Riyadh IGF Messages

Riyadh IGF Messages

The **19th annual meeting of the Internet Governance Forum** was hosted by the Kingdom of Saudi Arabia in Riyadh from 15 to 19 December 2024.

The **Riyadh IGF Messages** provide a high-level overview for decision-makers of the most current thinking on key Internet governance and digital policy issues. They are sourced directly from over 300 sessions held during IGF 2024. Session organisers 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 and Regional IGF initiatives.

A set of draft messages, curated by the IGF Secretariat, was published on 19 December for community review. These final IGF 2024 Messages are part of the annual meeting's outcomes.

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

- **Harnessing innovation and balancing risks in the digital space.**
- **Enhancing the digital contribution to peace, development, and sustainability.**
- **Advancing human rights and inclusion in the digital age**
- **Improving digital governance for the Internet We Want**

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

Riyadh IGF Messages

Riyadh IGF Messages 1

Table of content 2

Overarching Issues 3

Harnessing innovation and balancing risks in the digital space 4

The theme 4

IGF Riyadh messages 4

Enhancing the digital contribution to peace, development, and sustainability 7

The theme 7

IGF Riyadh messages 7

Advancing human rights and inclusion in the digital age 10

The theme 10

IGF Riyadh messages 10

Improving digital governance for the Internet We Want 13

The theme 13

IGF Riyadh messages 13

Overarching Issues

The 19th IGF annual meeting was organised at an interesting point in time, a few months after the **UN Summit of the Future** and the adoption of the **Pact of the Future** and **Global Digital Compact** in September 2024, and before the twenty-year review of the World Summit on the Information Society (**WSIS+20 Review**), which is scheduled for the General Assembly in 2025 and will also review the IGF's mandate. Many sessions, across the different IGF tracks and the four main themes, referred to these processes or focused their discussion on issues included in the documents.

Riyadh IGF Messages and other IGF outcomes

The **Riyadh 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/igf-2024-reports.

The Riyadh IGF Messages are complementary to outputs and observations compiled by other tracks; they are listed at https://intgovforum.org/en/content/igf-2024-outputs.

Harnessing innovation and balancing risks in the digital space

The theme

The Internet and digital technologies are an intrinsic part of every country's development, spurring innovation in many areas such as healthcare, distance learning, and socio-economic growth. However, this centrality of the digital space also creates global vulnerabilities that call for collective action, as individual actions alone cannot effectively address them. This theme aims to foster dialogue and knowledge exchange on success stories and best practices in reaping the benefits of digital innovation for all, as well as efforts of all stakeholders to tackle the risks arising from this rapid transformation.

IGF Riyadh messages

Governing artificial intelligence

- Progress has been made in global AI governance, but significant work remains to ensure the responsible, fair, safe, accountable, inclusive and sustainable development and use of AI for all and build trust for its widespread adoption. AI and its applications must uphold human rights, democratic values and the rule of law, while being inclusive, transparent and explainable.

- There is a critical need for trusted, inclusive, and secure digital identity systems as foundational infrastructure for global digital transformation. Privacy and security must be balanced to foster user trust while leveraging emerging technologies such as blockchain, biometrics, and AI to enhance identity verification.

- Governance of AI is not a "nice to have." Minimizing the risks of AI is crucial, but it is equally important to focus on tools that balance AI innovation and regulation. Overregulation can hinder AI's potential to benefit humanity and the environment, yet, we should not compromise on ethical standards, tackling biases or ensuring privacy.

- Public participation at the national and local levels should be an integral part of AI governance, as replicating international approaches without adaptation is not a sustainable solution. Working together and combining open-source development with regulations helps to prevent AI monopolies that selectively limit access to and use of technologies.

- A comprehensive approach to the entire AI lifecycle—from development and deployment to usage and impact—is essential for ensuring accountability for AI-related harms and promoting responsible AI development. This involves examining the roles and responsibilities of all stakeholders, including developers, operators, users, governments, and civil society.

