ENSURED

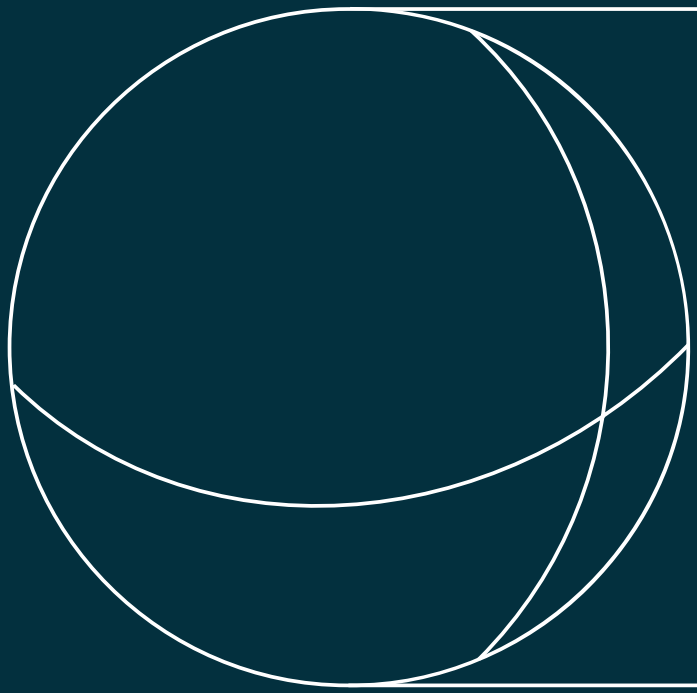
Shaping cooperation
for a world in transition

research report

Regulating Cyberspace:
UN Consensus-Building in a Fragmented Digital World

Lead authors: Federica Marconi (Istituto Affari Internazionali) and Ettore Greco (Istituto Affari Internazionali)

May 2025



Abstract

Cyberspace has become a critical area for global governance. In recent years, several efforts have been made to establish regulatory frameworks that can keep pace with its transnational and rapidly evolving nature in order to ensure the security of the technologies on which societies have become increasingly dependent. Key UN-led initiatives to regulate different areas of cyberspace include the UN Group of Governmental Experts, the Open-Ended Working Group, and the Internet Governance Forum. However, these initiatives have shown mixed results in terms of their robustness, effectiveness, and democratic participation. In many cases, their potentialities have been hindered by geopolitical tensions and geoeconomic ambitions, as well as by various state actors' efforts to impose their own visions of cyberspace regulation. As the 2025 review of these key UN processes approaches, unresolved issues persist and new challenges arise, highlighting the inherent complexity of cyberspace regulation.

Citation Recommendation

Marconi, Federica and Ettore Greco. 2025. "Regulating Cyberspace: UN Consensus-Building in a Fragmented Digital World." *ENSURED Research Report*, no. 10 (May): 1–34. https://www.ensuredeurope.eu

Table of Contents

Introduction

Cyberspace has been defined as a global domain that enables "the creation, storage, modification, exchange and exploitation of information via interdependent and interconnected networks using information communication technologies" (Kavanagh 2017, 7). In this way, cyberspace presents unique governance challenges due to its de-materialised and transnational nature, as well as its pervasiveness (Auby 2017). In 2016, NATO officially recognised cyberspace as an operational domain that requires governance and protection, alongside land, air, sea, and outer space. Moreover, its rapid technological advancements have outpaced the development of governance frameworks. Nevertheless, governments and, more broadly, the community of experts involved have generally agreed that cyberspace must be governed by the same international legal principles that govern 'physical' spaces (Henriksen 2019, 2–3).

Cyberspace has emerged as a core area for global governance, particularly as it intersects with several different policy areas.

Defining appropriate behaviour in cyberspace to ensure the safe and secure use of information and communication technologies (ICT) has become an urgent policy issue (Maurer 2011, 10). Despite its relatively recent development, cyberspace has emerged as a core area for global governance, particularly as it intersects with several different policy areas (Hofmann and Pawlak 2023). Cyberspace governance has evolved into an "emerging theatre for tensions and conflicts between States" (Kupchyna 2021), where they seek to advance their own broader geopolitical and geoeconomic ambitions (Sukuman and Basu 2024). In addressing these challenges, the United Nations (UN) regime has emerged as a key 'organisational platform' (Finnemore and Sikkink 1998, 899–900) aiming to facilitate intergovernmental negotiations and broader stakeholder engagement (Maurer 2011, 10). Discussions on ICT and its implications for international security began at the UN level in 1998.

First, beginning in that year, the Russian Federation urged the UN to include ICT in international security as a topic on its agenda out of concern that this new technology could be utilised "for purposes that are incompatible with the objectives of maintaining international stability and security and may adversely affect the security of states" (Stauffacher 2019, 2). This led to the establishment of the so-called UN Group of Governmental Experts (GGE) process under the auspices of the UN General Assembly (UNGA)'s First Committee on Disarmament and International Security. The GGE process has since become the primary avenue for interstate dialogue concerning the establishment of a rules-based environment for cyberspace (Maurer 2011) and the applicability of international law to state behaviour in the cyber domain. Five different GGE meetings took place from 2004 to 2018, when the UNGA's First Committee approved two separate proposals (UNGA 2018), which resulted in the establishment of the sixth and final GGE as well as a new UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. Operating in parallel from 2019 to 2021, these two groups addressed similar issues, including cyber norms, confidence-building measures, and the question of how international law

applies to cyberspace. However, the OEWG's mandate is more extensive, encompassing cyber threats and global IT security as well. Both groups have produced consensus reports that aim to make the normative framework for responsible state behaviour politically binding for all UN member states. The OEWG's work is ongoing, as its mandate – which was extended for another five years in 2021 (UNGA 2020) – will expire at the end of 2025.

Second, also in 1998, the International Telecommunications Union – a specialised UN agency – adopted a resolution to convene a World Summit on the Information Society (WSIS). This UN-sponsored summit was held in two phases – in Geneva in 2003 and in Tunis in 2005 – with the aim of defining a framework for global digital cooperation. While the first phase highlighted the lack of a global multi-stakeholder forum for discussing internet-related issues within existing structures and advocated for the establishment of such a forum (UN Working Group on Internet Governance 2005), the second resulted in the creation of an inclusive platform for dialogue and discussions on digital public policy: the United Nations Internet Governance Forum (IGF). Even though talks at the IGF have not dealt directly with cybersecurity, the IGF was designed to be open to governments and also – unlike traditional UN processes (Berry 2006, 4) – to the private sector and civil society organisations (CSOs) from both developing and developed countries, involving relevant intergovernmental and international organisations and fora, in line with the principle of multi-stakeholder participation on which the internet's governance ecosystem is based (Tjahja et al. 2022). The first review of the IGF process (the so-called WSIS+10; see Musiani 2013, 2–5; WSIS+10 2015) took place in 2015 and renewed its mandate for an additional 10 years (UNGA 2015a), which means that its mandate is set to expire in 2025.

This report takes stock of these UN initiatives. As both the OEWG and the IGF are nearing the conclusion of their respective mandates after years of activities and efforts, 2025 marks a critical juncture for discussions on the future governance of cyberspace. By analysing these initiatives, this report focuses on how they have attempted to resolve the tension between the robustness required to achieve common outcomes in such a strategic area and the flexibility needed to adapt to the constantly evolving nature of cyberspace as well as to ensure a democratic approach, given the far-reaching consequences of cyberspace development. Effectiveness is thus reflected not only in terms of success in reaching binding agreements, but also in creating synergies that leverage technical expertise and promote inclusive dialogue. As we see, the GGE and the OEWG illustrate the complexity of coordinating multi-faceted processes within the UN system, with the OEWG offering broader participation but also facing challenges in reaching consensus. In contrast, the IGF is a unique model – it does not take decisions, but it is instrumental in shaping debate and informing policy via its open, multi-stakeholder approach. The report then goes on to outline the key challenges in this domain and to clarify the major international actors' positions when it comes to the robustness, effectiveness, and democratic character of the cyberspace regime. The report also pays considerable attention to the EU's contribution in attempting to expand regulatory global governance in this area.

2025 marks a critical juncture for discussions on the future governance of cyberspace.

