IGF MESSAGES

This document is a summary of points raised during the 18th annual Internet Governance Forum meeting hosted in Kyoto, Japan from 8 to 12 October 2023.

Discussions at the Forum focused on the overarching theme of *The Internet We Want – Empowering All People*. Sessions were organised within eight subsidiary themes which were concerned with:

- Artificial Intelligence and Emerging Technologies
- Avoiding Internet Fragmentation
- Cybersecurity, Cybercrime and Online Safety
- Data Governance and Trust
- Digital Divides and Inclusion
- Global Digital Governance and Cooperation
- Human Rights and Freedoms
- Sustainability and Environment

The draft IGF Messages in this document emerged from the many sessions held within these themes.

OVERARCHING ISSUES

Many sessions during the Forum discussed the contribution which the Internet and digital technologies can make to supporting the Sustainable Development Goals (SDGs).

Attention to the role which digital technologies can play in achieving the SDGs has intensified, particularly in those areas that are currently lagging behind delivery schedules following the COVID-19 pandemic. Emphasis was placed during the Forum on access and infrastructure, the governance of new technologies such as artificial intelligence, the need to develop digital skills, ethical behaviour in the production and use of digital technologies (including issues of e-waste, data protection and cross-border data storage), and the need to bridge the gender digital divide and promote increased participation of women in technology and leadership roles.

Many sessions discussed the issues that are proposed for inclusion in the Global Digital Compact that is being prepared ahead of the United Nations Summit of the Future scheduled for 2024, including the role of the IGF as a source of multistakeholder expertise for the Compact and its outcomes. The forthcoming twenty-year review of the World Summit on the Information Society, which is scheduled for the General Assembly in 2025 and will review the IGF's mandate, was also considered.

The IGF Leadership Panel presented a paper on *The Internet We Want* proposing broad principles for the future development of the Internet, on which it invited views from the IGF community.

ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGIES

Theme

Artificial intelligence (AI) is a powerful and transformative technology. It is difficult to think of a sector that is not already affected and may not be transformed by its rapid development and scope, including growth in productivity, and the consequences of rapid change arising from this in economy, society and culture.

Recent developments are remarkable and pose new challenges as well as opportunities. In the past year, the emergence of generative AI and its applications has entered people's everyday lives and discussions.

Many people are concerned about the implications of this for human society and the environment, in both the short and longer terms. Global multi-stakeholder dialogue and cooperation are needed to ensure that AI is developed and applied responsibly.

The applications and impact of AI transcend national boundaries. Most AI policy discussion, development and analysis, however, is currently focused in and on the Global North. Opportunities and impacts for the Global South need to be more thoroughly understood and prioritised.

Messages

Global cooperation

- We can only realise AI's potential to benefit everyone through collective global efforts that draw on the wide range of views of policymakers, technologists, investors, businesses, civil society and academia from all countries and regions. High-level global governance dialogues and curated expert groups need to be balanced with inclusive dialogues that are open to all.
- Collaboration between global AI policy and governance fora and initiatives is needed to prevent fragmentation of efforts and inconsistent policy approaches. Developing and sharing best practices will be important and must include perspectives from the Global South. Governments in the South need to increase attention to responsible and safe development of AI within their countries, developing policies and strategies based on building blocks that include connectivity, digital literacy and cybersecurity.
- Multistakeholder consideration of digital governance should not be confined to experts but should find ways to engage and build on the experience of all people. An inclusive approach would ensure that diverse perspectives contribute to shaping policies that affect the broader population.

Governance

- AI and other emerging technologies should be developed and used in ways that respect human rights, democratic values and the rule of law. AI systems should be inclusive and privacy-respecting by design. The processes to develop AI technologies themselves, as well as AI policy, governance frameworks and regulation should be transparent and inclusive.
- Considerable progress has been made in developing global AI principles, including in the context of the G7 Hiroshima AI process that was initiated by the Government of Japan. We now need to move from developing ethical guidelines and principles to operationalizing AI governance.

- Concerted effort should be put into translating AI principles into actionable measures and effective implementation. Our efforts to operationalise globally shared values should be flexible enough for measures to be readily adaptable to diverse local and cultural contexts.
- AI standards, guidelines, self-assessment mechanisms and codes of conduct are important, and regulation is also necessary for effective AI government. There is an urgent need to clarify the responsibilities and accountability of all parties in the AI development lifecycle and define the necessary safeguards.
- It is essential to strengthen mechanisms of oversight and to track the implementation and impact of AI policies and plans that have already been agreed.

