IGF

Seventeenth Meeting of Internet Governance Forum

28 November – 2 December 2022
Addis Ababa, Ethiopia

IGF ETHIOPIA
2022 ኢትዮጵያ

Disclaimer:

The views and opinions expressed herein 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.

IGF 2022 Summary

Seventeenth Meeting of Internet Governance Forum
28 November – 2 December 2022
Addis Ababa, Ethiopia

citizens, violating human rights of individuals and groups. We need to keep working for a safe, equitable and open disability future that does not infringe on privacy or
IGF ETHIOPIA 2022 ኢትዮጵያ
The 17th Annual Internet Governance Forum
United Nations
IGF Internet Governance Forum
RESERVED
RESERVED

Contents

Glossary

BPF Best Practice Forum

CSTD Commission on Science and Technology for Development

DC Dynamic Coalition

DPIDG Division for Public Institutions and Digital Government (DPIDG)

IGF Internet Governance Forum

IoT Internet of Things

ITU International Telecommunication Union

MAG Multistakeholder Advisory Group

NRI National, Regional and Youth Initiative

PN Policy Network

PNIF Policy Network on Internet Fragmentation

PNMA Policy Network on Meaningful Access

UN DESA United Nations Department of Economic and Social Affairs

UNOG United Nations Office at Geneva

WG (MAG) Working Group

WG-OEC Working Group on Outreach, Engagement and Communications Strategy

WG-Hybrid Working Group on Hybrid Meetings

WG-Strategy Working Group on IGF Strategy

WSIS World Summit on the Information Society

Internet Governance Forum

The Internet Governance Forum (IGF) is a global multistakeholder platform that facilitates the discussion of public policy issues pertaining to Internet governance.

The IGF was one of the most important outcomes of the United Nations World Summit on the Information Society (WSIS) that mandated the United Nations Secretary-General to convene the Forum on 18 July 2006.

The existing mandate of the IGF as set out in paragraphs 72 to 78 of the Tunis Agenda was extended for a further 10 years in a resolution adopted by the UN General Assembly on 16 December 2015, (70/125), 'Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society.

Institutionally, the IGF is supported by the IGF Secretariat, which is administered by the UN Department of Economic and Social Affairs (UN DESA). The programme of the annual IGF meeting is developed by its Multistakeholder Advisory Group (MAG), whose members are appointed by the UN Secretary-General. An IGF Leadership Panel, with members also appointed by the Secretary-General, began its work in 2022.

So far, seventeen annual meetings of the IGF have been hosted by various governments. The eighteen annual IGF meeting will be hosted by the Government of Japan in Kyoto in 2023.

Foreword

Amid a new era of global challenges, the world has also embarked on a new wave of technological revolution. Digitalization has cemented its transformative role in current and future scenarios of sustainable development. Emerging technologies like artificial intelligence, robotics, blockchains and the Internet of Things are integrated rapidly into all sectors and woven into the fabric of our society, driving the irreversible digital transformation forward.

It is in this context that the Internet community alongside with key stakeholders from Governments, the private sector, civil society and more gathered in Addis Ababa for the 17th Internet Governance Forum (IGF), for a week in November and December of 2022.

The success of the Forum was evident in the intense debates and rich outcomes, illustrated vividly through this Summary Report and especially the Addis Ababa IGF Messages, across the five main themes of meaningful connectivity, avoiding Internet fragmentation, governing data, enabling safety, security, and accountability, and addressing advanced technologies.

This would not be possible without the immense support of the host Government of Ethiopia, the United Nations Economic Commission for Africa, the Multistakeholder Advisory Group of the IGF, as well as the close partnerships of many UN agencies, international and regional organizations, and many other strong supporting partners and stakeholders of IGF.

The Forum also marked the culmination of the work carried out throughout the past 12 months by the network of national regional IGF initiatives (NRIs), and multiple IGF intersessional activities such as the policy networks, the best practice forums and dynamic coalitions.