- Multistakeholder collaboration on AI needs to keep pace and adapt to the evolving technology landscape and support responsible innovation and governance. This includes recognising and documenting the new technologies' potential for inclusion

and contributing to achievement of the SDGs, as well as discussing principles of AI regulation, and tackling specific risks associated with AI.

- Generative AI systems are evolving rapidly, making it increasingly difficult to distinguish between human-created and AI-generated content. Ensuring their accountability and transparency is urgent. Today, children already grow up in a world where AI-shaped information influences their worldview.

- AI systems are transboundary, not patchwork, and their governance should reflect this reality. Achieving this requires a collective and comprehensive effort to prevent regulatory fragmentation, break down silos, build trust, cooperate on shared AI terminology and standards, the collection of statistics and development of indices and indicators. Effective AI governance must also align with the specific roles of actors across the AI supply chain to ensure it is actionable.

- AI fairness should be a key component of curricula to equip future technologists with the skills needed to develop ethical AI systems.

<u>Technology for inclusion and empowerment</u>

- Technology has the potential to drive inclusion, empowerment, and sustainable development, but significant challenges remain in ensuring equal and inclusive access. Greater efforts are needed to develop and adopt open-source technologies to make technology more accessible and affordable, especially for low-income populations. As the AI divide exacerbates the digital divide, promoting equitable access to AI tools for underserved communities is crucial.

- Active video gaming industries play a key role in promoting local human capital development, supporting start-ups and entrepreneurship, and driving new research and development. These efforts can be leveraged to boost economic growth, foster innovation, and enhance competitiveness in this dynamic and rapidly evolving industry.

- Connectivity has the power to transform lives and is essential for the adoption of emerging technologies. Achieving universal connectivity requires multistakeholder collaboration and investments in both infrastructure and skills. Governments and the private sector must work together to expand connectivity's reach.

- Local communities are best positioned to understand the context specific needs and challenges. By involving them in designing and implementing technology solutions, one ensures that solutions are appropriate, effective and tailored to local realities, languages, and needs. This effort should include marginalized groups to prevent exacerbating digital exclusion.

- Governments, private sector, the technical community and civil society must collaborate to provide affordable internet access, digital literacy programs, and encourage community-driven AI innovations. Governments need to prioritize funding

and policies that enhance digital infrastructure and promote equitable access to AI tools for underserved populations.

Enhancing the digital contribution to peace, development, and sustainability

The theme

Some of the biggest challenges facing the world are the need of improving sustainability and working together for peace, and at the same time working for social and economic development in our countries and regions. Harnessing the transformative potential of digital technologies and the Internet can be an important ally to achieve global progress that promotes peace, drives sustainable development and addresses pressing environmental challenges. This theme will explore the multifaceted ways in which digitalisation can drive socioeconomic change and development for present and future generations.

IGF Riyadh messages

Towards greener and sustainable Internet practices

- Collaboration, focusing on clean energy and green technologies, promoting energy-efficiency, using eco-friendly hardware, and encouraging recycling, is essential for a sustainable Internet. Providers, governments, manufacturers, and consumers must work together to manage the Internet's growing environmental impact. Governments must set clear sustainability benchmarks and incentivise renewable energy, while the private sector should invest in scalable, energy-efficient innovations that minimize environmental impact. Access to green and affordable energy is a critical element of digital transformation.

- Eco-friendly technologies and efforts to combat climate change must align with fostering inclusive progress. Local insights, regional studies, and academic contributions are essential for developing tailored, data-driven solutions, particularly in underserved areas. To ensure equitable access to sustainability, green and clean technologies and energy-efficient innovations must be both affordable and accessible.