Human rights and development

- The increasing deployment of AI in our societies can empower and connect people but could also further discrimination and deepen digital divides. AI innovation should respect human rights and the rule of law.
- If harnessed safely and responsibly, AI could help the world community to revitalize progress towards achieving the SDGs. We need to raise the level of ambition around this and employ new technologies to address the complex problems that we face. At the same time, we should be careful not to get carried away with AI's future promise but to root AI discussions and applications in global and local realities.
- It is crucial to involve communities and people with diverse backgrounds in the development of AI technologies. We need to build relevant technical, social and legal expertise. Cooperation can only grow if there is shared understanding of AI concepts and terms.

Generative AI

- Generative AI has shown that it can improve efficiency and accelerate innovation, but we also need to address and prioritise questions concerning the impact that this rapidly developing technology may have on human rights and democratic institutions across the world, including in the Global South.
- Policymakers need to take an inclusive approach to understanding AI impacts. Vulnerable groups that interact with generative AI should be proactively engaged in discussions about governing this new technology.
- All stakeholder groups should work together to protect and preserve truth. Disinformation and misinformation powered by generative AI (for example in the form of deepfakes) can obscure or change perceived reality. Promoting reliable information is vital, especially in the context of elections.
- It is important to accelerate the development of technologies that detect and identify AI-generated content. These efforts can help mitigate the risks associated with deep fakes and generative AI, promote responsible data use, and contribute to a more secure and trustworthy digital environment. Labelling AI-generated content will allow consumers to make more informed decisions and choices. Innovative interdisciplinary approaches are needed to develop the necessary approaches.

AVOIDING INTERNET FRAGMENTATION

Theme

There is widespread agreement within the IGF community about the value of a global, unfragmented Internet as a platform for human activity. Internet openness is considered instrumental in fostering the enjoyment of users' human rights, promoting competition and equality of opportunity, and safeguarding the generative peer-to-peer nature of the Internet.

Concern has been expressed, however, that divergence in the structure of the Internet may lead to fragmentation that could endanger connectivity and reduce the functionality and value of the Internet. A wide range of political, economic, and technical factors can potentially drive fragmentation. Concerns have also been raised about the effects of growing fragmentation of the Internet user experience, and about competition and lack of coordination between Internet governance processes and entities.

While legal, regulatory and policy approaches necessarily differ around the world, active coordination across international boundaries is vital to ensuring that fragmented approaches do not threaten the global reach and interoperability of the Internet. Global cooperation and coordination can identify early warning signs, mapping the impact of policies and other developments, and preparing to address the implications of such trends. A multistakeholder approach is widely considered to be that best suited for assessing, evaluating and monitoring the potential unintended consequences of measures that affect the Internet.

Messages

Multistakeholder participation

- The single global Internet is widely considered the bedrock of activity that is undertaken on it. The risks and potential impact of a fragmented Internet are, however, understood in different ways by different stakeholders in countries that have diverse Internet environments. There is a need to explore common ground and work towards a shared understanding of the issues in order to identify and collaborate on appropriate responses across these different contexts.
- The multistakeholder community should develop policy approaches and regulatory principles that are conducive to the continued evolution of a global and interoperable Internet. These approaches should avoid unnecessary limitations on the use of data and adverse impacts on the infrastructure of the Internet, while local data regulations should respect open and interoperable protocols. It should be possible to protect the legitimate interests of the general public and governments while avoiding Internet fragmentation and digital protectionism.
- States and other stakeholders may wish to explore the use of modular agreements to institutionalise dialogue and cooperation on Internet and digital economy issues, including those relevant to fragmentation. Developed countries should explore ways to faciltate developing countries' participation in such arrangements in order to advance digital development and attenuate the risk of Internet fragmentation.

