IGF LEADERSHIP PANEL

CONTRIBUTION TO CONSULTATION ON THE GLOBAL DIGITAL COMPACT

Introduction

In line with the mandate of the Internet Governance Forum (IGF) and as recommended in the Secretary-General's Roadmap for Digital Cooperation, the United Nations Secretary-General has established the IGF Leadership Panel as a strategic, empowered, and multistakeholder body.

Among the key functions of the IGF Leadership Panel are the responsibility to provide strategic inputs and advice on the IGF; promote the IGF and its outputs; and exchange IGF outputs from the Forum with other stakeholders and relevant fora, and facilitate the feeding of input of these decision-makers and fora to the IGF's agenda-setting process, leveraging relevant MAG expertise.

In this context and based on existing IGF outputs, the Leadership Panel is pleased to make the following contribution to the ongoing consultation of the United Nations on the **Global Digital Compact**. This contribution is based on the IGF 2022 messages, as agreed by the participants to the IGF in Addis Ababa. IGF messages are a summary prepared by the IGF secretariat after each annual IGF meeting, which are commented on and agreed by the multistakeholder community.

Support for the Global Digital Compact

The Leadership Panel strongly welcomes the initiative of the United Nations Secretary-General to propose a **Global Digital Compact** in the report on *Our Common Agenda*. We welcome the focal value the Global Digital Compact, and by extension the digital transformation, the internet and new technologies have in the *Summit of the Future*, scheduled to be held in September 2024.

The Global Digital Compact should represent important steps towards achieving the **UN Sustainable Development Goals**. Beyond this, the Global Digital Compact should not only recommend **guiding principles** for the internet of the future, but should identify **clear and concrete actions** to achieve its objectives, including metrics to **measure progress towards achieving these goals**.

The GDC should reaffirm the MSH model of Internet Governance, all while following a multi-stakeholder approach in its' genesis. The Leadership Panel would urge the Global Digital Compact facilitators to explore possibilities for the **whole multistakeholder community to be involved** in the Global Digital Compact process, **beyond the consultation phase**. We therefore call for a dedicated **Multistakeholder Drafting Group** to support the development of the Global Digital Compact, once the formal consultations are complete. While negotiations will take place among Member States in the UN General Assembly, the multistakeholder community should have the opportunity to meaningfully feed into their discussions. We recall that, while the GDC will be adopted by governments, implementation and monitoring will be undertaken by the whole multistakeholder community, and as such, their perspectives should be fully represented throughout. The IGF 2023 in Kyoto can play an important role in this regard.

Future of Internet Governance Forum

The Leadership Panel supports the Internet Governance Forum and its global, national and regional initiatives as vital fora for multistakeholder debate and policy discussions that can inform policy development across the world. The Global Digital Compact should reaffirm the definition of multistakeholder internet governance as agreed in the Tunis Agenda as well as reaffirm the importance of the Internet Governance Forum. At the same time, the Global Digital Compact should

not touch upon the mandate of the Internet Governance Forum, which is to be renewed in the WSIS+20 process.

We recommend that the **IGF be used as a follow-up and evaluation platform for the Global Digital Compact** beyond its adoption in 2024, as all stakeholders present at the IGF will have a role to play in the implementation of the GDC.

Connecting All People and Safeguarding Human Rights

IGF recognises that the digital divides within and between countries and regions remain powerful actors affecting national and international development, including progress towards the UN Sustainable Development Goals (SDGs). Meaningful access extends well beyond issues of connectivity and includes aspects of divide that cur across various parameters, including issues of accessibility, affordability, content, services, digital literacy and other capabilities as well as connectivity, especially in the Global South. The digital gender divide must be eradicated, including efforts to reduce gender-based violence online. Human Rights must be protected online by all stakeholders, including by expanding opportunities for education and digital skills.

OVERCOME THE DIGITAL DIVIDE

Core Principles:

- **The Digital Divide should be overcome among geographical regions, but also within societies, where some groups have less meaningful access, including women, individuals in vulnerable situations, and vulnerable and marginalized communities**. Meaningful access must be a guiding principle for connecting peoples, especially the Global South, and must address such issues as accessibility, affordability, content, services, digital literacy and other capabilities as well as connectivity.
- Meaningful access includes aspects concerning access to information, services, digital literacy, and other capabilities in relation to digital inclusion and capacity development that go beyond the issue of connectivity.