- The amount of e-waste produced globally is alarming and poses significant environmental and health hazards when not managed properly. Despite its continued growth, only a small portion is currently being recycled. Collaboration is key: Effective and sustainable e-waste management systems require strong partnerships among policymakers, industries, civil society organizations, and end-users, with shared knowledge and coordinated action at the forefront. Designers, developers, and companies must prioritize ease of repair, recyclability, and the integration of refurbished devices in product development.

Making use of new technologies for peace, development, and sustainability

- AI and AI-powered solutions have the potential to play a significant role in achieving the Sustainable Development Goals. Leveraging AI tools will enhance efficiency, decision-making, and innovation across sectors including the public sector, media, and judiciary. To harness AI for good effectively, there is a need for capacity building. Inclusive adoption requires special attention to underserved regions and resource-

limited communities. While AI offers significant opportunities, it also presents challenges like bias, misuse, and AI-driven misinformation. Transparency, accessibility, and human oversight help mitigate risks and ensure that AI serves the public good.

- Innovation and control need to be balanced through transparent policies for the use of AI that address operational challenges, define acceptable practices, and ensure human oversight to build trust and accountability. The Integration of AI safety standards may face challenges due to the fragmentation of ecosystems, sector-specific complexities, cultural and regulatory diversities, yet clear and unified standards are essential to ensure AI safety and reliability.

- Artificial intelligence is transforming government operations and optimizing administrative services, improving accuracy, and enhancing accessibility. A balance between openness and security is crucial. Open-source models enable collaborative innovation, while data sovereignty ensures privacy, compliance, and public trust. By prioritizing both accessibility and control, governments can responsibly adopt AI solutions that align with their unique societal goals. Businesses can help governance in public-private partnerships, investing in open-source tools, and offering expertise in AI deployment.

- Common barriers to e-Government development in local government are low digital literacy, limited funding, and a lack of specialized human resources. To foster meaningful progress, local governments must be encouraged to iterate, pilot, and test creative solutions, an approach that demands agility, learning from outcomes, and embracing failure as part of the innovation process.

<u>Protecting critical infrastructure and essential services</u>

- International peace and security forums and institutions must prioritize open, secure access to telecommunications infrastructure and the protection of the public core. The UN Security Council should monitor telecommunications in the conflicts, while peace and justice institutions ensure accountability for disruptions affecting fundamental rights and security. Collaboration among all stakeholders is essential to safeguard critical telecommunications and internet infrastructure, even during crises. To advance the Global Digital Compact guidance discouraging internet shutdowns, multistakeholder working groups and enhanced IGF Best Practice Forums should define the community's roles in protecting the public core and ensuring access during conflicts and crises.

- The interconnected digital space offers immense opportunities for development but also brings heightened risks to critical infrastructure and essential services, necessitating harmonized global efforts and multistakeholder collaboration for effective risk mitigation. Shared definitions of critical infrastructure and essential services, along with enhanced international collaboration to establish a global baseline for their protection, are vital.

- Cybersecurity is a shared responsibility that requires stakeholder alignment, strengthened public-private partnerships and leveraging industry best practices for enhanced resilience and establishing baseline cybersecurity standards.

- Cybersecurity and national security are deeply interconnected, requiring governments and stakeholders each in their respective roles and responsibilities to collaborate on frameworks to address transnational cyber threats while ensuring transparency, accountability, and inclusivity. Promoting cyber literacy and skill development through widespread educational initiatives is vital to empowering communities, fostering resilience, and enhancing national security. Additionally, cyber policies shall seek to prioritize decentralized infrastructure, open-source innovation, and hardware security-by-design to reduce vulnerabilities and strengthen overall cyber resilience.

- The key to cyberspace resilience lies in balancing innovation, ethics, and regulation. Emerging technologies like AI and blockchain offer immense opportunities for enhancing cyber resilience. Policymakers need to ensure ethical governance as well as foster innovation. Legal and ethical standards must be equipped to address the challenges of emerging technologies, ensuring frameworks and legislation that uphold human rights.

