Lillestrøm IGF Messages

The **20th annual meeting of the Internet Governance Forum** was hosted by the Kingdom of Norway in Lillestrøm from 23 to 27 June 2025.

The **Lillestrøm IGF Messages** provide a high-level overview for decision-makers of current thinking on key Internet governance and digital policy issues. They are sourced directly from 262 sessions held during IGF 2025. Session organizers were invited to self-identify key takeaways and call-to-action points at the end of their session as input for these messages. The Messages were also informed by reports from National, Regional and Youth IGF initiatives.

A set of draft messages, curated by the IGF Secretariat, was published on 27 June for community review until 14 July. The final IGF 2025 Messages are part of the annual meeting's outcomes.

The Forum was held under the overarching theme of ***Building Digital Governance Together***. Sessions were organised within four main themes:

- **[Building] Digital Trust and Resilience**
- **[Building] Sustainable and Responsible Innovation**
- **[Building] Universal Access and Digital Rights**
- **[Building] Digital Cooperation**

The messages in this document are structured accordingly.

Disclaimer: the views and opinions expressed in this document do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Table of content

Lillestrøm IGF Messages and other IGF outcomes

The **Lillestrøm IGF Messages** capture views expressed by the multistakeholder community during the IGF meeting. The reports that sourced these messages are available at https://intgovforum.org/en/content/igf-2025-outputs.

The Lillestrøm IGF Messages are complementary to outputs and observations compiled by other tracks; these are listed at https://intgovforum.org/en/content/igf-2025-outputs.

[Building] Digital Trust and Resilience

The theme

GDC 3, 4, 5 - WSIS C5, C9, C10 - SDGs 9, 16, 12, 17; Cybersecurity and Trust, Data Governance, Artificial intelligence, Media and Content, Rights and Freedoms [Capacity Building]

A resilient, interoperable and trustworthy Internet is critical to ensuring that communication infrastructure, services and data exchange remain stable and secure in the face of growing cyberthreats and disruptions to digital infrastructures. Misinformation, disinformation, hacked data, hate speech, misuse of private information, biased AI responses, and other confusing and imprecise elements of information are commonplace challenges to the Internet we use and enjoy.

IGF Lillestrøm messages

Digital infrastructure

- As reliance on digital services increases, tolerance for disruptions has declined. Peering and transit are essential for robust interconnection, enabling faster and more reliable Internet. Strong cooperation between governments and private infrastructure owners is critical to ensure resilience and strengthen and expand digital infrastructure.

- It is necessary to map the different crisis response models and mechanisms within the United Nations system and beyond, and to analyse how they can be extrapolated to respond to situations where communications are disrupted, and critical internet infrastructure is attacked in conflict and crisis zones. The establishment of a multi-stakeholder mechanism to ensure funding, political commitment, and other factors should allow to respond effectively, in a timely manner, and within the frameworks of international law on human rights protection and humanitarian assistance.

- The multistakeholder community's commitment to an open and interoperable Internet holds strong potential for action to ensure civilian access and secure core Internet infrastructure in contexts of conflict and crisis. However, it also faces significant limitations. Likewise, normative and regulatory frameworks, including international humanitarian and human rights law, offer important tools but are not without their own constraints. The Internet Governance Forum (IGF) and its Best Practice Forum should serve as a space where they connect, interact, and reinforce one another to address these critical challenges.

- The resilience of the global subsea cable network depends on proactive planning, built-in redundancy, and the capacity for rapid incident response. As threats to undersea cable infrastructure transcend national borders, regional and international collaboration is essential along with support for countries with limited resources.

- States should take practical steps to implement the UN framework of Responsible State Behaviour, which should become an actionable framework. Coordination and translation with all relevant stakeholders should happen at national, regional and global levels. Support for capacity building (including simulation exercises, strengthening CERT-to-CERT cooperation), sharing best practices, and discussion about how to improve the protection of critical infrastructure are an essential part of the implementation.

- A more resilient, diverse, and sovereign cloud infrastructure may reduce dependency on few dominant global providers. It could support local innovation, ensure regulatory clarity, and enhance trust. It would empower countries and communities to shape digital infrastructure on their own terms.