Regulating Cyberspace: A Multi-Faceted Endeavour

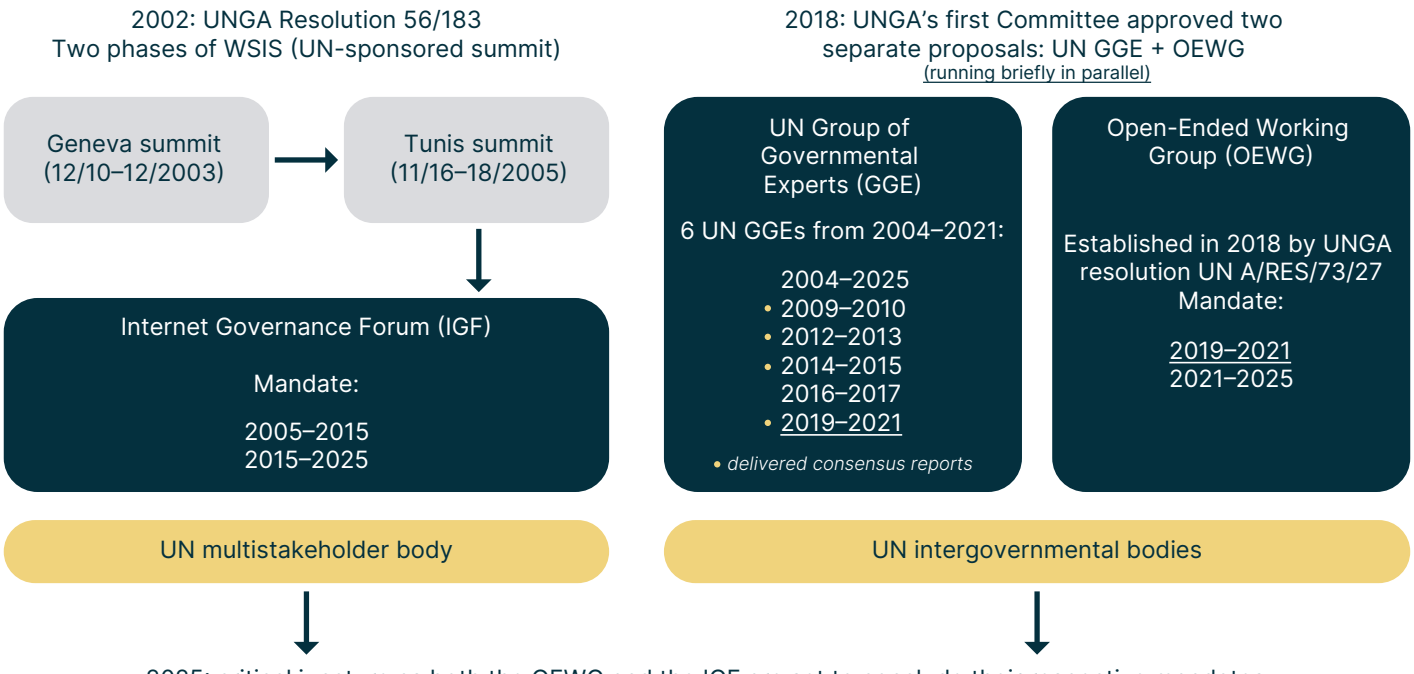
With the conclusion of the OEWG mandate and the WSIS+20 review of the IGF approaching, discussions are underway to either extend their respective mandates or establish new mechanisms, focusing on addressing the key issues that have emerged to date as well as maximising efforts in the field. Figure 1 outlines the development of today's cybersecurity regulation, including the main features and interwoven nature of the IGF, GGE and OEWG. (Also see the "Key Achievements and Future Prospects" section below.)

Applying the ENSURED conceptual framework (Choi et al. 2024) to the current situation, we assess the main features of the GGE, the OEWG, and the IGF through the lens of the three key concepts: robustness, effectiveness, and democracy.

Robustness and Effectiveness

One distinctive aspect of cyberspace governance is the need to balance the robustness required to achieve effective outcomes in such a strategic area with the flexibility necessary to adapt to its constantly evolving nature (Interview 1). Both the GGE and the OEWG present a complex and multi-layered structure, requiring coordination among multiple bodies. As

Figure 1: Key Features and Interconnections of the Major UN Initiatives on Cyberspace Governance



subsidiary bodies of the UNGA, they follow its procedural rules. The OEWG's efforts are supported by the UN Office for Disarmament Affairs (ODA), which serves as the secretariat to organise its meetings and sessions in New York. During the very first substantive sessions, the OEWG switched from formal to informal modes of work; this was due to the lack of agreement among participants on key aspects, such as the work programme and stakeholder participation. While this decision in favour of a higher degree of informality has facilitated a more open dialogue, it has also created confusion over the degree to which this aligns with the OEWG's mandate and budgetary allocations (Diplo Foundation 2024). The IGF operates with a small secretariat based in Geneva under the UN Department of Economic and Social Affairs, which receives strategic guidance from a high-level panel of 10 members representing governments, the private sector, civil society, and the technical community – all appointed by the UN Secretary-General. The secretariat's work is facilitated by the Multi-Stakeholder Advisory Group, which comprises 56 members. Despite being part of the UN, the IGF receives no direct funding from the organisation; it relies solely on contributions from stakeholders. This financial constraint limits its ability to grow and expand its operations (Interviews 5, 7, 8, and 9).

Cyberspace governance requires balancing the robustness required to achieve effective outcomes with the flexibility necessary to adapt to its constantly evolving nature.

The GGE has grown beyond the role of an expert body providing initial studies of a new topic and submitting follow-up recommendations to the UNGA: it has evolved into the primary global forum for international cybersecurity policy, taking significant steps towards a normative framework for state behaviour in the cyber domain. (Stauffacher 2019). Out of the six GGE meetings, four achieved substantive outcomes (see Table 2 below) by agreeing on reports containing conclusions and recommendations, which were welcomed by all UN member states and endorsed by the UNGA. The OEWG has built on the GGE's results to take the debate further, allowing all interested UN members to be involved and to participate in the negotiations (De Tomas Colatin 2019). However, the fact that adopting any of these reports requires reaching a consensus among all 193 UN member states has impeded progress in establishing rules for cyberspace. The OEWG has largely reiterated points made in previous GGE reports, deferring unresolved issues to the OWEG Chair's summary – a document that is not subject to member-state approval (Interview 3). The OEWG's record is mixed: it has made tangible progress in reaching a common understanding on the interpretation of international law in cyberspace, but the complexity of the topic and the breadth of issues under discussion has greatly complicated consensus-building (Interview 2).

For the past 19 years, the IGF has contributed to solidifying a growing consensus that "some form of regulation including options for self-regulation, coordination and co-operation should be welcomed" in the internet domain (UN Secretary-General 2004), and that the "international management of the Internet should be multilateral, transparent and democratic" (WSIS Executive Secretariat 2005). The primary objective of the forum is to facilitate continuous dialogue among stakeholders on emerging internet governance issues, with a view to transferring the outcomes of

this dialogue, cooperation, and partnership-building into concrete outputs to inform decision-making. However, the forum's capacity to promote meaningful change has often been called into question (Interview 5). Unlike intergovernmental bodies with mandates to negotiate, such as the GGE and the OEWG, the IGF does not produce binding agreements or norms. Efforts to make IGF insights and recommendations more politically impactful and to integrate them into intergovernmental negotiations have had limited success. Discussions about strengthening the actual impact of multi-stakeholderism are also part of the forum's ongoing review, as initiated by the UN Secretary-General (Kleinwächter 2025; Interviews 5, 6, and 9).

Democracy and Inclusion

Democratic participation has consistently been a central and contested element in the discussions surrounding the evolution of cyberspace governance. The GGE has been heavily criticised for its limited inclusivity and state-centric approach to cyber norms. It initially comprised governmental experts from 15 countries, but by 2019, it had expanded its membership to 25 countries. While all five permanent members of the UN Security Council have always been part of the group via their representatives, the other members were selected in a complex process led by the Office of the High Representative for Disarmament Affairs every time a new GGE was established (Tiirmaa-Klaar 2021).

To address these concerns, the OEWG was established as an inclusive platform, open to all UN members interested in taking part in the process. However, securing a seat at the table does not guarantee equal influence. Smaller countries often face challenges in matching the resources and expertise that larger states can leverage (Interviews 2 and 3). This imbalance affects their ability to meaningfully contribute to complex discussions. Moreover, seasoned diplomats often lack specialised knowledge of cybersecurity issues, which has created a disconnect between diplomatic language and technical expertise (Interview 2). Decision-making within the OEWG (as within the GGE) is based on consensus and only involves government representatives – the influence of non-state actors (NSAs) is quite limited. As some interviewees have pointed out, the broader range of states involved in the OEWG has made it more difficult for participants to negotiate agreements than in the smaller, closed setting of the GGE (Interviews 2 and 3).

Securing a seat at the table does not guarantee equal influence.

The GGE's mandate enabled only informal consultations with NSAs (Gavrilović 2021). From the outset, one of the most contentious issues within the OEWG has been the question of how to enhance stakeholder participation. Many members have advocated for moving beyond informal consultations with multi-stakeholders towards a more structured mechanism that would allow their participation in official sessions or specialised sub-groups (Gavrilović 2021). As a result, an open-ended dialogue on cybersecurity has been institutionalised via greater multi-stakeholder engagement, although this is limited to intersessional consultations and offers no decision-making authority. Moreover, NSAs and many of the stakeholders involved have

called for procedural improvements – such as reducing participation costs and simplifying the accreditation process – in order to facilitate the participation of smaller countries.