- Cyber peace cannot be achieved in isolation; it is vital for governments, the private sector, civil society, and international bodies each in their respective roles and responsibilities to t work together to share knowledge and build capacity to combat state-sponsored attacks, cyber warfare, and emerging cybercrime.

- Consistency creates impact in cyber capacity-building initiatives. Efforts must be contextual, rooted in local needs, and shared globally to ensure relevance and scalability. Localization plays a pivotal role in enhancing accessibility and driving broader adoption. Building trust requires a committed approach that includes sharing knowledge, actively listening, implementing solutions, and being open to change.

- Cyber capacity building should leverage existing mechanisms such as the IGF, established processes, and proven practices. Participatory multi-stakeholder engagement is recommended to be designed intentionally to optimize mapping, coordination, collaboration, and communication, even in low-resource environments. Education must focus on making cyber security accessible and demystifying its complexities, fostering resilience in future generations. Cyber security capacity-building should be approached as a culture and practice, prioritizing localization, contextual relevance, and adequate resourcing to ensure accessibility and long-term sustainability.

- Comprehensive capacity building should allow law enforcement and security agencies to use AI and new technologies to detect crimes and terrorist activities, as well as use them for counter-terrorism purposes. Parliamentarians have the important role of ensuring compliance with human rights standards. Additionally, literacy programs on AI and new technologies must empower both younger and older generations to navigate digital space, critically analyze information, and counter extremist propaganda.

Advancing human rights and inclusion in the digital age

The theme

The digital environment is an increasingly important facet of daily life all around the world. Therefore, discussions about how to empower all people and drive genuine inclusion of all communities in shaping its development is vital. This includes efforts to connect and empower all populations, in particular marginalised communities and vulnerable groups to reap the benefits that the Internet has to offer, and ensure that the same rights they enjoy offline also apply online. This theme will delve into the innovative solutions, frameworks and initiatives that foster universal meaningful connectivity and ensure the protection of human rights in the digital realm.

IGF Riyadh messages

<u>Meaningful Connectivity and Digital Inclusion</u>

- Multistakeholder collaboration is key in tackling the pressing challenges of the digital age, such as the digital divide, cybersecurity, AI ethics, and privacy. Addressing these issues requires resilient and inclusive digital infrastructure, equitable access to technology, and governance frameworks that uphold human rights, transparency, and accountability. Initiatives like the Global Digital Compact and the WSIS+20 review present significant opportunities to advance these collective goals, emphasizing a shared commitment to ensuring that technology serves humanity and empowers everyone.

- Governments, tech companies, civil society, parents, and educators share a collective responsibility to safeguard children's rights in the digital world. While technology holds transformative potential to empower children, proactive measures are essential to protect them from risks such as cyberbullying, misinformation, and exploitation.

- Meaningful and universal connectivity is essential for advancing human rights and digital inclusion, allowing full participation in the digital economy, while also enabling other socio-economic rights. It can only be achieved with affordable access to services and devices, obtainable digital literacy and skills, and equal occupancy of the online space by both men and women, boys and girls, young and old, urban and rural, local and global communities.

- Long-term initiatives such as national broadband plans and digital gender inclusion strategies are needed to achieve systemic change. Significant investments, particularly through Universal Service Funds (USF), drive digital inclusion. A close collaboration between governments, private sector, and CSOs ensures transparency, effectiveness, and accountability in USF implementations. Governments should ensure regular proactive disclosures of USF project expenditures and evaluations for public monitoring.

- Smaller, targeted and localized interventions on meaningful connectivity can yield immediate benefits and build momentum for larger changes. Policymakers should engage with local communities to understand their unique needs and tailor access strategies accordingly. The multistakeholder community should set measurable targets to close the digital divide with those that are marginalized (e.g., women and girls, persons with disabilities, rural and indigenous communities, displaced groups etc). A "whole of a society" approach is fundamental.