- Promoting responsible practices in Internet infrastructure requires the establishment of a trusted, multi-stakeholder process to foster collaboration on challenges such as harmful activity and censorship. This process should prioritize open communication over rigid standard setting, and emphasize transparency over restricted access. It must support mutual accountability and interoperability to build trust and enable effective cooperation.

- Comprehensive policy and legal analysis is needed to identify and clarify regulatory ambiguities, examine conflicts between legal frameworks, assess commercial influence and address jurisdictional inconsistencies that obstruct responsible Internet governance. A coordinated advocacy strategy should be developed to promote harmonized, transparent, and enforceable guidelines across relevant jurisdictions.

- Trust in the Internet's infrastructure, including in its domain name system (DNS), is essential. Collisions with blockchain identifiers must be avoided. Multistakeholder discussions on the responsible integration of blockchain identifiers are an opportunity for the Internet community to keep advancing the collective goal of building a safe, reliable and trusted Internet.

- Discussions on autonomous weapons systems (AWS) and their technological, legal, ethical, security, and developmental impacts should be inclusive and transparent, and not confined to closed, specialised forums. There is an urgent need for international cooperation, as underscored by the UN Secretary-General and the ICRC, who have called for the negotiation of a legally binding instrument on AWS by 2026. Holistic solutions demand the active engagement of governments, civil society, academia, the technical community, and industry. The Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS), Austrian-led UN General Assembly resolutions, the Dutch and Korean Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM) initiative, and multistakeholder platforms such as the IGF play a vital role in advancing collective action and raising public awareness.

Online safety / information integrity / child safety

- The Global Digital Compact's vision of an inclusive, open, safe and secure digital space is not just an aspiration, but a practical framework that should guide our daily work. Whether we are coordinating election integrity efforts, developing child protection guidelines, or building multi-stakeholder partnerships, we're actively contributing to this global vision.

- Initiatives that engage governments, scientists, media, advertisers, influencers, and other relevant professionals provide more effective and sustainable responses to information integrity threats. Rather than focusing on isolated actors, they should address the entire information ecosystem, redirecting it toward reliable, science-based content that supports public awareness and informed policymaking. In this context it is important to enable evidence-based regulatory measures, facilitating access to algorithms and content flows on large platforms for research purposes.

- Trust transcends technology. It is fundamentally human and social. Effective cybersecurity depends on embedding transparency, inclusive community engagement, and civic digital

literacy to foster public confidence and counteract practices like privacy-washing. This requires implementing security-by-design mandates through appropriate policy tools, launching human-centred trust building and digital literacy initiatives, and establishing regional and international interoperability frameworks.

- Effectively combating online abuse, including fraud and DNS abuse, requires coordination, cross-sector collaboration, and data-driven action. No single actor or sector can address these challenges alone. The Internet community should engage with other industries, such as the payments sector, hosting and cloud providers for targeted responses. Building an ecosystem that enables robust information sharing, through initiatives like the Global Signal Exchange and Net Beacon, is essential. This effort must be both cross-sector and multistakeholder.

- The encryption debate often becomes entrenched and adversarial, with polarised positions hindering meaningful progress. To move forward, stakeholders should focus on specific areas where compromise is both possible and urgently needed, rather than allowing ideological stand-offs that stall action. The IGF community should play a key role in facilitating focused discussions to explore and pilot technical and policy solutions that uphold both strong encryption and lawful access, particularly in contexts like child protection.

- Countries across regions and contexts are grappling with the challenge of delivering safe and empowering digital environments for children. Building a child rights-respecting and inclusive digital future goes beyond traditional tech companies and online platforms. Other industry players from brands to investors have a pivotal role to play, including using their leverage on other actors of the ecosystem.

- Platforms should adopt a child rights-based approach that upholds the dignity, privacy, and best interests of children. The absence of strong, standardised, and globally applied mechanisms to protect children in the digital environment remains a critical gap. A child-centred and transparent approach is essential to building a safe online space. Protecting children online must go beyond transparency reports and statistics, and demands sustained, meaningful commitment. Accessible, child-friendly reporting mechanisms are vital to empower children to speak up. They must know how and where to report harm, and feel safe, supported, and confident when they do.