Key commitments:

Targeted initiatives in infrastructure, devices and services can help to improve access for the non- or less-connected. Governments should **protect and promote required infrastructure**, along with support from the private sector, including – by means of innovative investment models – in rural areas. **Cooperation** among stakeholder groups is important in ensuring and enabling access: governments and multistakeholder partners should contribute to the establishment and work of effective regulatory agencies and frameworks, address challenges in commercially unattractive areas, and encourage innovative approaches to connectivity.

PROTECT WOMEN'S RIGHTS

Core Principles:

Concepts of gender equality, inclusion and women's and girl's rights and protection should be incorporated into the Global Digital Compact: the threat of violence and harassment is a deterrent to women's and girls' online participation. The role of technology services and platforms in propagating gender-based violence should be acknowledged and addressed. Also, built-in bias in algorithms reinforces existing structures of discrimination based on gender and have to be urgently addressed.

Key commitments:

- All stakeholders should contribute to ensure that the gender digital divide is eradicated.
- The GDC should call upon all stakeholders to work together towards eradicating the digital gender divide. Every member of society, especially the most marginalized must have equal access to digital technologies, services and skills. Digital services should be tailored and accessible for all women and girls.
- Governments should commit to promote digital, sciences and technology education for girls. All stakeholders have a role to play in ensuring the technology and innovation sectors are attractive to and welcoming of women.
- All stakeholders should commit to making digital technologies safer for women, more transparent and accountable and to ensure that no bias is embedded into algorithm-based technologies.
- Finally, governments, together with all stakeholders, must establish clear accountability for all forms of online discrimination, including violence, against women.

PROTECT HUMAN RIGHTS

Core Principles:

The Global Digital Compact should reaffirm the fundamental principle that all human rights that apply offline also apply online. Respect for human rights must be a key consideration for new and emerging technologies from the moment of their design throughout their entire life-cycle. Governments are responsible to ensure that human rights are respected, protected and promoted while businesses are obliged to comply with all applicable laws and to respect human rights. Blanket Internet shutdowns are not consistent with international human rights law and undermine the achievement of the Sustainable Development Goals by e.g. hindering access to health and education, access to information etc. . Any restriction must be lawful, suitable and legitimate, necessary, proportional, and non-discriminatory.

Key commitments:

- Transparency, accountability, and human rights due diligence are the responsibilities of all stakeholder groups, including intergovernmental and international organisations, governments and the private sector, the technical community and civil society.
- governments must ensure that any restriction of internet access is strictly compliant with the principles of legitimacy, adequacy, necessity, proportionality and non-discrimination. States should avoid recourse to limiting access to the internet at all costs, because of negative impacts on both human rights, sustainable development and economic welfare. Social media and technology companies should explore all legal options for challenging requests for shutdowns and support citizens in their advocacy efforts concerning shutdowns.
- All stakeholders can and should contribute to realizing the potential of the internet and digital technologies for **enhancing rights to education**, **helping smaller and local businesses take advantage of the digital economy**, and **improve access to training in digital technologies** to support the labour market to adapt to new paradigms.
- Standards development organisations should introduce processes to ensure due consideration of human rights in their work, including by inviting participation of experts in human rights, from all stakeholder communities.

Avoiding Internet Fragmentation

IGF holds as a core principle that the internet must be global, open, free and interoperable, supported by common technical standards and protocols. Such standards, including those for content and services, must be consistent with the rule of law and international human rights.

ADDRESS INTERNET FRAGMENTATION

Core Principles:

- The Global Digital Compact should reassert the value of a global open, free, interoperable internet for the realisation of the UN Charter, the achievement of the Sustainable Development Goals, and the exercise of human rights. Furthermore, the many aspects of internet fragmentation should be the focus of multistakeholder attention: technical, commercial and policy considerations can all contribute to a fragmented internet.
- Net neutrality, non-discriminatory traffic management, infrastructural and data operability, and platform and device neutrality are all important components of an overarching policy framework to support an open, interoperable internet.