The Global Digital Compact and WSIS+20 review

- The Global Digital Compact provides an opportunity to reassert the value of an open interconnected Internet within the context of the UN Charter, the Sustainable Development Goals and the exercise of human rights.
- It is important that the Compact should provide an opportunity for the technical community to engage constructively with government stakeholders and thereby bridge gaps between technical and policy perspectives. Using overly technical narratives in non-technical politicised discussions risks diluting trust in the Internet's technical layer and interoperability.
- The multistakeholder community should foster a comprehensive understanding of the challenges and opportunities surrounding content creation, access to information, and open Internet by re-evaluating the past, envisioning the future, and engaging in constructive dialogue.
- Ahead of the WSIS+20 review, the IGF community should look forward and seek to identify what the Internet could or should look like in twenty years' time and what actions are needed today to shape a positive vision for the future. Stakeholders should discuss the continued role of the Internet as a global network, identify potential risks associated with the splintering of the Internet and raise awareness about the perils of fragmentation and the need for collective action.

CYBERSECURITY, CYBERCRIME AND ONLINE SAFETY

Theme

The benefits of the Internet for economic development and social welfare cannot be fully realised without trust and security. Consideration of these aspects is integral to the development of safe, secure access to the Internet. It should reflect respect for human rights, openness and transparency in policymaking, and a multistakeholder approach that serves the interests of end-users.

Cybersecurity and cybercrime are important, sometimes overlapping but also distinct areas of public policy that require serious attention and the development of expertise. Cybersecurity – which seeks to protect the Internet's critical infrastructure, services, applications and devices from real and potential threats – is a central challenge for Internet policy. Cybercrime, meanwhile, poses an increasing threat to Internet users, with a long and growing list of types of harm that includes phishing, identity theft, Internet frauds, cyberstalking and online scams. Cyberattacks can also impact critical non-digital infrastructure including health systems and energy networks.

The international community should explore practical ways to mainstream cybersecurity capacity-building in broader digital development initiatives. Tensions between the desire to advance digital transformation and the need to enable effective cybersecurity pose challenges in enabling a safe, secure online environment and achieving the Sustainable Development Goals. Existing international agreements need to be translated into feasible actions.

Governments and policymakers should ensure that legal responses to criminal and terrorist use of the Internet safeguard the rule of law and human rights, take freedom of expression fully into account and demonstrate transparency and accountability.

Messages

Governance

- Governments should recognise the value of open, security-related Internet standards and use procurement processes to make their digital and digitally-enabled systems secure by design.
- The use of AI and machine learning may offer ways of strengthening cybersecurity and resilience. However, that use must be responsible and sustainable. Ethical principles can provide guidelines to help cybersecurity developers and users understand, assess and consider the application of these new technologies. Such principles are best developed in global multistakeholder discussions and should emphasise human control, transparency, safety, and privacy.
- Policy choices concerning cybersecurity, cybercrime and online safety are complex. Encryption, for example, is for some a privacy service but for others essential to guarantee freedoms of opinion and expression as well as other human rights. Anonymity has been a feature of much Internet activity and applications but can be abused to cause harm to other users. Examples like these suggest the need for systems that foster accountability while protecting expression and other rights. Layering identity levels may be one way in which such systems might develop.
- Policy choices may have effects that extend well beyond their intended objectives and beyond the jurisdictions, countries and regions in which they are introduced. Due to the interconnected nature of

the Internet, strengthening or weakening a service in one region may have a comparable effect on all users, where the impact of policy choices is not constrained by borders.

- The United Nations could do more to analyse the development of standards and regulations for the assessment of emerging technologies, share knowledge and best practice, and provide a platform for multi-stakeholder exchanges on how to develop common principles for emerging technologies. This could help to ensure that we have the right institutions in place to translate principles into binding standards and regulations.

Child safety

- All stakeholders should treat the best interests of children as a primary consideration. Addressing vulnerability and acknowledging the developing capacities of children across all areas of work related to digital development and Internet governance is essential if we are to ensure an inclusive, safe and secure online world – particularly for children who now make up a third of global Internet users.
- Children have the right to safe, inclusive age-appropriate digital spaces in which they can explore, learn and play. Data, evidence and knowledge-sharing are critical to placing children's safety and rights at the heart of global digital agendas including those concerned with cybersecurity and child online safety.
- States should ensure that consideration of children rights is integrated throughout legislation and regulation, rather than only in specific instruments, with reference to General Comment 25 to the Children's Rights Convention on children's rights in relation to the digital environment.
- Safety by design requires investment in child online safety across the entire ecosystem, with a particular focus on the capacities of low- and middle-income countries, as well as more upstream and collaborative action.