Case Studies and Frameworks

- Meaningful access is rapidly expanding across all regions. The Global Digital Compact recognises that providing content in local languages and offering services that really improve citizens' quality of life is a successful approach to promote access.

- Sharing examples, for example at the IGF, of digital inclusion initiatives and frameworks aimed at ensuring that no one is left behind can spark stakeholder engagement and cross-border collaboration. The good practices and cases presented and collected amongst others via the PNMA Repository must be proactively promoted throughout different regions and institutions, in order to amplify their impact across places and communities.

Human Rights Online

- The legal system must take care of the needs of all individuals, including marginalized groups and persons with disabilities. Legal frameworks should be creative and adaptable to ensure participation and protection for everyone in the digital age. Judges play a decisive role in shaping and interpreting digital rights, such as privacy, freedom of expression, and access to information. Equipping judges with the right tools and knowledge is essential to ensure justice keeps pace with technological advancements. Hence, initiatives that encourage cross-country collaboration among legal professionals should be implemented. The judicial officer should participate in the multistakeholder process.

- The enforcement of digital rights across borders requires harmonized legal frameworks and principles. Clear standards for handling digital evidence and cooperation mechanisms are needed to address issues like cross-border data flows and cybercrimes. Likewise, embracing AI in the judicial system requires proper training of court members and legal professionals to understand the tools, potential, and limitations. A significant reduction of algorithmic bias is achievable through training with robust, diverse, and jurisdiction-specific data and doctrinal materials. As a consequence, the conception of regulatory frameworks to ensure AI systems in the judiciary can be transparent, secure, and aligned with jurisdiction-specific legal and ethical standards.

- Moreover, dialogues with governments and regulatory bodies should be encouraged, to ensure they prioritize digital rights and understand the implications of evolving technologies. Additionally, collaboration between legal experts, civil society, businesses, technologists, academia, and policymakers can create well-rounded and

effective digital rights strategies. Establishing dedicated IGF tracks for judiciary and business discussions are recommended to foster dialogue and solutions.

- Stakeholders should document the benefits of rights-respecting laws and the harms of authoritarian ones, and encourage governments to adopt approaches which ensure that cybercrime laws or content restrictions are grounded in transparency, proportionality, and protection of human rights.

- Technical standards are critical tools for embedding human rights principles into emerging technologies, ensuring interoperability, security, and inclusivity. Involving human rights experts in standardization processes and translating human rights principles into practical, technical guidelines can empower technical communities to implement rights-based standards and so bridge the gap between technical innovation and human rights safeguards.

Digital Infrastructure and e-government

- Trustworthiness and security are the key precursors to a functioning e-government architecture. Before attempting to implement e-government initiatives from a technical standpoint, legislators and decision makers need to map the needs of their communities and be on the ground to uncover nuances and current access limitations of their citizens.

- To address the needs of historically marginalized groups, including those with disabilities, e-government services should be proactive and provide an interface that seeks to accommodate those of all abilities. In designing e-government systems, one must ensure that channels for accountability and feedback are built-in by design, enabling citizens to be active stakeholders and keep agency on how their data is being used. The implementation of a standard digital identity for every resident should be prioritized as the foundation for e-government.

- The cost of Internet access remains one of the main barriers to inclusion of the unconnected. The affordability of devices and services is a key challenge to tackle. Persistent gender digital divides and gaps in gender data remain major obstacles. Without deliberate action, the transition to data-driven economies risks reinforcing, rather than addressing, gender inequalities.

- Developing reliable measurement tools to evaluate access and digital inclusion policies is essential. These tools will help determine the effectiveness of existing solutions and identify areas where challenges persist.

Improving digital governance for the Internet We Want

The theme

The very nature of the global Internet requires effective models of multistakeholder governance to be at its core, garnering continued efforts by all stakeholders to address digital issues and the promotion of greater cooperation. This theme is about identifying ways to strengthen and support the open, transparent, inclusive and bottom-up governance process related to the use and evolution of the Internet, working towards the vision of achieving the Internet We Want.