The concept of accountability is notably absent from the OEWG consensus report (Basu et al. 2021). No mechanisms exist to hold states accountable for actions they take in cyberspace that harm international security and stability. This makes any normative efforts largely ineffectual (Lewis 2022).

The IGF is characterised by a multistakeholder format within a democratic model, driven by the principles of openness, transparency, inclusion, and bottom-up decision-making. It operates on a global scale, with a presence in 165 countries and regions – most of which have their respective national and regional IGFs. The IGF brings together governments, private sector entities, civil society, technical communities, intergovernmental organisations (such as the OECD), and various UN agencies (such as the International Telecommunication Union, the Office of the High Commissioner for Human Rights, and UNESCO). To ensure comprehensive stakeholder engagement, the IGF holds annual meetings structured around dedicated tracks (such as the High-Level Track, the Parliamentary Track, and the Youth Track) and includes the so-called dynamic coalitions, which are informal groups that bring together members from various stakeholder communities to address specific internet governance issues. As testimony to this commitment, the number of participants has increased exponentially over the years. Nevertheless, barriers to participation persist, including resource constraints (e.g., travel costs), strict accreditation requirements (Interview 5), and general scepticism of institutionalised policymaking environments – which is motivated partly by concern that participation would only serve to "legitimize the decisions taken by other agents (corporations, governments, lobbies, etc.)" (Napoli 2008, 16). Thus, the IGF serves as a platform for discussions, information exchange, and best-practice sharing among equal participants (Interviews 7, 8, and 9).

Becoming more transparent is one of the preconditions for multilateral initiatives seeking to improve their accountability. Both the GGE and the OEWG have faced criticism for lack of transparency and public access to documents. The six GGE meetings were closed, and no other observers were permitted to attend. Moreover, meeting summaries were not available to the public, and the final reports were subject to word limits, thus restricting the detail and descriptions they contained (Ruhl et al. 2020). By contrast, since its establishment, the IGF has made significant progress in promoting accessibility. This commitment is exemplified by the introduction of captioning for primary sessions, with the aim of supporting participants with disabilities. The IGF's dedication to inclusivity and transparency has been driven predominantly by advocacy groups focused on accessibility.

Competing Visions and Approaches

Differing state interests have played a significant role in shaping discussions on cyberspace governance. Indeed, the establishment of the GGE and the OEWG was the result of several state actors' positions and their efforts to impose their own vision in the regulation of cybersecurity.

After the fifth GGE failed to reach consensus on a final report, the UNGA adopted two separate resolutions to continue discussions on responsible state behaviour in cyberspace: one presented by the US (United States et al. 2018), which resulted in the establishment of the sixth GGE, and the other sponsored by Russia (Russian Federation et al. 2018), which led to the creation of the OEWG. In particular, the US, Australia, Canada, and the EU – among others – were not satisfied with the idea that the OEWG would become the sole venue for discussing cyberspace governance (Hofmann and Pawlak 2023), and the US expressed reservations about prolonging the OEWG's mandate until 2025 (UN 2021). Fearing that sovereignty would become the dominant policy frame, they eventually committed to "defend and universalise" (Hofmann and Pawlak 2023, 2141) the GGE's acquis. In contrast, Russian representatives argued that the new OEWG aimed to avoid the creation of "club agreements" (De Tomas Colatin 2019) – whereas the US-led proposal would have been the product of the extremely narrow interests of powerful Western countries – and to acquire authority to modify existing cyber norms (De Tomas Colatin 2019) as the only forum open to all UN member states. Russia has often asserted that without its efforts, "the international community would be left with total uncertainty regarding the continuation of an inclusive and democratic negotiation process on ICT-security" (Russian Federation 2021). It has sought recognition and appreciation on the international stage for its leadership in cyber diplomacy (Barrinha and Turner 2023).

Some states urged Russia and the US to work together on these parallel processes in order to avoid redundancy (e.g., the representative from the Philippines; see UN 2018). Moreover, the US and like-minded partners favoured existing international law and voluntary/non-binding norms, while China and Russia argued that the OEWG should establish a legally binding international framework for ICT, in line with their broader ambition to promote a UN cybersecurity treaty recognising cyber sovereignty and a state's right to non-interference in its internal affairs (Bilyana and Cheravitch 2020). In this regard, Russia has also indicated its willingness to "continue to actively promote its interests, as well as the interests of its friends in the future negotiation process on ICT-security, independently of its form and of the platform at which it takes place" (Russian Federation 2024).

These contrasting approaches mirror different interests, demonstrating how cyber norms have become an area of geopolitical competition (Moynihan 2021). To illustrate this complexity, the following table synthesises the most relevant positions of key state actors regarding each of the indicators considered here, organised based on their shared stances.

Table 1: Key Positions of Major State Actors on Robustness, Effectiveness, and Democracy in Cyberspace Governance

Continued on the next page.

	UN Group of Governmental Experts (GGE)	UN Open-Ended Working Group (OEWG)
United States and European Union		
Robustness	No clear stance on robustness.	Favour an informal approach to the development of cyber norms.
Effectiveness	Support the implementation of existing non-binding norms, particularly those from the 2015 GGE (Barrinha and Turner 2023), rather than the creation of new ones.	The US concedes that the OEWG can elaborate on existing norms but argues that establishing new binding obligations exceeds its mandate (United States 2022). The EU reaffirms that a universal cybersecurity framework can only be grounded in existing international law, including the UN Charter in its entirety, international humanitarian law, and international human rights law (European Union 2020, 3–4; European Union 2021b, 1–2).
Democracy	Advocate continuing the debate within the framework of a UN GGE.	Initially opposed the OEWG, fearing it could become a platform for states with restrictive views on internet governance to exert undue influence. Support a multi-stakeholder model, allowing NSAs (including regional organisations) to participate in cyber governance.
Overall position	The US advocates a non-binding approach to cyber norms, emphasises voluntary frameworks, and strives to limit platforms that might allow authoritarian states to influence cyber governance. The EU positions itself as a champion of multilateralism and a defender of a rules-based international order (Raymond and DeNardis 2015) as a tool to address global challenges such as cybersecurity (EU 2016).	
Russia and China		
Robustness	No clear stance on robustness.	Oppose an informal approach to the development of cyber norms.
Effectiveness	Consider the legal framework that resulted from the GGE inadequate.	Russia views the OEWG as a results-oriented rather than a report-oriented platform (and prefers it over the GGE) for engaging in discussions around a legally binding international treaty. China supports the implementation of the existing framework but also calls for new norms to address evolving ICT challenges (Ministry of Foreign Affairs of the People's Republic of China 2021).
Democracy	Criticise the GGE for lacking the legitimacy to set norms and rules for the entire UN membership.	Portray the OEWG as the primary, universal, and democratic venue for global cyber discussions, using this narrative to pursue policy frameworks with sovereignty claims at their core.
Overall position	Russia and China both aim to revisit existing cyber norms and to introduce new binding commitments that more closely reflect their interests, establishing cyber sovereignty and information security as central pillars of their cyber governance approach (OEWG 2021).	

Continued from the previous page.

	UN Group of Governmental Experts (GGE)	UN Open-Ended Working Group (OEWG)
Other states		
Robustness	No clear stance on robustness.	Indonesia argues that priority should be given to the existing vehicles without inventing a new body, taking into account existing resources and current mandates.
Effectiveness	India endorses the GGE view that applying international law to cyberspace is fundamental (Deb 2021).	India reiterates the importance of a collaborative rules-based approach in cyberspace, as well as leveraging the positive momentum generated by the GGE and the OEWG (Ministry of External Affairs of India 2021). Indonesia backs the establishment of a rules-based international regime as the most appropriate solution, while also recognising the value of voluntary and non-binding norms as well as the "automatic" application of existing law (Indonesia 2020). South Africa supports the development of legally binding obligations on ICT security.
Democracy	Via the GGE, Indonesia aims to protect weak groups from cyber incidents, encourage capacity-building for these groups, and build trust among countries to prevent cyberwarfare (Fitriani 2019).	India appears to prefer state-led solutions over multi-stakeholderism (for reasons of national security) and has backed both US and Russian proposals (Centre for Communication Governance 2021). Indonesia underlines the centrality of regional organisations' contributions. South Africa stresses the importance of the OEWG to further discussions on applying international law in the context of ICT and international security.
Overall position	Other states, primarily developing countries, have not devoted significant diplomatic resources to these negotiations and have largely remained neutral or passive in cyber norms discussions (Maurer et al. 2014).	