Gender-based violence

- Gender-based violence online deters many women and girls from taking full advantage of the benefits of the Internet. Policymakers need to develop multilayered strategies to prevent and respond to technology-facilitated gender-based violence that are grounded in human rights, evidence-based and can be applied to local contexts in partnership with communities and civil society organizations.

Cyber norms

- Informed discussions around cyber policy, norms and incidents require a comprehensive approach that considers dynamics across the entire ecosystem. When exploring the impact of norms on cyber incidents, it is not only important to examine them in relation to the cause, response, mitigation, and recovery of an incident, but also to consider consequential impacts across the ecosystem, including at the human level.
- The opportunities and challenges presented by the digital ecosystem empower and impact individuals and communities. Grounding efforts to improve cyber resilience at the individual, societal, economic, and even international levels would benefit from a full appreciation of the consequential impacts of policy decisions, norms, and incidents.

DATA GOVERNANCE AND TRUST

Theme

Data have become critical resources in the digital age and are being generated and stored in ever-greater volumes as a result of developments in digital technology, including AI and the Internet of Things. Existing legislative and regulatory frameworks at national, regional, and international levels are often insufficient to keep up with the pace of change in technology and applications.

Data flows are crucial to international cooperation in many fields including scientific research, law enforcement, and national and global security. The effective use and sharing of data on a global scale can help overcome shared challenges and the threats posed by cascading crises such as pandemics and climate change. Greater coherence is needed on a global level to achieve a balanced approach in which data work for people and the planet, including environmental sustainability.

Data can generate both commercial profit and social value. However, the benefits of a data-driven economy have so far been unevenly distributed. Many are concerned that individuals, and developing countries, have been and may remain primarily providers of data rather than beneficiaries. While the management of data is often highly concentrated, data poverty is also a significant problem, especially in local communities and among vulnerable population groups.

Lack of data privacy and inadequate data protection undermine trust in data management. Data flows and data exchange should take place without compromising the privacy of personal data. This can sometimes be sacrificed in the processes of data exchange, between the gathering of information and its application, with intentional and unintentional risks to trust and security.

Messages

International initiatives

- To make the power of data work for development, we need to establish trusted and secure ways to share data across borders. Data Free Flow with Trust (DFTT) is now widely discussed as a framing concept for the development of international data management and cross-border data flows.
- Principles and practical measures are needed to develop the concept of DFFT and establish common ground for data transfer that can facilitate the leveraging of data for development while addressing concerns about data privacy and data sovereignty. It is critical that developing countries participate fully in discussions concerning cross-border data flows and that the modalities for these reflect their needs and concerns.
- The African Union's Data Policy Framework has paved the way for a common continental approach to deriving strategic value for sustainable development from African data, and has shaped continental debates about more equitable data governance practices. Implementation of the Framework at national levels will be crucial in enabling African countries to take full advantage of the opportunities from cross-border flows and digital economy development within Africa's Free Trade Continental Area.

Data management and capacity-building

- Governments and regulatory bodies should work together to develop and implement comprehensive privacy regulations for private surveillance in public spaces. These regulations should address data control, transparency in data sharing, and protection of human rights. Collaboration amongst

stakeholders will help to ensure proper oversight and enforcement of these regulations to safeguard individual freedoms.

- Questions of data management, ownership and control are increasingly important. Civil society organisations, academia, the private sector and other stakeholders should collaborate on research and advocacy efforts, with the aim of unravelling the flow of data and holding both private surveillance companies and government authorities accountable for data management.
- Public-private data partnerships (which may require cross-border data sharing) have tangible benefits in times of discontinuity or crisis, but building trusted relationships requires time and often relies on informal relationships and intermediaries. Standard operating procedures and modalities for data interoperability would be helpful in bringing such collaboration forward.
- It is important to develop the capacity of policymakers, regulators, civil society, private sector and other stakeholders to participate meaningfully in discussions about data management at global, regional, and national levels.

DIGITAL DIVIDES AND INCLUSION

Theme

It is estimated that some 2.6 billion people- or one third of the world's population – are not yet users of the Internet. There are substantial digital divides between and within regions, countries and communities and there is a significant gender digital divide in many countries. Groups that are disadvantaged economically, socially and educationally also tend to be disadvantaged digitally.

Addressing these gaps in access, including the quality of access, is a central issue in building an inclusive Internet. The goal of digital inclusion is to level up the online environment so that everyone can embrace equitable digital development and socio-economic growth.