IGF Riyadh messages

Global Digital Governance and Coordination

- The Global Digital Compact (GDC) must transition from a vision document to an actionable framework, strengthening and aligning with existing structures like the WSIS process, the IGF and, the STI Forum. Enhanced coordination among these platforms is essential to avoid fragmentation, foster synergies, and ensure cohesive, inclusive policy making.
- Avoiding Internet fragmentation remains a key concern, demanding a balanced, inclusive, and forward-looking approach. The GDC commitment (Article 29(c)) presents a vital opportunity for the multistakeholder community to sustain inclusive dialogue, report on follow-up actions, and establish a mechanism to monitor and evaluate progress effectively. The NRIs and the IGF2025 are key venues to address these opportunities.
- The IGF remains a pivotal agenda-setting platform, where critical issues like AI, cybersecurity, and digital inclusion are addressed, often before they gain traction in intergovernmental processes. Its agenda-setting power must deliver actionable outcomes to close gaps in connectivity, skills, and infrastructure, especially in developing countries and promote human-centric, rights-based digital governance.
- The WSIS+20 review presents an opportunity for the IGF to align with global priorities such as the 2030 Agenda for Sustainable Development. Strengthened engagement with national governments and policymakers will foster governance models that link global objectives to regional and national realities and shape a digital future that is equitable, resilient, and secure for everyone.
- Academic researchers contribute significantly to refining multistakeholder approaches. By advancing governance models through IGF discussions, they help ensure adaptability to diverse policy contexts and support the evolving digital landscape.

Inclusivity and Bridging Digital Divides

- Bridging the global digital divide requires urgent action to address gaps in connectivity, skills, and infrastructure, particularly in developing countries. Meaningful Internet access must prioritize underserved and marginalized communities with investments

in capacity-building and empowerment to support digital literacy and economic inclusion.

- Addressing the gender digital divide is critical to equitable participation in the digital economy. Efforts to tackle emerging divides such as the AI skills divide and compute capacity divide, must involve global collaboration to ensure equitable access to resources and opportunities.

- Recognizing youth as stakeholders in digital governance frameworks ensures that policies reflect diverse perspectives and the needs of future generations. Lessons from the GDC consultation process underline the importance of improving inclusivity in such initiatives. Ensuring balanced participation from diverse regions and stakeholder groups will make these processes more democratic and representative.

Cybersecurity and Resilience

- Transnational critical infrastructure (CI) faces growing cyber threats, including malicious ICT activities targeting essential systems like subsea cables and cloud infrastructure. Protecting CI requires stronger CERT-to-CERT cooperation, effective communication during ICT crises, and inclusive multi-stakeholder engagement.

- Governance frameworks need to balance innovation with human rights, embedding ethical and transparent guidelines into adaptable policies to support sustainable development without deepening inequalities. Using cybersecurity regulations for protectionism hinders global development and cooperation.

- Oversight and accountability mechanisms are critical for clarifying responsibilities in the development and deployment of digital technologies. These frameworks will ensure the Internet remains a platform for empowerment and equitable development.

Collaboration and Ethical Data Governance

- Cross-sector collaboration is key to address online harms. Regulators, industry, and technical communities must develop harmonized regulations informed by technical expertise. Enhanced data-sharing and capacity building initiatives are necessary to empower stakeholders, strengthen global responses, and increase transparency across the Internet ecosystem.

- Interoperable frameworks that balance national interests with the benefits of cross-border data flows are crucial for effective data governance. Multistakeholder approaches, promoted by the IGF can restore trust, reduce silos, and enhance policy interoperability to drive inclusive growth.

- Dynamic Coalitions (DCs) within the IGF contribute to inclusive and accountable digital development through thematic expertise and collaboration, they address challenges like digital divides, promote accessibility for persons with disabilities, foster ethical AI governance and promote sustainable data practices.

-