Key commitments:

- Effective multistakeholder governance mechanisms are essential for the governance of a global unfragmented Internet.
- The **multistakeholder community must remain vigilant** against new or developing risks of internet fragmentation. In this regard, the Leadership Panel welcomes the work done by the IGF Policy Network on Internet Fragmentation, and encourages the continuation of this work, to support governments, private sector, civil society and the technical community to be aware of possible threats to the open internet.
- While legal and regulatory approaches may differ among jurisdictions, concerted effort must be made to **maintain active policy compatibility at the global level**, to ensure that fragmented approaches do not threaten the global reach and interoperability of the internet. Maintaining the integrity of the global network requires international collaboration and consensus on basic principles. In addition to international regulatory collaboration, frameworks must keep pace with rapid change in technology and services.
- Cyber-diplomacy networks and mechanisms should support the regulatory framework to protect the open and interconnected internet; standards development organisations should maintain active engagement and outreach to improve understanding and collaboration between the technical community and policymakers.

Governing Data and Protecting Privacy

IGF recognises the centrality of data in today's economy and society, and the fundamental role of data in the future. Data are a critical resource, and data flows can be a vital element for international cooperation (e.g. scientific research, law enforcement, and national and global security), and can support with management of transversal crises such as pandemics and climate change. IGF recognises that data can generate both profit and social value, but that issues of data poverty and the protection of the right to privacy and personal data can cause populations to be left behind economically, and erode trust in the digital economy.

PROTECT PRIVACY

Core Principles:

Privacy is not only an individual right but also a social value and should be considered with a whole-of-society approach and not restricted to governments. **Privacy laws should be substantial, evidence-based and subject to clear enforcement, accountability and remedy**. Laws should ensure that data flows and data exchange can take place without compromising on security and data privacy, and that internet access and use should not be dependent on data-tracking. Furthermore, personal data should not be exported into jurisdictions which do not provide adequate guarantees.

Key commitments:

- **Policies, developed through meaningful multistakeholder input, must ensure the protection of personal data**. Independent oversight bodies should be established and enabled with adequate resources.
- The private sector must endeavour to adopt a privacy-by-design approach in its innovations and developments to safeguard the rights of users.

ESTABLISH GOOD DATA GOVERNANCE

Core Principles:

- Policies should ensure that individuals have agency over their personal data and that privacy protections contribute to a safer and more prosperous global digital economy. Interoperability and compatibility of approaches to data governance would help achieve a balanced approach in which data work for people and the planet.
- **Transparency, participation and accountability are important aspects of good data governance**. This includes consideration of standards, sharing, interoperability, security, privacy, infrastructure, fairness, transparency and explicability, data minimization, and quality and accuracy.
- Current multilateral, regional and bilateral trade agreements are insufficient to enable current and future cross-border data flows: there is thus a growing need to develop and harmonise measures to manage cross-border data flows with trust and in full respect of personal data protection.

Key commitments:

- Policies for good data governance should be **designed with the full input of the multistakeholder community**, including regulators, researchers, standards development organisations, consumer organisations, end-users, private sector and civil society.

- Policy frameworks should enable the free-flow of data across borders with trust, underpinned by the highest standards of personal data protection, in order to allow for the full benefits of e-commerce and digital trade to be realised, in addition to the realisation of development goals.

Enabling Safety, Security and Accountability

IGF recognises the multifaceted nature of the threats on the internet, including cybersecurity (protection of networks and data), misinformation and disinformation, and other safety considerations. This encompasses the ongoing problem of cyber-attacks, whether perpetrated by individuals or state-sanctioned. Furthermore, there should be a harmonised approach to protect victims, particularly women and girls, and to empower women to lead in the digital space.

IMPROVE CYBERSECURITY

Core Principles:

- Cybersecurity should be seen as a **central challenge for internet policy** and the digital transformation as a whole. Ensuring cybersecurity and preventing cybercrime are both important areas of policy requiring a high level of expertise and multistakeholder input.
- **Whole-of-government and whole-of-society approaches** are required, which include strong partnerships and coordinated efforts, involving parliaments, regulators, the judiciary, law enforcement and other relevant government agencies, the private sector, technical community, academia and civil society.

Key commitments:

- **Standards that enable cybersecurity, in particular the UN normative framework of responsible State behaviour in cyberspace, are essential** for an open, secure and resilient internet that enables social progress and economic growth, and are particularly important for those not yet connected. The Global Digital Compact should promote such standards and related advocacy and capacity-building activities.
- The Global Digital Compact and multistakeholder community should contribute to **raising awareness** among policymakers and other stakeholders **of the challenges of cybersecurity and of existing international norms** and principles.