Meaningful access includes much more than connectivity. ICT infrastructure alone will not bridge digital divides, nor can online inequalities be addressed without understanding and responding to their relationship with offline inequalities. To achieve true value access must be inclusive, useful, sustainable, affordable and linked to digital literacy opportunities that respond to users' circumstances, skills, needs and priorities.

Policies and practices to promote access need to address the risk of leaving behind the most vulnerable, including those with disabilities, minority and refugee communities, sexual and gender minorities, older people, and those living in poverty or remote and rural areas. These communities need to be able to access goods and services both offline and online.

Messages

Meaningful connectivity

- As connectivity has increased, discussion of digital divides has shifted from coverage to usage, including the range of services available to users. Meaningful universal connectivity – which can be defined as the opportunity for everyone to enjoy a safe, satisfying, enriching, productive and affordable online experience – is increasingly seen as a fundamental enabler of human rights as well as economic and social development.
- Meaningful, universal connectivity is critical for enabling digital transformation and achieving the Sustainable Development Goals. Achieving it will require policymakers to embrace the concept as a policy goal, set indicators and targets for its measurement and achievement, and include it in national digital strategies, policies and implementation plans.
- Good quality data on all aspects of universal and meaningful connectivity are essential to inform and monitor digital policies, establishing the nature and severity of digital divides and identifying priority targets for policy interventions. Steps need to be taken to ensure such data are available to policymakers.
- Innovative policy and regulatory approaches are important in reaching unserved and underserved communities. Non-traditional financing approaches can support and build networks, including community networks, in areas with little or no connectivity. Libraries and other public services can provide connectivity to marginalized communities and individuals.

Digital Inclusion

- Overcoming digital divides requires access to be available to all within society. Governments and businesses should take steps to ensure accessibility for those with disabilities, for those with limited literacy and language skills and other marginalised groups.
- To connect communities that mainly communicate in oral forms, the Internet will need to adapt or create non-text-based communications, such as audio and video files/messages, transcription of alphabets and other intuitive forms of exchange. The online dominance of the Latin alphabet also needs to be challenged in order to facilitate access and usage by users of languages that use other alphabets.
- Open Education Resources (OER) have an important role to play in raising awareness and digital literacy skills. Governments and other stakeholders should help to ensure the quality of teaching and learning experiences by providing inclusive and accessible OER. Educational resources developed with public funds should be made available as OER, and more investment sought from both public and private sources.
- The development of initiatives for access and inclusion must be inclusive of target communities. Locally relevant and purpose-driven content is important for inclusion and requires incentives and funding to be sustainable, from production to distribution.

Capacity Development and leadership

- A holistic approach to capacity development is important for achieving sustainable and meaningful connectivity. Digital and media literacy skills are needed to enable full participation in online activity, including access to quality services and the capacity to deal with cybersecurity challenges. Technical skills are needed to understand emerging technologies and identify useful applications.
- ICT leadership amongst minority groups should be encouraged, reducing technology bias and improving localisation of services and products across different regions and communities.

GLOBAL DIGITAL GOVERNANCE AND COOPERATION

Theme

A positive vision for the future of the Internet has to consider many different strands and values concerned with sustainable development, human rights, access and openness, transparency and the rule of law, as well as technical considerations. This can best be done in an inclusive multistakeholder manner, where the interests of all actors can be addressed.

While the Internet contributes to social, cultural and economic growth, questions of governance, accountability, trust and access persist. As the Internet cannot be dealt with from a one-dimensional perspective, collaborative, equitable and inclusive Internet governance is imperative and requires well-structured coordination and consolidation. Dialogue between those concerned primarily with the Internet and those concerned primarily with other economic and public policy domains is essential in order to achieve best outcomes.

Monitoring of the impacts of Internet and other digital developments is also critically important to identifying opportunities, risks and ways of addressing these that are consistent with sustainable development and human rights.

The sustainability of the Internet governance ecosystem requires the involvement and engagement of young people, who are the next generation of users, experts and leaders. Given the rapid pace of technological change, it is important to build the capacity of future generations in all countries at all levels.