Mr. Li Junhua
United Nations Under-Secretary-General
for Economic and Social Affairs

It was more than ten years ago when the IGF was held in Nairobi in 2011. The 17th IGF was, therefore, particularly meaningful for the African continent, where we need to step up global efforts to connect the unconnected in meaningful ways, and where we also need to better harness the energy of the African youth. I am certain that we will continue to engage, cooperate and collaborate with the African Governments, Parliamentarians as well as other important stakeholders a free, inclusive open and save Internet for all.

Secretary-General António Guterres reminded us about the perils of the Internet through his opening remarks, about online bullying and deadly disinformation that undermines democracy, human rights and science. While technologies are transforming lives and livelihoods, they are also outpacing regulations and exacerbating inequalities. The Secretary-General urged us to keep working for a safe, equitable and open digital future that does not infringe on privacy or dignity.

The proposed Global Digital Compact of the Secretary-General speaks to the need and reality of our interconnected society, and that we need unity and digital cooperation. The IGF Leadership Panel together with the Multistakeholder Advisory Group, will join us as changemakers of the Internet for good.

The Internet Governance Forum is now primed to rise further to the challenge of delivering the full potential for all. Together, let us make full use of the important outcomes of the 17th IGF and to continue building on these successes for the 18th IGF, to be hosted by the Government of Japan in Kyoto in 2023.

Foreword

Mr. Antonio Pedro
United Nations Acting Executive Secretary
Economic Commission for Africa

Information and Communication Technologies (ICT) and the digital economy play an ever-growing role in shaping a successful and prosperous society and economy. ICT drives all facets of modern life, from our healthcare, education, economic development, and daily activities. Divergent trends in global development outcomes, driven by the multitude of exogenous shocks in the last four years, threaten to slow down Africa's digital transformation and economic development at large. Further, in light of the world population reaching eight billion, it is critical to redouble efforts to bridge the digital gap between the connected and unconnected people.

The 17th Internet Governance Forum (IGF), held in Addis Ababa, Ethiopia and hosted by the Government of Ethiopia and UNECA, offered a direct opportunity to shape the global digital agenda and brought together ICT practitioners and policy makers from around the world with a mission to leverage digital technologies to transform national and international development outcomes.

In the 17th IGF, we were privileged to host for the first time the African Parliamentary network on Internet Governance – a fete of its own with sessions that strengthened the parliamentary track. The Youth congress and Volunteers brought with them vibrancy and strength. In addition, the launch of the Coalition for Digital Africa, Africa Internet Community Backpack Initiative, ECA's Cyber Security Model Law as well as the town hall with the UN Tech Envoy on the Global Digital Compact reaffirmed our collective commitment to digital transformation. The UN Global Digital Compact consultations, for instance, offer a platform to continue the learnings and networks forged at IGF.

With its over three hundred sessions, this has been the largest IGF since its inception 17 years ago. We truly did make history and I extend my special gratitude to the government and people of Ethiopia for hosting this historic event in the diplomatic centre of Africa. This honour has been 11 years in the making, since IGF was last hosted on African soil. I would like to express my appreciation to the United Nations Department of Economic and Social Affairs (UNDESA), the IGF Secretariat, ITU and the many other partners, and participants for making the 17th United Nations Internet Governance Forum a reality.

The 17th IGF shone a critical light on the key issues challenging Africa's digital transformation efforts. The forum pinpointed the need for governance of advanced technologies such as AI, local context, universal service funds and community networks, inclusive and safe cyber space, and partnership for digital transformation.

Post-IGF, we must strive for resilient frameworks amid uncertainty, unforeseen situations, and a prevalent digital divide. UNECA reassures its commitment to connect the unconnected and safeguard human rights. We will continue to publish evidence of the digital development agenda that is policy-oriented, data-centric and politically driven.

I am certain that participants left the Forum inspired and even more determined to deliver together for inclusive digital development. We look forward to passing this baton, a baton of an internet that is resilient, open, unfragmented, affordable and inclusive to the next hosts of the IGF.