- Problems with deepfakes and sexual deepfakes are escalating globally, driven by gender-based violence and the rapidly evolving dynamics of online platforms. Legal, educational, and technical systems are struggling to keep pace. Addressing this issue requires coordinated, multi-stakeholder collaboration, yet current efforts remain fragmented and insufficient. To strengthen prevention and accountability, targeted investment is needed in localized detection datasets and immutable image technologies. At the same time, comprehensive digital literacy programmes are needed to educate both young people and decision makers about the risks, harms, and responsibilities associated with the use and misuse of such technologies.

- Cybercrimes causing personal harm or emotional impact are just as critical to address as those driven by financial motives. Gender-sensitive responses should be embedded in efforts to combat cybercrime and online harms, which disproportionately affect women and girls. Robust legal frameworks and legislative instruments are essential, but they must be paired with comprehensive training for the entire criminal justice system, from law enforcement to prosecutors and judges, on how to support victims effectively.

[Building] Sustainable and Responsible Innovation

The theme

GDC 1, 2, 4, 5 - WSIS C1, C6, C7, C10, C11 - SDG 7, 8, 9, 13, 14, 15, 16, 17; Environmental Sustainability and Climate Change, Economic Issues and Development, Emerging Technologies and Innovation, Artificial intelligence, Technical and Operational Topics

Advances in artificial intelligence, quantum computing, blockchain, the Internet of Things, and other areas have the potential to improve efficiency, decentralization, and accessibility, driving economic growth, digital inclusion and societal development. However, their development and adoption entail risks including negative environmental outcomes and widespread socio-economic impacts. Ethical oversight and inclusive governance are increasingly important as the role of these technologies grows within society. A balance needs to be achieved between innovation, responsibility, and sustainability in digital platforms and emerging technologies.

IGF Lillestrøm messages

Digital Public Goods

- Digital Public Goods (DPGs) are essential for creating an inclusive society where everybody can participate and meet their aspirations. DPGs are essential for attaining the Sustainable Development Goals.

- No single country can lead technological transformation alone. We need to use our resources more effectively, cooperate and share technology through global partnerships, knowledge sharing, and collaborative development.

AI, Work and Skills

- AI is entering every sector. The AI revolution extends beyond job displacement and fundamentally alters how value is created and who reaps the benefits. Those who know how to work with AI will be in high demand, while those without access to training or tools risk being left behind.

- We can set the course for the future of work through our policies and choices; technology itself does not determine it. We need to ensure workers are empowered, not marginalized to avoid widening the digital divide. It is vital to invest in digital literacy especially for women, young people and those who work in the informal economy, and to promote transparency, accountability and fairness in the workplace.

- Investment in citizens' digital skills is needed for competitiveness but also for people to have the chance to benefit from digital technologies and services. Education systems should help people to know when to question AI systems, and empower people to use their own data.

- National strategies should prioritize inclusive education and AI literacy to empower societies for climate-conscious digital futures and integrate environmental literacy and green AI principles into AI curricula.

Misinformation, Content moderation & AI and Media/Journalism

- Large language models (LLM) have emerged as a new tool for content moderation, but they pose risks of reinforcing systemic discrimination, censorship, and surveillance. Most platforms fine-tune a small number of foundational models rather than developing their own, which leads to concentration of power in content moderation as decisions made at LLM training stage cascade down across platforms.

- AI content moderation lacks sufficient transparency around implementation and risk mitigation, as the AI hype often overshadows documented human rights harms. We need to invest in tools for AI content transparency and foster multi-stakeholder product co-design where policy experts, users, civil society, and underrepresented groups are included in early product ideation and testing. The emergence of artificial intelligence fundamentally alters the fight against disinformation, with AI-generated responses, that often are detached from original sources and makes impossible to identify the reliable ones.

- More cross-sectoral engagement and coalition building between media actors (including digital rights and media for development organisations) is needed to understand the impact of AI and to mainstream responsible and ethical AI use in media. Voices of independent and public interest media from the Global South need to be actively engaged.

- Declarations on ethical AI are important, but we also need to monitor their translation into practice and assess their impact to ensure ethical AI use in everyday media work.