Messages

Digital governance

- Debates on digital governance increasingly recognise the symbiotic relationship between governance of the Internet and broader governance of economies and societies in the digital age. While the Internet remains a core component of the digital society, these discussions should extend to broader concerns, including the ways in which digital technologies impact society, issues such as data rights, AI ethics, and the broader digital ecosystem. The challenges of digital governance transcend the traditional boundaries of Internet governance, and it is important to view them holistically.
- Digital governance rests on a number of fundamental or foundation issues. Emphasising these ensures that the digital governance ecosystem is grounded in principles that have stood the test of time. By addressing core challenges such as data privacy, digital rights, cybersecurity and infrastructure development, the digital governance community can create a more resilient and secure foundation for the evolving digital age, which can respond more effectively to challenges of the moment.

Multistakeholder participation

- Diverse participation promotes a comprehensive understanding of the complex issues surrounding digital governance. Ensuring that a wide range of perspectives is represented in the digital governance dialogue is therefore crucial. This extends beyond gender, nationality and stakeholder participation to encompass a broad spectrum of voices, including those from legislative and judicial branches of government. Inclusivity should ensure that no single group dominates the conversation and that all voices are considered when shaping the future of Internet governance.

- The multistakeholder model has been a defining characteristic of Internet governance, allowing a diverse range of stakeholders, including governments, civil society, businesses, and the technical community, to participate in decision-making, facilitating both inclusivity and collaboration and promoting a balanced and fair approach to addressing the challenges of the digital age.
- Multistakeholder processes have seen success and increasing use over the last two decades. The multistakeholder community has evolved since WSIS and the range of different interests represented within stakeholder grouping has increased. It is important that Internet governance and international processes such as WSIS+20 reach beyond referencing the importance of multistakeholderism and shape modalities that include stakeholder mapping, welcome diverse participation and draw on diverse expertise. Innovative channels for contributions should be considered, with particular emphasis on the value of broadening engagement by individuals and under-represented stakeholder groups and countries.
- Businesses play a crucial role in the digital ecosystem. Their involvement is vital in addressing the complex challenges and opportunities presented by the digital age. They also have a wider responsibility to contribute to shaping digital governance, contributing expertise on issues such as cybersecurity, data governance, and digital inclusion.
- Businesses have an interest in a stable and secure digital environment that fosters innovation and growth. While they seek profitability and market growth, they should also recognise that digital governance must also serve the broader public good.

The role of the IGF

- The IGF's evolution from discussing solely Internet governance to addressing a wider range of digital governance issues reflects the dynamic nature of the digital age.
- The IGF's visibility and profile need to be raised, through an effective outreach strategy, if it is to continue serving as a hub for constructive dialogue and collaboration, attract new stakeholders and engage diverse groups in shaping the future of Internet governance.
- To address the complex and multifaceted nature of Internet governance, entities like the IGF need adequate funding and resources. Sufficient funding is needed to support research, operational activities and the coordination of stakeholders. Without proper resources, critical initiatives and projects may go unrealised, impeding the development of ideas and initiatives in global digital governance.

HUMAN RIGHTS AND FREEDOMS

Theme

Access to the Internet should be accessible and safe for all. It should respect the civil, economic, social and cultural rights set out in international rights agreements, including human rights treaties and other relevant rules of international law. It is important to improve the monitoring and implementation of digital rights at all levels, building on national and global mechanisms.

The Internet provides a crucial opportunity for access to information and expression as described in Article 19 of the International Covenant on Civil and Political Rights. Governments should avoid recourse to Internet shutdowns because of their negative impact on both human rights and economic welfare. The Internet also provides opportunities for enhancing rights to education, as part of broader policies for educational improvement.

Concerns are widespread about disinformation and misinformation, the use of online services for criminal activity, child abuse, hate speech and interference in election and legal processes. Regulatory approaches to these and other challenges are under discussion in many countries and fora. Outcomes should be consistent with the full range of human rights set out in international rights agreements, standards and norms.

Artificial Intelligence needs to be developed and deployed in ways that allow it to be as inclusive as possible, non-discriminatory, auditable and rooted in democratic principles, the rule of law and human rights. Concerns are increasingly expressed about risks associated with AI, including surveillance and the automation of decision-making. These should be addressed in multistakeholder fora in the context of sustainable development and human rights.