When it comes to the IGF, the roles and positions of state actors are harder to categorise, given the different roles they play in this forum as compared to the GGE and OEWG. The creation of the IGF as a forum for enhanced cooperation was a compromise aimed at resolving the 2005 debate over whether internet governance should be led by governments (via an Intergovernmental Internet Council) or by the private sector. One key aspect of this debate was perceived US dominance in internet governance, especially due to its role overseeing the Domain Name System (DNS) root server, managed by ICANN. Some countries saw this as a violation of the UN principle of sovereign equality: to address this, the Tunis Agenda embedded a compromise in Article 68, stating that all governments should have equal roles and responsibilities in international internet governance. However, the article did not specify how this principle should be implemented (Estier 2024). Despite these developments, some governments remain dissatisfied with the current arrangements. While the US and the EU are striving for an "open, interoperable, reliable and secure information communications technology environment" (United States et al. 2018; Basu et al. 2021), China and Russia are pushing for greater state or multilateral control over the internet, particularly under the guise of combating the "dissemination of false or distorted news" (Russian Federation et al. 2018). For instance, in October 2024, Russia called for the establishment of a "distinct intergovernmental political platform" designed to discuss and take decisions on international internet governance within the UN – a return to the traditional UN process – alongside the more neutral approach that the IGF ensures (Kleinwächter 2025).

The US and EU are striving for an open technology environment; China and Russia are pushing for greater state or multilateral control over the internet.

Key Achievements and Future Prospects

Looking ahead, two distinct models have been put forward for the future of the OEWG. The first proposal (Concept Paper 2021) – co-sponsored by several states, including Russia, but notably not China – envisages a permanent OEWG as a platform for negotiations on a new cyber convention. In contrast, several Western countries have supported a second initiative – led by France and Egypt – which advocates establishing a Programme of Action (France et al. 2023). Once again, these proposals reflect competing visions of cyberspace governance and further exemplify the underlying power dynamics presented above: the first advocates the negotiation of new, legally binding obligations, the second supports voluntary commitments.

Before we consider the key features of these proposed mechanisms, the table below summarises the key achievements of the six GGEs and the OEWG, with particular attention to their respective mandates and the geopolitical contexts in which they operated (Tiirmaa-Klaar 2021; Tikk and Kerttunen 2017).

Over the years, the GGE mandate has undergone modifications. The first two GGEs were tasked with studying "existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the international information security concepts" (UNGA 2003; UNGA 2011). By 2011, the mandate included reference to "norms, rules or principles of responsible behaviour of States, and confidence-building measures with regard to information space as well as the concepts aimed at strengthening the security of global information and telecommunications systems" (UNGA 2011). By 2013, it also stressed "promoting common understandings" and included "the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States" (UNGA 2013; 2015b). Most notably, the latest iteration of the mandate, in addition to promoting common understandings, also explicitly refers to promoting "effective implementation" (UNGA 2018). The OEWG overlapped with the GGE insofar as its mandate was to further develop or change norms, rules, and principles for responsible state behaviour, as well as to address the ways in which international law applies to cyberspace. However, it placed particular emphasis on addressing confidence- and capacity-building measures as well as establishing a regular institutional open dialogue within the UN (Digital Watch 2024). Its 2021–2025 mandate includes two other crucial objectives: (1) ensuring the uninterrupted and continuous nature of the democratic, inclusive, and transparent negotiation process on security in the use of ICT; and (2) further developing ways to implement rules, norms, and principles of responsible state behaviour and, if necessary, to introduce changes to existing rules or elaborate additional ones.

Table 2: Key GEE and OEWG Achievements

● no consensus ● consensus achieved ● ongoing process

Years	Outcomes	Context
2004–2005 GGE ●	Given the complexity of the issues involved, no consensus was reached on the preparation of a final report (UNGGE Report 2005).	Permanent members of the UN Security Council were unwilling to agree on the direction of the report; this was coupled with a lack of broader international interest in cyber stability issues.
2009–2010 GGE ●	The report includes (general) recommendations focusing on (UNGGE Report 2010): • Dialogue among states to reduce risk and protect critical national and international infrastructure; • Confidence-building, stability, and risk-reduction measures; • Information exchanges on national legislation and strategies; • Elaboration of common terms and definitions concerning information security; • Capacity-building in less developed countries.	Several cyber incidents were reported in the period from 2006 to 2008 (e.g., in Georgia and Estonia), coupled with the US' cyber policy under the Obama Administration, which authorised diplomats to pursue GGE goals (i.e., the Cyberspace Policy Review in May 2009).
2012–2013 GGE ●	The report refers to the findings of the 2010 report and, for the first time, creates a general framework for responsible state behaviour in cyberspace by acknowledging that the application of norms derived from existing international law relevant to state use of ICTs is essential to reducing risks to international peace, security, and stability (UNGGE Report 2013).	US President Obama and Russian President Putin agreed to establish a new working group within the US–Russia Bilateral Presidential Commission as a part of cybersecurity confidence-building measures between the two countries.
2014–2015 GGE ●	The report (UNGGE Report 2015) expands on the recommendations of the 2013 report and additionally: • Lays out state responsibilities under existing international law, affirming the full applicability of the UN Charter; • Mentions the principles of humanity, necessity, proportionality, and distinction as elaborated in international humanitarian law; • Recommends 11 voluntary, non-binding peacetime norms of responsible state behaviour.	US President Obama met with Chinese President Xi Jinping in September 2015 and reached a bilateral agreement that neither the US or China would knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, for commercial advantage.
2016–2017 GGE ●	No consensus was reached on a final report; the right to self-defence as enshrined in Article 51 was the most contentious issue.	Russian interference in the 2016 US presidential elections impacted the relationship between the major powers.
2019–2021 GGE ●	The report reaffirms the application of international law and states that additional norms can be developed over time; it also notes the possibility that additional binding obligations may be elaborated in the future and develops a supplementary understanding of the 11 voluntary GGE 2015 norms, according to its mandate (UNGGE Report 2021).	Overarching political motivation to work towards consensus prior to the US–Russia Summit, which was scheduled to take place in Geneva in June 2021.
2019–2021 OEWG ●	The report records a rich exchange of views and new proposals, including the possibility of additional legally binding obligations (OEWG 2021), but it does not go beyond the GGE's findings.	OEWG's activities coincided with the emergence of the Programme of Action proposal; many stakeholders were hoping for more progress along these lines, but this would have to wait for the subsequent mandate (ICT for Peace Foundation 2021).
2021–2025 OEWG ●	Ongoing discussions focusing on (Gafoor 2024): • A Voluntary Checklist of Practical Actions for the implementation of voluntary and non-binding norms; • An Initial List of Voluntary Global Confidence-Building Measures.	The international environment remains challenging, with rising concerns over the malicious use of ICTs by state and non-state actors, which impacts international peace and security.

The progress made in cyberspace governance thus far, as well as the instances in which the groups have fallen short of achieving the expected outcomes, provide useful insights into the reasons for the ongoing divide in approaches to addressing these challenges. We have summarised the main features of these approaches below.

Approach 1: A State-Led, Single-Track Permanent Mechanism

The mandate of the proposal co-sponsored by Russia focuses on promoting an "open, secure, stable, accessible and peaceful ICT environment" through the practical implementation of agreements reached at the 2021–2025 OEWG. It also seeks to develop legally binding rules, norms, and principles for responsible state behaviour, as well as effective enforcement mechanisms, as fundamental elements of a future universal treaty on international information security. This approach reflects Russia's preference for a top-down, state-led method of international lawmaking in order to preserve states' status in the rule-making process, as well as its opposition to empowering transnational corporations, international non-governmental organisations (NGOs), or other NSAs in this process (Lumiste 2023). The permanent mechanism as Russia envisions it should be flexible and able to keep up with states' changing needs as well as the emergence of new tasks in ICT security. Such a mechanism should start work when the current OEWG concludes in 2025, holding two substantive sessions per year at the UN Headquarters in New York at which all UN member states can take part without exception, and adopting progress reports by consensus at the UNGA every two years.

This approach reflects Russia's preference for a top-down, state-led international lawmaking to preserve states' status in the rule-making process.

According to Russia's proposal, UN member states may decide to create subsidiary sub-groups for more detailed, in-depth consideration of specific aspects of the mandate. The governance of this permanent mechanism (which would be approved by consensus every two years) would be entrusted to a bureau composed of a chair, two vice-chairs, a rapporteur, and sub-group chairs as necessary, with membership rotating among regional groups to ensure geographic balance and inclusivity. Decision-making would be state-only and consensus-based, thus ensuring broad legitimacy while avoiding the fragmentation of international cybersecurity efforts across different platforms. In addition, the mechanism would maintain continuity with previous OEWG and GGE agreements, reinforcing and building on established cyber norms and recommendations. States would retain the leading role in decision-making, while NSAs – such as NGOs, businesses, and academic actors – would play a strictly consultative, informal role, participating only in annual intersessional meetings. Official events would be limited to accredited NSAs approved by member states in order to ensure that discussions remain state driven while allowing for expert input.