Infrastructure

- Building next-generation infrastructure is imperative for digital inclusion globally. Data agency is central to a fair and inclusive digital future, and this should be reflected in international funding mechanisms, capacity building, and standards development should reflect that. Empowering users in the Global South through data agency supports local innovation, enables competitive participation in digital markets, and reduces dependency on centralized platforms.

- Bridging technical innovation and public policy is essential. Builders, investors, policymakers, and civil society actors must collaborate more closely to ensure next-generation infrastructure reflects both market realities and public values. Multilateral and national digital development strategies should prioritize infrastructure that empowers users by design.

- Public interest, equality, interoperability and inclusion are crucial to digital public infrastructure (DPI). Ensuring DPI is developed and used in an inclusive and secure manner is an essential foundation for global digital cooperation. There is a critical need for government capacity building, open-source policies where feasible, and comprehensive digital governance frameworks for building trust and ensuring safe DPI adoption.

- Digital public infrastructure (DPI) comes with natural monopoly characteristics that, particularly in foundational identity, payments, and health platforms, create the risk that public-private partnerships may grant excessive operational control to incumbent firms, enabling them to monetise public data with minimal societal return.

- We need to design contractual arrangements that maintain Digital public infrastructure (DPI) as shared public infrastructure while enabling innovation through private sector partnerships. We should establish regulatory sandboxes for participatory data governance approaches, invest in capacity-building of public sector officials, data protection authorities, civil society organizations, and community leaders to ensure policy decisions are informed by local knowledge with the aim of preventing market concentration and ensuring competitive data use.

Connectivity

- Around 2.6 billion people around the world remain unconnected to the Internet. Accelerating international collaboration is essential to bridge the digital divides. Accessibility and connectivity to the Internet are a right. Stakeholders must collaborate on inclusive policies and connectivity models that support openness and affordability.

- We need to empower internet users in rural areas by equipping them with the digital skills needed for a sustainable future of community networks.

Environment and health

- Scalable, energy-efficient models are already operational and enable low-cost, low-power AI deployment in climate-vulnerable and low-resource settings. Open-source AI can significantly reduce duplication, costs, and energy use while fostering global collaboration.

- Embedding transparency across the AI lifecycle to ensure energy and resource use is measured, disclosed, and minimized, is a key component of equitable AI governance. Governments and industry should prioritize and incentivize energy-efficient AI innovation and require developers and deployers to measure and report energy, emissions, and water impacts of AI systems through sustainability standards, audit frameworks, and lifecycle disclosure requirements.

- The quality and granularity of digital data remain critical for credible modelling of environmental and health risks. To tackle concerns about accessibility, standardisation, and interoperability, we need to invest in digital literacy and capacity-building for public health, especially in the Global South.

- Digital solutions should be grounded in value-driven design and governed through inclusive frameworks. We need to shift from engagement-driven to purpose-driven digital ecosystems, particularly for underserved communities.

AI equity gap, AI ethics & small AI players

- The global AI equity gap is widening, putting the Global South at increasing risk of exclusion. Locally driven, inclusive, and human-centred AI approaches are critical to delivering meaningful impact. There is a need to build local capacities by intentionally investing in training, infrastructure, and linguistic inclusion.

- Policymakers should design AI regulation that both protects public values and enables innovation. Ethical considerations cannot be added as an afterthought to emerging technologies. Ethics must be a core competency for all stakeholders, and developers should balance technical success with ethical and sustainability perspective at every stage.

- Smaller states and start-ups can remain competitive in AI by leveraging open-source tools, domain expertise and strategic partnerships, especially in areas where agility, deep domain expertise, and contextual trust matter more than scale. They should not wait to be invited but position themselves as co-creators of the digital future.

- Large technology companies should commit to genuine collaboration with small actors by investing in open ecosystems, supporting lightweight AI development, and co-developing tools that reflect diverse contexts and constraints.