Foreword

Mr. Belete Molla Getahun (PhD)
Minister of Innovation and Technology
Federal Democratic Republic of Ethiopia

The 17th annual meeting of the IGF was successfully conducted in Addis Ababa from November 28 December 2, 2022. I would like to thank all participants, organizers and partners involved in making the IGF 2022 a success. The level of engagement by the participants during the conference was remarkable, and it was this active engagement that made the IGF 2022 a success. We are also grateful to all guests who travelled to Ethiopia to participate in the IGF 2022, generating meaningful engagement and support in the IGF 2022 sessions.

By hosting the IGF 2022, Ethiopia has shown to the world its commitment to the development of the Internet as well as its dedication for creating a conducive environment for meaningful access to the Internet for all citizens. As a country, we have put great effort into hosting the IGF, and we understand that many countries also strive to host the IGF. In the last three years, Ethiopia has increased its efforts to use digital technologies to ensure inclusive and sustainable development. Ethiopia was chosen to host the IGF 2022 in recognition of its recent efforts for pursuing digitally enabled and supported social and economic developments.

The main theme of the conference was “Resilient Internet for a shared sustainable and common future.” More than 300 sessions were conducted and discussed on various agendas related to the main theme. We believe that important insights that are crucial for common understandings of the shared Internet, as well as ideas that can contribute to a resilient Internet, were identified during the Forum.

Digitalization has the potential to transform many aspects of human life, including in the areas of education, economy and peace. There are foundational elements that are necessary conditions for digital transformation, such as infrastructure, digital payments, skill, and digital platforms. However, to create a real impact there is a need to have a holistic approach. For instance, providing infrastructure is a necessary condition, but not sufficient on its own. To gain actual benefits, skills, right content and above all affordable access are also necessary. With these components, real opportunities for social prosperity through digital transformation are possible. At the same time, cyber security is essential -

online harms and cyber-attacks can also be the cause for not properly using available infrastructures. Such attacks can hamper the use of digital systems and cause further harms by inhibiting equal access and equal opportunities.

The IGF 2022 in Ethiopia, conducted in the aftermath of COVID-19 pandemic was amazingly attended by a large number of participants coming from around the world, government and industry participants, youth and parliamentary representatives, as well as individuals and civil society representatives. 5120 participants from 170 countries participated onsite and online, with record numbers of those being governments and stakeholders from the African region. With this, we know that there were voices able to speak with greater volume at this IGF on crucial issues that particularly affect our continent, related to connectivity, infrastructure, cybersecurity and digital literacy.

The diversity, as well as the number of participants, together with the number of ideas presented and discussed are clear indications of the success of the IGF 2022.

Thank you.

IGF 2022 at a Glance

In 2022, the forum held its 17th annual meeting in a hybrid format, in Addis Ababa and online. Under the overarching theme Resilient Internet for a Shared, Sustainable and Common Future, the meeting featured discussion on some of the most pressing Internet and digital policy issues, from connectivity and human rights, to Internet fragmentation, cybersecurity and new and emerging technologies.

Its thematic structure was closely aligned with the community's interest and the issues proposed to be tackled in the upcoming Global Digital Compact (GDC).

The IGF 2022 Multistakeholder Advisory Group (MAG), with members appointed by the UN Secretary-General from all stakeholder groups, supported the planning of the 17th annual IGF meeting. The IGF Leadership Panel met in person for the first time in Addis Ababa to exchange views on approaches to strengthening the Forum and enhancing its visibility.

.

