OEWGs with a standing platform for continuous dialogue on responsible state behaviour. The Global Mechanism is expected to convene its first organisational session no later than March 2026 and substantive plenary sessions will be held once a year during each biennial cycle, with a review conference every five years. The work will be carried out through two dedicated thematic groups (one general and one on capacity-building).

The report also clarifies NSAs' participation in the Global Mechanism to ensure that these actors engage in "a systematic, sustained, and substantive manner." NSAs with UN Economic and Social Council (ECOSOC) status are eligible for accreditation for the Global Mechanism's plenary sessions and review conferences, while other NSAs must undergo a separate round of so-called 'non-objection accreditation', which is then valid for the duration of each five-year cycle.

As for the IGF, the WSIS+20 Review will determine its fate beyond 2025. As of today, there is broad agreement on the importance the IGF's work and the need to ensure its continuation, with the goal of making its mandate permanent. In particular, IGF's efforts to "broaden the participation of governments and other stakeholders, particularly from developing countries and under-represented groups" have been acknowledged by its members, together with the proposals for further improvements to its working modalities. These include strengthening intersessional activities, supporting national and regional initiatives, and expanding participation from all relevant stakeholders. An outcome document is expected to be adopted during the UNGA's High-Level Meeting on the Overall Review of the WSIS+20, taking place on 16-17 December 2025 (a revised version of the WSIS+20 Outcome Document, Revision 1, was published on 7 November).

There is broad agreement on the importance the IGF's work and the need to ensure its continuation.

Recommendations

The key objective of these diplomatic processes is to make the post-2025 iterations of the Global Mechanism and the IGF fit for purpose. To properly regulate cyberspace on a global scale, these mechanisms must address the internal structural and functional shortcomings, as well as confront geopolitical deadlocks that have hindered progress.

The OEWG

Looking ahead, the OEWG's efforts to strengthen global cyber governance will face both opportunities and challenges. Some key policy recommendations for the post-2025 OEWG iterations include:

1. To enhance its effectiveness, the new Global Mechanism should **bridge the internal divide** over the legal framework for responsible state behaviour, either by clarifying the relationship between existing international law and potential new norms, or by operationalising the 11 voluntary, non-binding norms that are already agreed upon.

2. The Global Mechanism should embed **accountability mechanisms** into the existing framework to monitor state conduct, which will be crucial for credibility.

3. For greater robustness, the Global Mechanism should establish a **clear, lean institutional structure** that achieves the needed synergy between plenary sessions and **avoid overlaps and duplications** between the two thematic groups.

4. Democracy and inclusiveness should be reinforced through the **sustained engagement of NSAs**, the **reform of the veto mechanism**, and expanded **technical assistance and capacity-building programmes** to ensure all countries can participate meaningfully.

The IGF

Meanwhile, the IGF must consolidate its role as the world's central platform for multi-stakeholder dialogue beyond 2025. To make this happen, the IGF should focus on addressing key challenges:

1. The IGF should secure **sustainable, diversified funding** by: (1) expanding its donor base as to include increased contributions from the largest online platforms and other private-sector actors; (2) leveraging the role of the IGF Support Association and of the Internet Society Foundation, as well as the IGF Trust Fund; (3) exploring innovative financing for digital inclusion.

2. At the same time, the IGF should secure its **independence via dedicated mechanisms** to ensure even greater transparency and accountability.

3. The IGF's effectiveness should be enhanced through **closer integration** with the UN's Global Digital Compact, more visible and **policy-relevant outputs**, and intensified efforts to **address structural barriers** to digital equality.

4. To increase its democratic legitimacy, **multi-stakeholder participation should be institutionalised** and **human rights should be integrated** across all lines of action, with the Office of the United Nations High Commissioner for Human Rights (OHCHR) providing guidance and supporting monitoring activities.

Taken together, these pathways suggest that the two mechanisms can complement one another: the OEWG as a state-led forum focused on implementation and accountability, and the IGF as a permanent, inclusive space for multi-stakeholder dialogue and norm-building. Strengthening their respective mandates, structures, and engagement practices will prove essential to ensure a resilient, effective, and democratic global cyber governance.

About ENSURED

In an era marked by global challenges, international cooperation is more essential than ever. Yet multilateral initiatives too often end in gridlock, as dominant states seek to bend the global order to their own interests. Enter ENSURED, a Horizon Europe-funded research consortium studying how the EU and its member states can better defend multilateralism and make global governance more robust, effective, and democratic.

ENSURED focuses on key policy domains that by their very nature pose complex transnational challenges. Our research assesses the state of play in these different areas and investigates the EU's strengths and weaknesses as an actor working to defend and transform multilateralism. Embracing the ethos of multilateral cooperation, the ENSURED consortium comprises universities, think tanks, and civil society groups from across Europe, Brazil, India, South Africa, China, and the United States. We aim to equip policymakers in the EU with evidence-based insights, actionable recommendations, and practical tools to promote better global governance for a world in transition.

ENSURED publications are available via the project website: https://www.ensuredeurope.eu/

Funded by
the European Union

The ENSURED project is funded by the European Union's Horizon Europe research and innovation programme under the Call HORIZON-CL2-2022-DEMOCRACY-01 – Grant agreement n° 101092077. The views and opinions expressed on this site are those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (granting authority). Neither the European Union nor the granting authority can be held responsible for them.

Copyedited by: Oliver Jung
Editorial coordination: Global Public Policy Institute (GPPi)

Reinhardtstr. 7
10117 Berlin
Germany
ensured@gppi.net