Approach 2: An Institutional Framework for Implementation and Monitoring

Initially proposed by a cross-regional group of 54 UN member states in October 2020 (Digital Watch 2024), the Programme of Action (PoA) aims to promote tailored capacity-building efforts specifically focused on the implementation of cyber norms (European Union 2023). The PoA mandate would provide the UNGA's First Committee with a single, dedicated, permanent forum for cybersecurity, which would not require subsequent iterations. This PoA would carry on the previous consensus-building efforts of the GGE and the OEWG while overseeing the implementation of the agreed frameworks, mapping and addressing any implementation challenges, and promoting continuous discussion and further development of the acquis. It would be state-led and should be flexible enough to address any additional concrete issues that would benefit from information exchange, practical implementation, and multi-stakeholder engagement.

The Programme of Action aims to promote tailored capacity-building efforts specifically focused on the implementation of cyber norms.

The First Committee has adopted the PoA resolution on cybersecurity, with a recorded vote of 157 in favour and 6 against (namely China, the Democratic People's Republic of Korea, Iran, Nicaragua, the Russian Federation, and Syria), with 14 abstentions (Digital Watch 2022). The PoA is set to be established when the OEWG concludes in 2025.

Future Mechanism: The Chair's Working Paper

Singapore's Ambassador Burhan Gafoor, Chair of the 2021–2025 OEWG, attempted to reconcile these two proposals for the future mechanism in his Third Annual Progress Report (Gafoor 2024). In this document, he outlined the key features of a "future permanent mechanism for regular institutional dialogue," to be discussed prior to the formal OEWG meetings scheduled to take place in New York from December 2021 to July 2025. The aim was to forge a compromise which would result in the adoption of the mechanism by consensus.

The revised working paper, published on May 1, 2024, shares most of the elements of the Russian proposal – particularly the idea of a single-track, state-led, permanent initiative under the UN, reporting to the UNGA's First Committee. An open, secure, stable, and peaceful ICT environment, building on consensus agreements from previous OEWG and GGE reports, is the prevailing option – even though the resolution adopted by the UNGA's First Committee in November 2022 (A/RES/78/16) demonstrated almost universal support for the PoA. As Gafoor noted, such a mechanism would further develop and implement a framework for responsible state behaviour in ICT use, addressing threats (both extant and potential), norms, international law, confidence-building, and capacity-building. With an agenda including two annual substantive sessions, biennial progress

reports, and intersessional meetings, this permanent mechanism would include dedicated thematic groups addressing key topics such as the Global Points of Contact Directory, capacity-building, and the application of international law (similarly to the sub-groups included in the Russian proposal). Operating as a subsidiary organ of the UNGA, with the UN ODA as its secretariat, this future mechanism would be led by a chair appointed for a two-year term, based on equitable geographical representation; would hold formal meetings at the UN Headquarters in New York; and would have an e-portal to facilitate its work. All decisions would be taken by states, by consensus, with a review session held every four years to assess the permanent mechanism's progress (Gafoor 2024).

Although most of the features outlined above follow the framework of the Russia-led proposal, certain elements indicate that the PoA proposal also influenced Gafoor's revised working paper. In particular, the proposed mechanism would be "open-ended," meaning that its final objective would not be the adoption of a universal treaty, as the Russia-led proposal envisioned. Legally binding obligations would be considered only if deemed appropriate by a dedicated thematic group on international law, comprising legal advisors and experts, and the working paper does not mention the development of enforcement mechanisms at all.

The modalities by which stakeholders engage and participate remain contested.

Gafoor's proposal supports NSA participation in any future institutional dialogue, while the Russian proposal limited such opportunities to the annual intersessional meetings. As in the past, the modalities for relevant NSA involvement remain a central issue in the ongoing discussions, although the final OEWG report recognised that "the broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment." In addition, the annual progress report published on June 11, 2024 states: "The OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner [...] and in line with its mandate [...] to interact, as appropriate, with other interested parties, including businesses, non-governmental organisations and academia." Nevertheless, the modalities by which stakeholders engage and participate remain contested.

The tenth substantive OEWG session on regular institutional dialogue, held in New York on February 17–21, 2025, further highlighted these primary divergences. Finland, for example, supported the proposal on stakeholder participation advanced by Canada and Chile, noting that this proposal enjoyed cross-regional backing (Finland 2025). The United Kingdom (UK) stressed that the veto repeatedly exercised by a single state (Russia) is preventing a large number of capacity-building and research organisations from participating in the OEWG. According to the UK, the UN membership as a whole should decide whether or not a stakeholder should participate. Canada and Chile have proposed that those member states which object to the participation of a particular stakeholder should provide a justification for their objection, and that the matter should then be subject to UNGA evaluation (United Kingdom 2025). By contrast, Russia "strongly opposes

the idea of starting consultations on the NGO accreditation requests that have received objections," arguing that this would undermine the no-objection procedure (veto power) and insisting on equal accreditation rules for all NGOs (Russian Federation 2025). Nevertheless, some states have complained that the principle of consensus has been abused (Permanent Mission of Mexico to the United Nations 2025).

The degree of stakeholder involvement (including private-sector stakeholders) in the future mechanism will be a central topic of the discussions planned for the remainder of 2025. As 2025 also marks the twentieth anniversary of the Tunis Agenda, the WSIS+20 review will assess the progress made thus far and present its findings to the UNGA, shaping discussions on the future of the IGF beyond 2025. After 19 iterations, the IGF is widely regarded as a successful, future-proof multi-stakeholder model. Member states will have to define the post-2025 WSIS framework. They will likely renew the IGF mandate in view of the implementation of select principles from the Global Digital Compact (GDC; see Global Digital Compact 2023). The GDC was presented to the UNGA by UN Secretary-General Antonio Guterres on June 5, 2023 as an intergovernmental process to establish a comprehensive framework for global governance of digital technology and artificial intelligence. It aims to balance multilateral and multi-stakeholder models, integrating key principles to maintain the internet as a unified global public good, upholding human rights and ensuring equal online access. Additionally, the GDC proposed a Digital Cooperation Forum, which would ensure regular assessment of GDC implementation by means of accessible maps, visuals, and policy notes, without engaging in negotiations. It would operate in a similar manner to the IGF, but with the potential to replace the multi-stakeholder IGF with a multilateral alternative (Cramer 2024).

After 19 iterations, the IGF is widely regarded as a successful, future-proof multi-stakeholder model.

However, as the WSIS+20 process considers reforms, securing sustainable IGF funding from a diversified funding base will be crucial to ensuring its neutrality and independence, and protecting it from undue influence. Despite their reliance on a stable and secure internet environment, many Very Large Online Platforms (VLOPs) – such as TikTok, Meta, Google, Apple, Alibaba, and Microsoft – make minimal contributions to the IGF budget. Increasing their financial contributions could strengthen the IGF's ability to fulfil its mission and thus enhance its global impact (Kleinwächter 2025).

The EU's Push for a New Start

Taken collectively, the EU remains among the largest contributors to the UN, with its member states financing around one-third of the total UN budget. As the European External Action Service states: "Despite challenging times over the past decade, the EU has continued and stepped up its funding to the UN system aligning its support to the global needs of our time" (European External Action Service 2024). Furthermore, the EU is one of the IGF's major supporters (UN 2025). This position was further reinforced in the context of the Council of Europe's Committee of Ministers, where member states adopted the WSIS+20 declaration and decided to extend the IGF's mandate. This declaration reaffirms the commitment to securing the human rights and fundamental freedoms enshrined in the European Convention of Human Rights (Council of Europe 2024).

The EU aims to establish an independent and autonomous mechanism in which no single state has the final word on cyberspace governance.

The EU is actively shaping the reform of the OEWG (2021–2025), which serves as an alternative to the former GGE, by helping to define the future mechanism that will replace the OEWG from 2025 onwards. These EU contributions focus on strengthening robustness, effectiveness, and democratic principles. As an enhanced permanent observer within the UN system, the EU profits from its privileged status and coordinates its 27 member states to present unified positions, with a number of non-EU countries – including members of the European Free Trade Association and countries in Eastern Europe – regularly aligning with the EU's statements on ICT in the context of the OEWG.