Messages

Governance and rights

- Human rights and dignity should be at the centre of governance frameworks for digital technologies, including AI, addressing risks and threats in respect of data privacy and surveillance, freedom of expression and assembly, manipulation and hate speech, disinformation and misinformation.
- Governments have the responsibility to ensure that human rights are implemented in practice, both online and offline. To do so effectively, they need to invest in training and capacity-building of policymakers, judges and other legal professionals.
- Policymakers need to improve their understanding of Internet technologies, the infrastructure underpinning them, their modalities and business models if they are to make informed policy decisions and design appropriate regulatory frameworks. Greater transparency on the part of businesses and other stakeholders can help to achieve this.
- It is important to acknowledge the interconnection of local and global issues and to ensure representation and access to digital policy discussions for those communities and sectors that will be most affected by them.

- Technology is not confined by geographic boundaries. Laws and regulations governing the use of technology in areas such as encryption should be consistent with international standards and norms concerned with privacy, freedom of expression, due process and access to information.

Access to information

- Discrepancies in data access (particularly in the Global South) and potential conflicts between international and local regulations limit the capacity of research, analysis and reporting about the impact that digital platforms have on society, including their impact on journalism and news media.
- High quality journalism is an effective medium against the impact of disinformation but faces an uncertain future. More work needs to be done to strengthen independent journalism, particularly in countries with a high incidence of disinformation.
- Governments should avoid recourse to Internet shutdowns, which impede the free flow of information and threaten human rights and democratic processes, particularly during election periods. While some governments lack the tools, knowledge, digital literacy and access to the wider multistakeholder community to address issues of concern through effective content moderation, shutdowns do not address the root causes that need to be addressed but undermine rights and prosperity.
- The information space plays an increasing role in conflicts. Digital risks and restrictions on the free flow of information can harm civilians in conflict zones. Digital companies have become important actors in conflict and often find themselves in extremely challenging circumstances, having to ensure safety of staff and deal with demands made by belligerents. Alongside their responsibility to respect human rights and humanitarian law, they should be guided by the principle to minimise harm during conflict.

Misinformation and disinformation

- Misinformation is defined as the unintentional spread of inaccurate or false information, while disinformation is deliberately falsified content specifically designed to deceive. These pose significant challenges for public policy within society as a whole as well as in the digital sector.
- Governments need to work together with technology companies and civic actors around a shared set of values to address the changing nature of misinformation and disinformation as technology evolves. Communities need to be empowered with the digital literacy tools and training to identify false content.
- Synthetic information or content is media manipulated from its original meaning or appearance for whatever purpose. Generative AI makes the production of synthetic information faster and easier with potentially adverse consequences for political processes, including elections, where disinformation by malicious actors can mislead and subvert democratic outcomes.
- A more nuanced approach to disinformation is called for, which should focus not only on social networks or digital platforms but also consider the wider media landscape. More empirical research is needed to assess the risks of disinformation for political activity and democratic process.
- There is not one global solution against disinformation that works in every instance or context. It is unlikely that governments will agree on how best to address it. However, it should be possible to work towards a common set of principles to guide policy development, building on human rights and access to information.

The role of businesses

- Private companies can play a crucial role in securing human rights and have a responsibility to the societies in which they operate to respect rights in their business practices. This requires careful and effective risk assessment, monitoring of their impact on human rights, and due diligence in their delivery and supply chains when designing, developing and using digital technologies, including AI.
- Digital businesses would benefit from greater guidance on what it means for them to respect international human rights and humanitarian law. A multistakeholder approach (including international organisations, humanitarian actors, digital companies, and human rights organisations) can help to fill gaps in understanding on how they can contribute to ensuring rights and freedoms.

SUSTAINABILITY AND ENVIRONMENT

Theme

Digital technologies can contribute towards environmental protection and the mitigation of environmental harms, but also have significant adverse environmental footprints that need to be addressed.

Digitalisation can provide tools and devices that help to monitor, mitigate and adapt to climate change – for instance by using digital technologies to evaluate consequences of actions already taken, monitor emission and pollution levels, and develop new approaches in other economic sectors that will be more sustainable. Areas of beneficial application of digitalisation include (among others) environmental data, food and water systems.

However, current levels of exploitation of some scarce resources used in digital and other new technologies, including rare earth elements, are known to be unsustainable. Extraction of resources critical for digitalisation is also associated with biodiversity loss and water stress. At the other end of the digital lifecycle, more than 50 million tonnes of e-waste are generated globally each year, little of which is currently recycled.