[Building] Universal Access and Digital Rights

The theme

GDC 1, 2, 3, 4 - WSIS C2, C3, C4, C7, C8, C10 - SDG 1, 2, 3, 4, 5, 8, 10, 11, 16; Rights and Freedoms, Universal Access and Meaningful Connectivity, Economic Issues and Development

Gaps and inequality in meaningful digital access pose profound challenges for communities across the world. Such digital divides cannot be addressed without recognising the essential link between universal access and human rights: an inclusive, open, sustainable, fair, safe, and secure digital future can only be realised when human rights are respected both offline and online.

IGF Lillestrøm messages

Human Rights and Digital Harms

- There is a need for stronger digital rights protections and accountability for digital harm, including all forms of state and non-state digital surveillance and data privacy violations. Accountability requires multistakeholder action and stronger domestic laws to curb spyware misuse and protect civil society.

- Stakeholders should advocate for political commitment to enforce a progressive interpretation of international law that protects individuals and communities from human rights abuses in the digital space. Legal scholars and practitioners should pool their expertise to reconcile human rights and international law principles to ensure that both are upheld in digital and cyber activities.

- Transparency and reform of national surveillance laws is required, including judicial oversight, public reporting and bans on unchecked state intrusion. There is a need for support for victims and civil society through legal aid, device forensic testing, and cross-border solidarity to challenge spyware abuses and secure reparations. Digital rights provisions should be equal for all.

- Successful digital policies include diverse voices in their formulation. Technology companies, governments and regulators should invest in adequate safeguards and accountability mechanisms that consider the growing digital inequality in Global Majority communities. Global South voices need to be amplified in global frameworks to ensure policies address regional realities, not just Northern priorities.

- Violations of human rights may occur through actions or through failing to act and prevent wrongful acts. Both states and companies have responsibilities, but boundaries between state and corporate accountability are currently blurred. Efforts to address this issue are underway but require further development.

- The UN Guiding Principles clearly define human rights due diligence responsibilities, but corporate accountability should become platform accountability by building an application method that reflects what human rights due diligence means in the digital context.

- Digital threats impact everyone. However, some groups are far more vulnerable as real-life patterns of inequality and oppression are reproduced and deepened in digital spaces. Women and

girls are amongst the most affected, with higher records of online intimidation or threats of violence, in particular after engaging in activism or human rights advocacy.

- It is important to centre the perspectives of people and communities most at risk of digital harm and exclusion in digital governance processes to ensure these remain rights-based, multistakeholder, transparent and democratic. Digital technologies should serve human rights and social good, not prioritise profit for a few over the wellbeing of all.

Ethical AI

- The implementation of AI ethical guidelines is paramount. Multifaceted domains should be taken into account in their formulation, including privacy and confidentiality; informed consent; bias and fairness; integration of human oversight; continuous improvement; coding with ethical guardrails; and support for community driven/local solutions.

- Without ethical guidelines, the development, implementation and deployment of AI models can result in technology that spreads misinformation and harmful stereotypes, lacks real-time fact-checking, violates ethical and privacy concerns, performs with a limited understanding of complex human emotions, and perpetuates bias and discrimination.

- There is a need to integrate mental health and suicide awareness into policy conversations, guidelines and standards for the development of the Internet and AI. Stakeholders should cooperate to facilitate community-centred frameworks that prioritize user control over personal mental health data and information.

Meaningful Access

- Digital connectivity is not just about access to the Internet; it is foundational for inclusion. Gaps are caused by a mix of infrastructural, economic, policy and socio-cultural barriers. Deep digital disparities exist in the developing regions, with new technologies often exacerbating offline divides. While economies rush to respond to new and emerging technologies, persistent challenges with respect to connectivity and meaningful access remain.

- Digital inclusion requires a rights-based, whole-of-society approach, including flexible construction of digital systems tailored to national or regional needs. No single entity can bridge the digital divide alone: governments, private sector, NGOs, and communities must work together towards long-term impact, reachable with inclusive policymaking and public-private partnerships. Efforts made by multistakeholder partners to assist, incentivize, promote and measure meaningful access should be permanent.

- For the large group of unconnected people living in areas with mobile coverage, digital inequality is no longer primarily about infrastructure coverage. Instead, the main barriers are affordability (particularly device costs), digital literacy, and meaningful usage skills. Addressing these needs requires a holistic approach that includes infrastructure investment, affordability, digital literacy, and local engagement.