COMBAT CYBERCRIME

Core Principles:

Regulations meant to counter cybercrime should be **proportionate**, human rights compliant and sensitive to the size, capacity and resources of service providers, with legal obligations considering the diversity of the private and technical sector.

Key commitments:

Governments and policymakers should ensure that legal responses to cybercrime **safeguard both the rule of law and human rights**, taking freedom of expression fully into account.

COMBAT DISINFORMATION AND ILLEGAL CONTENT

Core Principles:

Disinformation should be addressed through risk-based **mechanisms while protecting freedom of expression**, pluralism and democratic process.

Key commitments:

- The multistakeholder community should collaborate to improve **media and digital literacy skills**, which empower citizens to take a more critical view of the content of information they encounter, helping to identify misinformation and strengthen democratic participation. **Educational curricula** should also include digital literacy skills that help children to be safe online.
- Policies should take full account of the technical landscape, recognizing that the **domain name system** has limited technical capacity in this context – stakeholder dialogue should continue to clarify when and how it may be used to remedy specific content problems. Encryption also plays an important role in building an open, safe and democratic internet. It has the ability to validate provenances and bona fides as well as protecting information from unauthorized access.

Addressing Advanced Technologies, including Artificial Intelligence

IGF recognises that new digital technologies are increasingly shaping our economy and society, including AI systems. Taking advantage of the opportunities offered by advanced technologies, while addressing related challenges and risks is a task that no one actor can take up on its own. Multistakeholder dialogue is required to ensure that these technologies are developed and deployed in a manner that is human-centric and respectful of human rights.

DEVELOP HUMAN-CENTRIC AI

Core Principles:

Advanced technologies, including artificial intelligence, should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and includes appropriate safeguards. Risks, including bias, should be mitigated in design and implementation of such technologies, with the objective of protecting vulnerable and marginalized groups.

Key commitments:

- Governments, together with the whole multistakeholder community, should work together to progress towards internationally agreed norms and standards to govern the implementation of AI. The Global Digital Compact should recognize existing and ongoing efforts and processes.
- Capacity-building is of the utmost importance: AI literacy, skills development and language resources for minority languages must be priorities for education and training policies.

ENSURE TRUST

Core Principles:

- Transparency in the operation, explainability and reporting of algorithmic systems is essential for human rights.

Key commitments:

Stakeholders from technical and non-technical communities should share expertise and work together to develop principles, guidelines and standards that are sufficiently flexible for application in diverse contexts and **foster trust in AI systems**.

PROTECT RIGHTS IN CONTENT MODERATION

Core Principles:

Policies on content governance by online platforms, and their governance, should be designed in line with international human rights standards.

Key commitments:

- Automated tools employed to moderate online content, such as AI applications, should be **used in a context of transparency**, accountability and oversight. Unintended consequences of

such technologies, which can be particularly detrimental in times of conflict or crisis, should be avoided.

- **Technical standards play an important role** in enabling the development and enhancing the value of digital technologies and related infrastructures, services, protocols, applications and devices. Effort should be made to ensure that such standards are set in transparent and clear processes, to take human rights concerns fully into consideration and **encourage full participation from all stakeholders**, **including financial support** for expert participants from governments, academia, private sector, technical community and civil society.

Other issues

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE CHANGE

Core Principles:

- Digitalisation provides opportunities, tools and devices to combat and adapt to climate change, including the use of environmental data to mitigate climate change, data to manage food and water systems, support the circular economy, and reduce e-waste

Key commitments:

- The enabling role of digital technologies and the ICT ecosystem should be recognised and harnessed in public policy, to allow for the development of impactful new applications to combat the effects of climate change
- A more extensive use of new technologies, in the appropriate legal framework, should be encouraged, as a way to achieve sustainability and drive digital inclusion.
- Stakeholders should agree upon a core set of environmental variables, which are systematically collected, shared, and validated on a global basis. This should be published as Digital Public Goods for the benefit of all. The roles of such stakeholders as collective data-stewards of digital public goods should be developed through a multi-stakeholder process. It should seek to include, collect, and utilise environmental data under clear principles and procedures, within a human-centric framework.