RESILIENT INTERNET FOR A SHARED, SUSTAINABLE AND COMMON FUTURE

28 NOVEMBER- 2
DECEMBER 2022
ADDIS ABABA, ETHIOPIA

5120
PARTICIPANTS

170
COUNTRIES

293
SESSIONS

PROGRAMME
STRUCTURE

- THEMATIC TRACKS - COMMUNITY SESSIONS
- IGF HIGH-LEVEL LEADERS TRACK
- GLOBAL YOUTH SUMMIT
- PARLIAMENTARY TRACK
- NTERSESSIONAL WORK TRACK

THEMES
ISSUE AREAS

- CONNECTING ALL PEOPLE AND SAFEGUARDING HUMAN RIGHTS
- AVOIDING INTERNET FRAGMENTATION
- GOVERNING DATA AND PROTECTING PRIVACY
- ENABLING SAFETY, SECURITY AND ACCOUNTABILITY
- ADDRESSING ADVANCED TECHNOLOGIES, INCLUDING AI

IGF 2022 Quotes

The meeting opened with remarks from the Prime Minister of Ethiopia, the United Nations Secretary-General and the Acting Executive-Secretary of the United Nations Economic Commission for Africa (ECA), followed by remarks from experts from different stakeholder groups.

"We often hear that the future will be digital, but the future of digital must be human-centred. That ambition is reflected in your theme - building a resilient Internet for a shared sustainable and common future. It is also the motivation behind my proposed Global Digital Compact on an open, free, inclusive and secure digital future for all."

Mr. António Guterres, United Nations Secretary-General

"Ethiopia is hugely proud to be the host of the 17th edition of the IGF and the third country on African soil since its maiden launch in 2006… This global multistakeholder platform is a historic event for the host nation of over 120 million people, most of whom are young men and women. Ethiopia as a country has demonstrated its commitment to the same goal by developing its own national digital strategy known as Digital Ethiopia 2025 with a motto digital strategy for inclusive prosperity of Ethiopia''

H.E. Mr. Abiy Ahmed, Prime Minister of the Federal Democratic Republic of Ethiopia

"IGF presents a vital opportunity to discuss accelerators for digital transformation and bridging the digital divide through coordinated action and advocacy. In this regard, we must not forget where this forum is taking place. On the African continent, only one in three people has access to the Internet.''

Mr. Antonio Pedro, Acting Executive Secretary, UN Economic Commission for Africa

''Digital technology is a uniquely powerful enabler. Through digital, we can put the life-changing power of education in the hands of all. We can empower the socially and economically disadvantaged. We can ensure that everyone everywhere has access to healthcare. We can turbo charge human knowledge through collaboration in science, engineering, agriculture, and more.''

Ms. Doreen Bogdan-Martin, Secretary-General-elect, International Telecommunications Union

''We recognize that the Internet and digital technologies are the backbone of digital transformation, a topic that His Excellency the Prime Minister emphasized in his opening remarks. But there is no successful digital transformation if it is not anchored in human rights and other key humanistic values...''

Mr. Tawfik Jelassi, Assistant Director-General for Communication and Information, UNESCO

''The future of a secure, robust, and open Internet is inherently a matter of youth who are the forefront developing its core. We are poised to build mutual understanding between stakeholders in the Internet community. In order to make better policies towards building an Internet for all, young people are ready to get involved.''

Ms. Lily Edinam Botsyoe, Ghana Youth IGF

''The challenge before us is to realize the demonstrated and potential benefits of the Internet now that we know that it can be both a productive environment and one in which material harms can be perpetrated. The world is looking at the IGF, its Leadership Panel, its MAG and the IGF participants, to throw light in dark corners and highlight paths to successful use of the Internet for all of the worlds and the countries in which they live.''

Mr. Vint Cerf, Chair, IGF Leadership Panel

''It's also great to see its multistakeholder character come alive in all of the sessions, all of the different discussions that take place, in the deliberations of the MAG, the Multi-stakeholder Advisory Group, and in the newly constituted IGF Leadership Panel which Vint Cerf and Maria Ressa are Co-Chairing. A lot has been achieved in 17 years. A lot more needs to be done.''

Mr. Amandeep Singh Ghill, UN Envoy on Technology

''You might think that you go online and everything works. And I can bet you probably speak English. 80% of the content on the Internet is actually in English. Less than 20% of all people in the world speaks English. Our next big generational change of the Internet is to make Internet accessible regardless of which language, which culture you come from, which key word you want to use that is accessible to the Internet. That's a big thing.''