In terms of robustness, the EU has reiterated its support for the creation of a "permanent, action-oriented, inclusive, transparent, and results-based mechanism" (EU 2023). By advocating for a more structured, permanent mechanism, the EU aims to promote a more consistent operational framework. Moreover, its ongoing support for the OEWG confirms its commitment to this process. As for governance autonomy (that is, the degree to which institutional agents are insulated from the influence of certain member states in their resource management and decision-making processes), the EU aims to establish an independent and autonomous mechanism, supporting the PoA proposal, in which no single state has the final word on cyberspace governance (European Union 2024a).

The EU supports the OEWG's goal of continuing the development of rules and norms that began under the auspices of the GGE. Most importantly, on November 18, 2024, the Council of the European Union published a declaration reaffirming its position with respect to the application of international law in cyberspace (Council of the EU 2024). The EU has (*inter alia*) also pledged to support national implementation programmes by undertaking capacity-building initiatives. Once again, the EU's support for these initiatives, as well as for the PoA, represents a significant attempt to further legitimise the whole process.

Pointing to the clash between major international actors as illustrated above, the EU wants future OEWG work to be based solely on proposals that enjoy the broadest possible support (European Union 2024b). With this in mind, the EU has reiterated its support for the PoA as its favourite option for the future permanent mechanism. Among other things, EU officials have welcomed the creation of 'dedicated working groups' (which constitute an effectiveness-oriented approach) that would serve to build cyber resilience, increase cooperation, and eventually ensure stability in cyberspace (European Union 2024a).

The EU has adopted a strong multi-stakeholder approach in order to increase legitimacy in governance efforts.

As for the two key indicators of democracy – democratic participation and democratic accountability – the EU has adopted a strong multi-stakeholder approach in order to increase legitimacy in governance efforts. The EU's support for inclusive dialogue and cooperation on cyberspace governance brings academic actors, CSOs, businesses, and the tech community to the table. EU statements frequently emphasise inclusivity and transparency, as well as the need to ensure that all stakeholders participate meaningfully and that decision-making processes are open and clear. The EU has embraced the principle of "a voice but not a vote," whereby stakeholders are allowed to participate but not to cast a vote. In this light, the OEWG has been seen as a "meaningful avenue to express that voice more fairly and with more integration" (European Union 2024a).

The EU has further demonstrated its influence in ensuring that bureaucracy is representative, reflecting fair and democratic member-state participation. It has frequently emphasised the need for capacity-building measures to ensure effective participation by all countries, offering technical assistance, training, and resources to strengthen capabilities in cybersecurity and ICT governance. These efforts reflect the EU's commitment to fostering a more inclusive and representative governance structure, equipping less-developed countries with the necessary means to actively engage in discussions.

The EU has advocated for including a wide range of stakeholders in the OEWG to ensure a diversity of perspectives."

In terms of the depth and range of access opportunities (both *de jure* and *de facto*) granted to NSAs, the EU has advocated for including a wide range of stakeholders in the OEWG – including CSOs, the private sector, and academic actors – to ensure a diversity of perspectives. To this end, the EU has also strongly advocated for the establishment of public–private partnerships, leveraging private-sector knowledge and experience to strengthen response systems, protect national interests (such as infrastructures), and adhere to the UN framework for responsible state behaviour.

Given its nature, the OEWG makes it difficult to apply the ENSURED parameters mentioned above to this body. In terms of accountability, the EU has consistently argued that the annual progress reports issued by the OEWG Chair should be published (European Union 2021a).

Internally, the EU has recently adopted its own legislation addressing cybersecurity and safety in the internet environment. Notable examples include the 2019 Cybersecurity Act and the NIS-2 Directive. The former aims to achieve high levels of cybersecurity, resilience, and trust within the EU by strengthening the mandate of the European Union Agency for Cybersecurity (ENISA). The latter aims to achieve a high level of cyber security across the EU, specifically to improve the functionality of the internal market. In particular, the NIS-2 Directive lays down obligations for member states to adopt national cybersecurity strategies and to establish national cybersecurity governance and response bodies for the purpose of enhancing cyber capabilities, risk management and reporting, and information exchange. Also worth mentioning as an example of EU cyber diplomacy is EU Cyber Direct, which organises events that take place adjacent to OEWG intersessional meetings.

Conclusion: The Future of Cybersecurity Governance

By its very nature, cyberspace is de-materialised and de-territorialised, transcending the physical boundaries of national systems and permeating multiple sectors. It also undergoes continuous and rapid evolution. This makes effective regulation of cyberspace a unique and daunting challenge. There is widespread recognition among scholars, practitioners, and experts in the field that cyberspace is a truly global domain and requires appropriate governance mechanisms, but the conflicting interests of multiple actors make global consensus-building and cooperation extremely complex. The positions of state actors often reflect their entrenched geopolitical interests as well as their quest for technological supremacy and competitive economic advantages. Taken together, these various elements lead to a fundamental contradiction. On the one hand, we see increasing efforts to develop common solutions within multilateral fora; on the other, state actors remain reluctant to compromise on politically sensitive issues due to their divergent interests. These persistent divergences, along with the difficulties inherent in reaching consensus, have weakened the efficiency of global cyber governance and resulted in legal frameworks that are often diluted and lack enforceability. According to the key concepts of the ENSURED project, as applied in this report, the evolving landscape of cyberspace governance reveals an ongoing tension between the need for robust, effective outcomes and the flexibility required to navigate the dynamic nature of cyberspace. GGE and OEWG processes have underscored the structural and political complexities of achieving consensus in multilateral settings, while the IGF has provided a distinct, non-binding forum that fosters open, multi-stakeholder dialogue. Taking stock of these different initiatives, it is clear that in an area such as cyberspace, effectiveness is not solely indicated by achieving binding agreements, but also by establishing synergies that leverage technical expertise and promote inclusive dialogue. In the latter respect, democratic participation remains a contested yet essential component across all formats, and inclusiveness proves to be both a strength and a challenge.

The core principles of cybersecurity governance are inherently tied to global power structures.

The core principles of cyberspace governance are inherently tied to global power structures. While the OEWG will continue attempting to create at least minimal areas of agreement – particularly on capacity- and confidence-building measures, as well as information sharing – the competition between voluntary, non-binding norms (favoured by Western countries) and legally binding international treaties (advocated first and foremost by Russia) is likely to persist. The IGF will continue to be a platform for the exchange of information and views as well as for broader stakeholder involvement. The results of discussions in this forum have the potential to influence policymaking.

While consensus at the global level remains elusive, an increasing number of regional and like-minded state agreements will continue to emerge. For instance, the EU has once again demonstrated its support for multilateralism as a major financial contributor and political actor within the UN system, actively supporting more durable, inclusive, and action-oriented governance mechanisms. The EU's consistent advocacy of multi-stakeholder cooperation – including CSOs, academic actors, businesses, and the tech community – positions it as a champion of both robust coordination and democratic legitimacy in global cyberspace governance.

The future of cyberspace will likely be defined by coexisting, sometimes competing governance structures.

Concurrently, NSAs are likely to take on an increasingly prominent role, although their involvement will remain subject to significant political dynamics and government contestation (Herbst and Jakobi 2024). For instance, the Swiss Federal Department of Foreign Affairs (FDFA – EDA) and the Diplo Foundation have developed the "Geneva Manual" (Geneva Dialogue on Responsible Behaviour in Cyberspace 2023) as a handbook to clarify the roles and responsibilities of NSAs in cyberspace, building on the results of the GGEs and the OEWG. At the regional level, cyberspace governance initiatives have emerged within the ASEAN Regional Forum, the Organisation of American States, and the Organization for Security and Co-operation in Europe (Ott and Osula 2019). Furthermore, coalitions of like-minded states may produce plurilateral agreements, such as the Paris Call for Trust and Security in Cyberspace or the Quad Cybersecurity Partnership (comprising the US, India, Japan, and Australia), which aim to advance common cybersecurity norms and practices (Henriksen 2017). Given that much of cyberspace infrastructure is privately owned, private-sector stakeholders such as Microsoft and Siemens have spearheaded efforts to self-regulate and to shape international governance discussions.

While efforts to build shared global frameworks will continue, they will be constrained by competing national interests and geopolitical tensions. Rather than a singular, enforceable global governance model, the future of cyberspace will likely be defined by coexisting, sometimes competing governance structures in which certain agreements find traction among like-minded actors.

List of Interviews

Number	Date	Interviewee	Location
1	12/20/2024	Non-state expert	Online
2	01/14/2025	Non-state expert	Online
3	01/23/2025	Government official	Online
4	01/02/2025	Non-state expert	Online
5	01/31/2025	IO official	Online
6	01/31/2025	Non-state expert	Online
7	02/07/2025	Non-state expert	Online
8	02/07/2025	IO official	Online
9	02/07/2025	IO official	Online
10	02/20/2025	IO official	Online

References

Auby, Jean-Bernard. 2017. "Chapter 2: Areas of Legal Globalisation." In *Globalisation, Law and the State*, 29-47. London: Hart Publishing.