- We need to ensure that people have access to useful and meaningful services in their own languages. The Internet and the technology around can be powerful tools for the preservation and usage of endangered Indigenous languages. Open source codes can be downloaded by educators, researchers and industry experts aiming to promote and multiply the impact towards the

revitalization of these languages. Collaboration with the private sector and use of local languages will enhance the impact of digital literacy programmes.

- Stakeholders should design and support scalable solutions, such as community networks and public Wi-Fi initiatives, tailored to the unique needs of underserved regions. It is also necessary to subsidize digital devices and connectivity for marginalized groups, along with local capacity building in local languages. The IGF has developed tools through intersessional activities to encourage successful meaningful projects' replication, scaling and localisation.

- A diverse ecosystem of providers is essential for last-mile access. The traditional model of relying solely on large mobile operators is insufficient for reaching marginalised communities. This includes community networks, local libraries, post offices, and other intermediaries that can provide culturally relevant, affordable solutions. Regulatory frameworks need to encourage this diversity rather than creating barriers that favour only large conventional operators.

Digital Public Infrastructure

- All regions seek digital public infrastructure (DPI) that is inclusive, resilient, and people-centred. A commons-based approach to DPI governance can unite these efforts without homogenizing them, respecting local ownership and enabling global alignment. Moreover, governance can be "built into the code." DPI systems must be structured to reflect principles such as accountability, privacy and equity from the outset.

- Policies should aim to promote equitable and safe access to digital technologies. They should ensure that the rights and needs of traditionally marginalised and oppressed groups are prioritised. To support the development and deployment of inclusive digital solutions, it is essential to engage diverse financing modalities and shape the actions of funders and financers.

[Building] Digital Cooperation

The theme

GDC 3, 4, 5 - WSIS C1, C2, C3, C4, C6, C10, C11 - SDG 9, 10, 11, 16; Digital Cooperation, Emerging technologies and Innovation, Artificial intelligence, Sustainable Multistakeholder Governance

2025 is a pivotal year in the ongoing, multistakeholder effort to refine and evolve the governance and coordination of our digital world. The Internet Governance Forum (IGF) serves as a key platform in this effort, interfacing with a wide range of stakeholders and processes, including the WSIS+20 review, the recently agreed Global Digital Compact and ongoing global dialogues on AI governance, to address a large and growing array of challenges.

IGF Lillestrøm messages

- There is a growing risk of digital inequality, particularly in developing countries, as emerging technologies such as AI advance rapidly. High deployment costs and limited digital skills prevent many communities, especially in the Global South, from fully benefiting from digital progress.
- It is essential to increase the participation of the Global South and civil society in global digital dialogues. It is important to strengthen articulation around common objectives but also understanding of local needs and realities.
- The Internet is not ownerless, and the growing concentration of power and increasing dependence on big tech raises serious concerns about the resilience of societies in maintaining healthy information spaces, freedom of expression, and access to information. To ensure that information technologies serve democratic and ethical values, and to support the sustainability of open information societies, a shift away from deregulation, non-intervention, and corporate consolidation may be necessary, towards responsible, collective governance and regulation, with transparency and accountability at the forefront.
- Sustainable business models to ensure broad access need to be explored. International legal or institutional mechanisms should be strengthened or established to prevent private satellite broadband providers from exercising disproportionate or unregulated influence over Internet access and connectivity in foreign jurisdictions.
- It is important to strengthen multilateral and multi-stakeholder cooperation to help ensure that the benefits of digital transformation are shared broadly and no one is left behind.
- Technical standards can have significant real-world human rights implications, affecting access to critical services and increasing the risk of surveillance or exclusion. Therefore, inclusivity in technical standard-setting is essential. This calls for support mechanisms and capacity-building efforts to enable meaningful participation from diverse communities, including civil society and non-engineers, and for the integration of international human

rights frameworks at all stages of standards development to ensure ethical and inclusive outcomes.

- The IGF should be used as a confidence- and capacity-building space for further discussions on Internet fragmentation, especially given the current lack of coordination among various stakeholder groups in addressing fragmentation questions. Inclusive input from all stakeholder groups is essential as the global digital environment faces increasing territorialisation, the growing use of sovereignty-based approaches, and the normalisation of network control.