Mr. Göran Marby, CEO and President, ICANN

''International organisations should set the example and include proactive measures to allow historically marginalized groups to have their voices heard and meaningfully considered. This includes intergovernmental and standard setting and technical organisations, development agencies and banks among several others which should also build transparency and accountability mechanisms into their own processes and pressure national Governments and global tech companies in the same direction. The IGF is a central piece of the Internet governance ecosystem and key to improve the coordination in global Internet governance and digital cooperation.''

Ms. Jamila Venturini, Co-Executive Director, Derechos Digitalis

IGF 2022 Highlights

Hybrid IGF

The 17th IGF was held as a fully hybrid meeting, with participants joining onsite, in Addis Ababa, and online. With the overall objective of making participation in the meeting meaningful and inclusive for all attendees, the hybrid format included several features:

- Participating platform through which the meeting discussions were facilitated in an as-equal-as-possible manner for all participants, regardless if they connect to it from the venue or any other part of the world. The platform also meant that speakers/moderators/rapporteurs were able to participate and contribute either online or onsite.
- 3D Venue was created as an equivalent to the onsite venue. As onsite participants, the online participants also had an opportunity to enter the meeting rooms and connect to the participating platform.
- GF Village booths, hosted by over 60 organisations at the venue, had their online equivalents.
- Remote hubs facilitated the participation of those unable to travel.
- Bilateral meetings could also be organised with online participation.
- Networking opportunities also allowed for online participation through digital networking platforms and online connection to physically hosted events.
- New website and mobile app were also made available to support easier navigation of the IGF 2022 content.

Involvement of UN Agencies

Following last year's practice, the Forum saw over 45 entities from the UN system involved in the 17th IGF as organisers or speakers in sessions. A high-level UN Open Forum dedicated to how the United Nations system can support digital transformation and the Global Digital Compact engaged senior officials of 11 UN agencies and entities, who discussed the tremendous potential of digital technologies to boost sustainable development and called for more cooperation across the system.

Focus on Youth

To effectively engage youth, a dedicated IGF 2022 Youth Track was designed and implemented throughout the year. In cooperation, the Host Country, IGF Secretariat, all Youth IGF coordinators, as well as international youth-focused organisations, designed the track and delivered four capacity development workshops hosted in conjunction with regional IGFs, namely EuroDIG, African IGF, APrIGF and LACIGF, as well as a IGF 2022 Global Youth Summit at the 17th IGF in Addis Ababa. The track focused on unpacking various digital transformation policy aspects and engaged over seven thousand young people.

Thematic Approach and GDC focus

The IGF 2022 themes were aligned closely with the priorities outlined in the Secretary-General's proposed Global Digital Compact, as well as with community inputs received through a traditional public call. The programme's structure aims to encourage focused discussion that delves more deeply into specific issue areas thereby potentially leading to more focused outcomes.

The five thematic areas are associated with corresponding narratives, policy questions and issues, to help orient session organisers when submitting session proposals.

Capacity Development

Throughout 2022, the IGF Secretariat has been engaged in a series of capacity development activities, including organising workshops, providing grants to NRIs, supporting youth engagement and schools of Internet governance, providing travel support for IGF 2022 participants and remote hubs.

Specifically, capacity development included several activities:

- Workshops organised in conjunction with the NRIs, to foster cooperation and develop capacity. Among these, some specifically were organised as part of the youth and parliamentary tracks.
- Training sessions for IGF 2022 session organisers and participants, focused broadly on explaining mechanisms of hybrid participation.
- Newcomers session for orienting the first time IGF participants.

The Secretariat also supported capacity development activities delivered by different stakeholders in the IGF ecosystem, such as training for African parliamentarians of the African Union and GIZ or women's inclusion in IG delivered by several African women-focused organisations.