Barrinha, André and Rebecca Turner. 2023. "Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India." *Contemporary Security Policy* 45 (1): 1–6.

Basu, Arindrajit, Irene Poetranto, and Justin Lau. 2021. "The UN Struggles to Make Progress on Securing Cyberspace." Carnegie Middle East Center. https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace?lang=en&center=middle-east.

Berry, John. 2006. "The World Summit on the Information Society (WSIS): A Global Challenge in the New Millennium." *Network of Illinois Learning Resources in Community Colleges* 56: 1–15.

Bilyana, Lilly and Joe Cheravitch. 2020. "The Past, Present, and Future of Russia's Cyber Strategy and Forces." In *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*, edited by Tatiana Jancarkova, L. Lindstrom, M. Signoretti, I. Tolga, and G. Visky, 129–155. Tallinn: NATO CCD COE Publications.

Centre for Communication Governance. 2021. "Cyber Security at the UN: Where Does India Stand?" The CCG Blog. https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2/.

Choi, Ha Eun, Hylke Dijkstra, Andrea Liese, Thomas Sommerer, and Clara Weinhardt. 2024. "EU Support for Robust, Effective, and Democratic Global Governance: A Conceptual Framework." *ENSURED Research*, no. 4 (July): 1–44. https://www.ensuredeurope.eu/publications/conceptual-framework.

Council of Europe. 2024. "The Council of Europe supports the extension of the IGF mandate. Freedom of Expression." https://www.coe.int/en/web/freedom-expression/-/meeting-of-the-ministers-deputies-on-25-september-2024.

Council of the EU. 2024. "Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace." Press release, Council of the EU. https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/.

Cramer, Dana. 2024. "Assessing the Near Future of Multistakeholder Internet Governance." Centre for International Governance Innovation. https://www.cigionline.org/static/documents/DPH-paper-Cramer.pdf.

De Tomas Colatin, Samuele. 2019. "A surprising turn of events: UN creates two working groups on cyberspace." The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

Deb, Sidharth. 2021. "Cyber Security at the UN: Where Does India Stand? (Part 2)." The CCG Blog. https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2/.

Digital Watch. 2022. “Resolution on the programme of action (PoA) on cybersecurity adopted.” https://dig.watch/updates/resolution-on-the-programme-of-action-poa-on-cybersecurity-adopted.

—. 2024. “Geneva Internet Platform: OEWG’s ninth substantive session: Limited progress in discussions.” https://dig.watch/updates/oewgs-ninth-substantive-session-limited-progress-in-discussions.

Diplo Foundation. 2024. “What’s new with cybersecurity negotiations: OEWG 2021–2025 second substantive session.” https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-second-substantive-session/.

Estier, Malou. 2024. “The Relevance of WSIS & IGF for International AI Governance.” Simon Institute. https://www.simoninstitute.ch/blog/post/the-relevance-of-wsis-igf-for-international-ai-governance/.

European Union. 2016. “Global Strategy. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union’s Foreign and Security Policy.” European External Action Service. https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en.

—. 2020. “Joint comments from the EU and its Member States on the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.” UN Office for Disarmament Affairs. https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf.

—. 2021a. “EU Key Messages. United Nations Open-ended Working Group on ICT: Formal Session.” OEWC. https://www.eeas.europa.eu/delegations/un-new-york/eu-key-messages-%E2%80%93-united-nations-open-ended-working-group-ict-formal-session_en?s=63.

—. 2021b. “Key EU messages, OEWG virtual session on Zero-draft.” UN Office for Disarmament Affairs. https://disarmament.unoda.org/open-ended-working-group/.

—. 2023. “EU Statement – UN Open-Ended Working Group on ICT: Regular Institutional Dialogue.” European External Action Service. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-regular-institutional-dialogue_en?s=63.

—. 2024a. “EU Statement – Open-Ended Working Group on ICT: International Law.” European External Action Service. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-––open-ended-working-group-ict-international-law_en?s=63.

—. 2024b. “EU Statement – Open-Ended Working Group on ICT: Regular Institutional Dialogue.” European External Action Service. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-open-ended-working-group-ict-regular-institutional-dialogue_en.

European Union External Action Service. 2024. “EU Funding to the UN system, 20 September 2024.” https://www.eeas.europa.eu/eeas/eu-funding-un-system_en.

Finland. 2025. “Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021–2025, Tenth Substantive Session, February 2025, Agenda item: 5 (Regular Institutional Dialogue).” UN Office for Disarmament Affairs. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Finland's_Statement_in_OEWG_10th_session_Regular_institutional_dialogue.pdf.

Finnemore, Martha and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change.” *International Organization* 52 (4): 887–917.

Fitriani. 2019. “Indonesia and Global Cyber Norms.” Kompas.id, December 13, 2019. https://www.kompas.id/baca/english/2019/12/13/indonesia-and-global-cyber-norms/.

France et al. 2023.“Programme of action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security.” A/RES/77/37. Cosponsored by Albania, Argentina, Australia, Austria, Belgium, Bulgaria, Chile, Colombia, Croatia, Cyprus, Czechia, Denmark, Dominican Republic, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Paraguay, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Senegal, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Türkiye, Ukraine, United Kingdom of Great Britain and Northern Ireland, and the United Republic of Tanzania. UN Office for Disarmament Affairs. https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Eighth_session_(2023)/77-37-France-EN.pdf.

Gafoor, Burhan. 2024. “[DRAFT] Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security.” UN Office for Disarmament Affairs. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_1_May_2024_0.pdf.

Gavrilović, Andrijana. 2024. “What’s new with cybersecurity negotiations? The second cyber OEWG’s organisational session.” Diplo Blog. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-second-cyber-oewgs-organisational-session/.

Geneva Dialogue on Responsible Behaviour in Cyberspace. 2023. “Geneva Manual.” https://genevadialogue.ch/geneva-manual/.

Global Digital Compact. 2023. “Secretary-General’s policy brief on a Global Digital Compact: An open, free and secure digital future for all.” United Nations. https://indonesia.un.org/sites/default/files/2023-07/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf.

Henriksen, Anders. 2019. “The end of the road for the UN GGE process: The future regulation of cyberspace.” *Journal of Cybersecurity* 5 (1): 2–3.

Herbst, Lena and Anja P. Jakobi. 2024. “Opening up or closing down? Non-state actors in UN cybersecurity governance.” *Journal of Global Security Studies* 9 (3): 26.

Hofmann, Stephanie and Patryk Pawlak. 2023. “Governing cyberspace: Policy boundary politics across organizations.” *Review of International Political Economy* 30 (6): 2122–2149.

ICT for Peace Foundation. 2021. “The OEWG final report: Some progress, much remains unresolved.” https://ict4peace.org/wp-content/uploads/2021/03/OEWG-FinalReportAnalysisMar212021PM.pdf.

Indonesia. 2020. “Indonesia’s Response on the Pre-Draft Report of the UN OEWG on the Developments in the Field of ICT in the Context of International Security.” UN Archives and Records Management. https://front.un-arm.org/wp-content/uploads/2020/04/indonesia-respose-to-oewg-ict-initial-pre-draft.pdf.

Kavanagh, Camino. 2017. "The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century." UN Institute for Disarmament Research, Resource 7. https://unidir.org/publication/the-united-nations-cyberspace-and-international-peace-and-security-responding-to-complexity-in-the-21st-century/.

Kleinwächter, Wolfgang. 2025. "Internet Governance Outlook 2025: Unbordered Spaces vs. Bordered Places." *CircleID blog*, January 16, 2025. https://circleid.com/posts/internet-governance-outlook-2025-unbordered-spaces-vs-bordered-places.

Kupchyna, Alena. 2021. "Confronting the challenges of working in cyberspace." Organization for Security and Co-operation in Europe. https://www.osce.org/blog/confronting-the-challenges-of-working-in-cyberspace.

Lewis, James Andrew. 2022. "Creating Accountability for Global Cyber Norms." Centre for Strategic and International Studies Report. https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

Lumiste Liina. 2023. "There and back again? Russia's Quest for Regulating War in Cyberspace." *Polish Yearbook of International Law* 43: 239–60.

Maurer, Tim. 2011. "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security." *Science, Technology, and Public Policy Program*, Belfer Center: 2–68. https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security.

Maurer, Tim, Robert Morgus, Georgia Bullen, and Danielle Kehl. 2014."Visualizing Swing States in the Global Internet Governance Debate." New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/visualizing-swing-states-in-the-global-internet-governance-debate/.

Ministry of External Affairs of India. 2021. "Foreign Secretary's Statement at the UN Security Council Open Debate on Maintenance of International Peace and Security: Cyber Security, June 29, 2021." Government of India, Ministry of External Affairs, Speeches and Statements. https://www.mea.gov.in/Speeches-Statements.htm?dtl/33963.