- The development of inclusive and innovative digital governance models that address the structural barriers contributing to digital inequality should be promoted. It is important to prioritize investment in digital capacity building, especially in underserved and developing regions, to ensure equitable access to emerging technologies.

IGF, Global Digital Compact and WSIS

- The international community should avoid overlap or fragmentation of mandates within the UN system. It is important to make use of existing platforms and spaces, such as the IGF, and improve collaboration capacities, and put further effort into including diverse actors to strengthen multi sectoral dialogue.

- Within the IGF, efforts should further strengthen the inclusion of the underserved communities and stakeholders from all generations, amongst others, by reinforcing connections between and with the National and Regional IGF Initiatives.

- To further digital cooperation, it is necessary to strengthen commitments and existing mechanisms with special attention to the Global South, and marginalized populations.

- WSIS should reform its multistakeholder framework to address contemporary challenges of digital sovereignty, platform consolidation, and emerging technologies. This requires strengthening institutional accountability mechanisms, expanding Global South participation, increasing regional coordination and empowering the IGF.

- There is a shared understanding that the WSIS Action Lines were elaborated in a broad and technology-neutral way, so that they can be adapted and applied to the constant technological innovations. The main gap within the WSIS Framework and between its different parts (such as the IGF and the WSIS Forum) is the lack of coordination, both regarding the procedural aspects or the subjects that are discussed in each of these fora.

- Some aspects that need to be worked on to strengthen the IGF include (i) the need for coordination with other digital governance spaces; (ii) rethinking procedural aspects, including the MAG operation (in order to create solid and permanent institutional knowledge, for instance); (iii) obtaining a more robust funding; (iv) establishing a longer or permanent mandate, to allow for continuous improvements; (v) improving the mechanisms for sharing IGF outcomes, so that more people and audiences are reached, including decision-makers; (vi) increasing coordination between global governance and local and regional governance, such as greater interaction with the NRIs.

- Integration and coordination mechanisms should be established between the WSIS Forum and the IGF, which would help to achieve greater alignment between the WSIS Action Lines and SDGs.

- Multistakeholder platforms like the IGF should be preserved and strengthened. All stakeholders, including governments, businesses, technical community and civil society, should actively support the IGF as a global public good - both politically and operationally.

- The IGF serves as a valuable global platform for cross-border, cross-sector collaboration. It helps to empower both small and large nations to influence the shape of the digital future across generations, industries, and interests.

- The upcoming WSIS+20 review offers a crucial opportunity to reassess global governance structures and better integrate legal and technical approaches. It invites reflection on how far multistakeholder processes have come and where alignment with international law could be strengthened.

- The "broad" definition of Internet governance formulated by the WGIG and adopted at Tunis still holds up despite the technological changes and new issues that have arisen in the past twenty years. The WGIG demonstrated the value and viability of real multistakeholder decision-making in the UN context. Its model could be used to address other issue areas on which governments are uncertain or deadlocked and a new approach is needed e.g. data and AI governance.

- The WSIS Review should facilitate real multistakeholder engagement (including between stakeholders and governments) and establish stronger multistakeholder arrangements for future follow-up and implementation efforts.

- The IGF needs to be preserved as a venue for effective conversations on the governance of the technical layer of the Internet while also creating the space for multi-stakeholder engagement on emerging digital governance challenges.

Global AI cooperation

- Multistakeholder and cross-sector collaboration is vital to ensure AI contributes to the Sustainable Development Goals (SDGs). AI must be governed with human rights at the core. AI systems should support sustainable development, promote gender equality, and reflect cultural diversity.

- Inclusive, multistakeholder approaches to AI governance should involve civil society, independent experts, and underrepresented communities to ensure governance models are not dominated by authoritarian or purely commercial interests.

- Local AI ecosystems will be instrumental in empowering diverse communities to shape the future of technology. Global efforts must prioritize the development of local language AI and culturally relevant datasets to empower underrepresented communities in shaping international AI governance frameworks.

- Multi-stakeholder partnerships should be strengthened to enhance digital skills and develop trustworthy AI systems, thereby fostering inclusive adoption across diverse global contexts.