Leadership Panel and Follow-up to the Secretary-General's Our Common Agenda

Continuous efforts are invested to improve the IGF, in line with its mandate. This also includes responding to the UN Secretary-General's Roadmap for Digital Cooperation and Our Common Agenda. The Secretary-General appointed the Leadership Panel, as a strategic high-level multistakeholder body. The 15-member Panel met in person for the first time at the 17th annual IGF meeting. Members also met with many other organisations and engaged with the community through an open town hall to gather inputs on needs and expectations which could orient the panel's work in 2023.

An Expert Group Meeting was organised by DESA during 2022 to contribute to advancing digital cooperation and strengthening and improving the IGF as a space for global multistakeholder discussion on Internet policy issues. Its report and recommendations contribute to the work of the Leadership Panel and the MAG.

The IGF continues to plan its contribution modality to the Secretary-General's proposed Global Digital Compact on norms, principles and values. The IGF 2022 Messages, reflecting key takeaways from the forum's discussions, are expected to constitute input into the GDC development process.

In parallel with structural changes, efforts are invested in advancing long-term sustainability of the forum. In this regard, the next host countries are being explored, new partnerships and cooperation mechanisms.

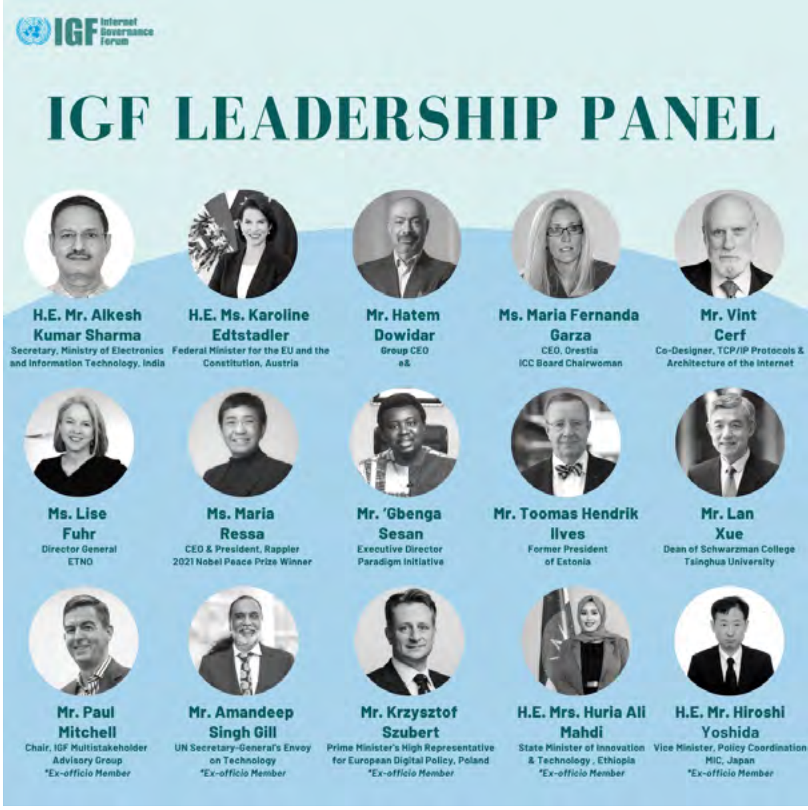
IGF 2023 Multistakeholder Advisory Group

Following the public call for nominations, the Secretary-General appointed eleven new members to its IGF Multistakeholder Advisory Group, to plan the 18th annual IGF meeting in 2023.

The Chair of the MAG was reappointed. The list of MAG 2023 members and its Chair is available at the IGF website.