Urgent action is required concerning the digital sector's carbon emissions, which are substantial, growing and projected to grow further as the Internet of Things and AI become more widespread.

Environmental impacts arise at all stage of the digital lifecycle, including manufacturing, infrastructure, data storage, analysis and computation, usage by organisations and individual, and disposal. Increased attention is being paid to the potential for a more circular digital economy, including measures to improve energy efficiency, extend the life of digital devices, foster sustainable production and consumption, encourage reuse and recycling, and recover scarce resources.

Messages

The relationship between digitalization and the environment

- Discussions about digital transformation and climate change are still held overwhelmingly in separate silos, and there can be misunderstanding of the links between digital technology and the environment. It is important to make the link between digital technology and environment more widely understood, in particular by building a stronger interface between decision-making bodies concerned with digital development and environmental sustainability at both national and international levels. The achievement of an inclusive and environmentally sustainable digital society is critical to the achievement of the SDGs.
- Digital and environmental transitions should be consistent and mutually sustainable, not least because digital policies that are not environmentally sustainable will not be sustainable in any other sense. Responding to this requires progress from high-level discussion towards clear standards, regulation and action by all stakeholders.
- Environmental experts should discuss the challenges they face with technologists in order to identify practical ways in which digital technology might facilitate sustainability. It is important that digital approaches reflect the real circumstances in which they are to be deployed, including cost, connectivity,

reliability and maintenance constraints. What is appropriate in one context is very often inappropriate in others.

- The IGF's community of NRIs can play a useful part in linking digital and environmental issues at global and national levels.

Addressing environmental challenges

- Digital technologies can contribute to better understanding of the environmental problems facing the world community. The large volumes of data now generated by digital services and the scope and scale of AI-powered analysis can complement environmental monitoring systems to enable better targeting of policies and interventions to reduce environmental impacts and support mitigation of and adaptation to the impact of climate change.

Addressing the digital environmental footprint

- Digital technologies have significant adverse environmental impacts which are particularly concerned with the exploitation of scarce resources, energy consumption and climate change, and the generation and dumping of electronic waste. All stakeholders have a responsibility to minimise these impacts.
- The adoption of principles of environmental sustainability by stakeholders within decision-making processes will be critical to enabling a just green transition. Such principles should be incorporated in the design of national digital strategies, business models and practices, and the design and deployment of networks, devices, applications and services.
- Environmental responsibility in the digital sector should be increased. Efforts in greening the digital sector must reach beyond data centres to cover the entire value chain. Governments and international bodies should collaborate to mandate responsible production, usage, and disposal of electronic devices. Penalties for non-compliance and incentives for eco-friendly practices are crucial for accountability and driving sustainability.
- Standards play an important part in setting the framework within which digital products and services are deployed within societies. Standard-setting bodies should consider environmental impacts in their decision-making processes, reflecting the need for products and services to reduce their use of scarce resources and minimise energy consumption and carbon emissions. Businesses should commit to the use of environmentally responsible standards in product and service development.

A circular digital economy

- There is increasing interest in transition towards a more circular digital economy, characterised by more efficient use of scarce resources, increased use of renewable energy and improved energy efficiency in networks and devices, more selective data storage, increased longevity and adaptability of digital devices (including repair and re-use) and better management of devices at their end of life.
- Recycling and recovery of scarce resources have a vital role to play in the environmental management of digitalisation. Levels of recycling – particularly of toxic chemicals and scarce minerals – must be increased to ensure the safety of individuals and long-term security of supply, and the international trade in electronic waste should be regulated to protect the interests of recipient countries, particularly in the Global South.

- Information on environmental choices should be easily accessible to all individuals. Digital businesses should be transparent about the environmental impact of their products and services and provide information to consumers. Governments can adopt sustainable procurement policies to encourage more sustainable product development.

AI and new technologies

- Environmental and climate considerations need to be incorporated into the development of AI. We need to ensure that AI does not create more problems than it solves and mitigate its impact on climate. The environmental efficiency of AI should be carefully and transparently evaluated. Capacity-building, information-sharing and support for sustainable, local AI ecosystems should be promoted.
- Governments and the private sector should fund research in renewable energy, eco-friendly hardware and efficient cable-laying and satellite deployment. Financial support and incentives can fuel the development of impactful, environmentally conscious approaches, paving the way for a greener digital future.