Ministry of Foreign Affairs of the People's Republic of China. 2021. "China's Positions on International Rules-making in Cyberspace." UN Office for Disarmament Affairs. https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf.

Moynihan, Harriet. 2021. "Power Politics Could Impede Progress on Responsible Regulation of Cyberspace." Chatham House. https://www.chathamhouse.org/2019/12/power-politics-could-impede-progress-responsible-regulation-cyberspace.

Musiani, Francesca. 2013. "WSIS+10: The self-praising feast of multi-stakeholderism in internet governance." *Internet Policy Review* 2 (2): 2–5.

Napoli, Philip N. 2008. "Issues and Challenges Facing Internet Governance: A Report from the 2007 Internet Governance Forum." The Donald McGannon Communication Research Center, Fordham University. https://research.library.fordham.edu/mcgannon_working_papers/14/.

NATO. 2016. “Warsaw Summit Communiqué – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016.” https://www.nato.int/cps/cn/natohq/official_texts_133169.htm.

OEWG. 2021. “2019–2021 final substantive report.” Digital Watch. https://dig.watch/resource/oewg-2019-2021-final-substantive-report.

Ott, Nicholas and Anna-Maria Osula. 2019. “The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level.” *11th International Conference on Cyber Conflict: Silent Battle*, edited by Tatiana Jancarkova, L. Lindstrom, M. Signoretti, I. Tolga, and G. Visky, 1–25. Tallinn: NATO CCD COE Publications.

Permanent Mission of Mexico to the United Nations. 2025. “Mexico’s Statement on the future regular institutional dialogue in the context of the 10th Substantive Session of the Open-Ended Working Group on Security of and in the use of ICTs 2021–2025.” UN Office for Disarmament Affairs. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/SPA-ENG_Intervenci%C3%B3n_de_M%C3%A9xico._RID_1.pdf.

Raymond, Mark. 2019. “Rules for State Conduct in the Cyber Domain.” In *Social Practices of Rule-Making in World Politics*, 203–235. New York: Oxford Academic.

Raymond, Mark and Laura DeNardis. 2015. “Multistakeholderism: Anatomy of an inchoate global institution.” *International Theory* 7 (3): 572–616.

Republic of Belarus et al. 2021. “Concept paper on a permanent decision-making Open-ended Working Group on security of and in the use of information and communications technologies.” Cosponsored by Republic of Belarus, Burkina Faso, the Republic of Burundi, the Republic of Cuba, the Democratic People’s Republic of Korea, the State of Eritrea, the Republic of Mali, the Republic of the Union of Myanmar, the Republic of Nicaragua, the Russian Federation, the Syrian Arab Republic, the Republic of Sudan, the Bolivarian Republic of Venezuela, and the Republic of Zimbabwe. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_paper_on_a__Permanent_Decision-making_OEWG.pdf.

Ruhl, Christian, Duncan Hollis, Wyatt Hoffman, and Tim Maurer. 2020. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.” Carnegie Endowment for International Peace, February 26, 2020. https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en.

Russian Federation. 2021. “Statement by Dr. Vladimir Shin, Deputy Director, Department of International Information Security, Ministry of Foreign Affairs of the Russian Federation, at the online-consultations of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.” UN Office for Disarmament Affairs. https://front.un-arm.org/wp-content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-19.02.2021.pdf.

—. 2024. “Statement by the Russian delegation at the eight session of the UN Open-Ended Working Group on Security of and in the use of ICTs 2021–2025.” UN Office for Disarmament Affairs.

—. 2025. “Statement by the Russian Interagency Delegation at the Tenth Session of the UN Open-Ended Working Group on Security of and in the use of ITCS 2021–2025.” UN Office for Disarmament Affairs. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_RID_-_ENG.pdf.

Russian Federation et al. 2018. “Developments in the field of information and telecommunications in the context of international security – Algeria, Angola, Azerbaijan, Belarus, Bolivia (Plurinational State of), Burundi, Cambodia, China, Cuba, Democratic People’s Republic of Korea, Democratic Republic of the Congo, Eritrea, Iran (Islamic Republic of), Kazakhstan, Lao People’s Democratic Republic, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Pakistan, Russian Federation, Samoa, Sierra Leone, Suriname, Syrian Arab Republic, Tajikistan, Turkmenistan, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe.” A/C.1/73/L.27.Rev.1. https://digitallibrary.un.org/record/1650510?v=pdf.

Stauffacher, Daniel. 2019. “UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes.” ICT for Peace Foundation. https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf.

Sukumar, Arun and Arindrajit Basu. 2024. “Back to the Territorial State: China and Russia’s Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order.” *Journal of Cyber Policy* 9 (2): 256–87.

Tiirmaa-Klaar, Heli. 2021. “The Evolution of the UN Group of Governmental Experts on Cyber Issues. From a Marginal Group to a Major International Security Norm-Setting Body.” *The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace – Cyberstability Paper Series*: 2–14. https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

Tikk, Eneken and Mika Kerttunen. 2017. “The Alleged Demise of the UN GGE: An Autopsy and Eulogy.” Cyber Policy Institute. https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf.

Tjahja, Nadia, Trisha Meyer, and Jamal Shahin. 2022. “Who do you think you are? Individual stakeholder identification and mobility at the Internet Governance Forum.” *Telecommunications Policy* 46 (10).

UN Secretary-General. 2004. “Report of the International Telecommunication Union on information and communication technologies statistics: note/by the Secretary-General.” E/CN.3/2004/16: 4.

UN Working Group on Internet Governance. 2005. “Preliminary report of the Working Group on Internet Governance/Working Group on Internet Governance.” UN Digital Library. https://digitallibrary.un.org/record/542570?v=pdf.

UN. 2018. “First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct.” GA/DIS/3619. Meetings Coverage and Press Releases. https://press.un.org/en/2018/gadis3619.doc.htm.

—. 2021. “Compendium of statements in explanation of position on the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 25 March.” A/AC290/2021/INF/2.

—. 2025. “Department of Economic and Social Affairs, Internet Governance Forum.” https://www.intgovforum.org/en/content/donate.

UNGA. 2003. “Resolution adopted by the General Assembly on 8 December 2003.” A/RES/58/32.

—. 2005. “Resolution adopted by the General Assembly on 8 December 2005.” A/RES/60/45.

—. 2011. “Resolution adopted by the General Assembly on 2 December 2011.” A/RES/66/24.

—. 2013. “Resolution adopted by the General Assembly on 27 December 2013.” A/RES/68/243.

—. 2015a. “General Assembly Resolution 70/125 UN General Assembly. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society.” A/70/L.33.

—. 2015b. “Resolution adopted by the General Assembly on 23 December 2015.” A/RES/70/237.

—. 2018. “Resolution adopted by the General Assembly on 5 December 2018.” A/RES/73/27.

—. 2020. “Resolution adopted by the General Assembly on 31 December 2020.” A/RES/75/240.

UNGGE. 2005. “Report of the Secretary General, United Nations, Submitted by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/60/202.

—. 2010. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/65/201.

—. 2013. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/68/98.

—. 2015. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/70/174.

—. 2021. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/76/135.

United Kingdom. 2025. “Consolidated Statements by the United Kingdom at the Tenth Session of the Open-Ended Working Group on Security of and in the Use of ICTs.” UN Office for Disarmament Affairs. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UK_statements_at_Tenth_Session_OEWG.pdf.

United States. 2022. “United States Remarks for March 2022 session of the OEWG, as prepared.” UN Office for Disarmament Affairs. https://documents.unoda.org/wp-content/uploads/2022/04/US-remarks-for-March-OEWG-norms.pdf.

United States et al. 2018. “Advancing Responsible State Behaviour in Cyberspace in the Context of International Security – Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, United Kingdom of Great Britain and Northern Ireland and United States of America.” A/C.1/73/L.37.

Weber, Valentin. 2022. “How to Strengthen the Program of Action for Advancing Responsible State Behavior in Cyberspace.” Just Security, February 10, 2022. https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace/#:~:text=The%20Programme%20of%20Action%20%28PoA%29%2C%20a%20proposal%20initiated,cyberspace%20based%20on%20multi-stakeholderism%2C%20capacity-building%2C%20and%20democratic%20norms.

WSIS Executive Secretariat. 2005. “Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16–18 November 2005.” World Summit on the Information Society. https://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf.

WSIS+10. 2015. “Summary report from the UN GA WSIS review meeting.” Digital Watch. https://dig.watch/wp-content/uploads/2021/12/WSIS10SummaryReport.pdf.

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. Views and opinions expressed are, however, 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.

Edited by: Dr. Alissa Jones Nelson
Editorial coordination: Global Public Policy Institute (GPPi)

Reinhardtstr. 7
10117 Berlin
Germany
ensured@gppi.net