Communications

Daily bulletins were issued on each IGF day to provide key highlights from the current day and announce the most important activities for the next day. All sessions were streamed and transcribed. The high-level and main sessions were also interpreted to six UN languages


IGF Internet Governance Forum
IGF LEADERSHIP PANEL
H.E. Mr. Alkesh Kumar Sharma
Secretary, Ministry of Electronics and Information Technology, India
H.E. Ms. Karoline Edtstadler
Federal Minister for the EU and the Constitution, Austria
Mr. Hatem Dowidar
Group CEO e&
Ms. Maria Fernanda Garza
CEO, Orestia ICC Board Chairwoman
Mr. Vint Cerf
Co-Designer, TCP/IP Protocols & Architecture of the Internet
Ms. Lise Fuhr
Director General ETNO
Ms. Maria Ressa
CEO & President, Rappler 2021 Nobel Peace Prize Winner
Mr. 'Gbenga Sesan
Executive Director Paradigm Initiative
Mr. Toomas Hendrik Ilves
Former President of Estonia
Mr. Lan Xue
Dean of Schwarzman College Tsinghua University
Mr. Paul Mitchell
Chair, IGF Multistakeholder Advisory Group *Ex-officio Member
Mr. Amandeep Singh Gill
UN Secretary-General's Envoy on Technology *Ex-officio Member
Mr. Krzysztof Szubert
Prime Minister's High Representative for European Digital Policy, Poland *Ex-officio Member
H.E. Mrs. Huria Ali Mahdi
State Minister of Innovation & Technology , Ethiopia *Ex-officio Member
H.E. Mr. Hiroshi Yoshida
Vice Minister, Policy Coordination MIC, Japan *Ex-officio Member

The 17th Annual Internet Governance Forum
IGF ETH
OPIA

IGF ETHIOPIA ኢትዮጵያ
The 17th Internet Governance Forum
WIFI: IGF2022
PASSWORD: IGFUneca@2022
IGF ETHIOPIA 2022 ኢትዮጵያ
The 17th Annual Internet Governance Forum
United Nations
IGF Internet Governance Forum
MInT

IGF 2022 Themes

The headline of this year's Forum is Resilient Internet for a Shared Sustainable and Common Future. This title symbolises the need for an open, strong, safe and reliable Internet that can truly foster a sustainable digital future based on common values and principles.

It was associated with five subsidiary themes which were related to issues for consideration within the Global Digital Compact. All IGF sessions, including the community-led sessions were built around the five IGF 2022 themes:

- Connecting All People and Safeguarding Human Rights
- Avoiding Internet Fragmentation
- Governing Data and Protecting Privacy
- Enabling Safety, Security and Accountability
- Addressing Advanced Technologies, including Artificial Intelligence (AI)

Each theme is associated with a corresponding narrative. These helped inform over 420 session proposals received and reviewed for final adoption into the IGF 2022 programme.

The final output of the rich Forum's discussions feeds into **Addis Ababa IGF Message**s.

Addis Ababa IGF Messages

The Addis Ababa IGF Messages provide an overview of digital policy issues discussed at the Forum for all stakeholders and particularly for decision-makers. They are derived from discussions at close to 300 sessions held during IGF 2022, including main sessions, workshops, open forums and other activities. Session organisers were invited to identify significant takeaways from their sessions for consideration as inputs to these messages. A set of draft messages, curated by the IGF Secretariat, was published for community's review. The final IGF 2022 Messages are published as part of the annual meeting's outputs and annexed to this Report.

IGF 2022
High-Level Leaders Track

Co-organised by the Host Country and UN DESA/IGF Secretariat, the IGF 2022 High-Level Leaders' Track engaged experts and leaders from all stakeholder and regional groups into discussions on a series of critical Internet governance issues. The track saw participation of seventeen ministers and vice-ministers. Overall, sixty-three high level experts took part in the track.

The sessions of the high-level leaders' track addressed the following topics:

- Universal, affordable and meaningful connectivity
- Digital Rights
- Digital trust and security

These sessions, interpreted into six official UN languages and live broadcasted, set foundation for the subsequent IGF high-level sessions given the number of identified issues which require multistakeholder effort to resolve, but also potentials to tap into for achieving sustainability with support of digital. The main takeaways from the high-level leaders' are integrated in the Addis Ababa IGF Messages.

performed now for 14 years.
A second example of the sustainable cooperation are digital
prescriptions
IGF ETHIOPIA 2022 ኢትዮጵያ
The 17th Annual Internet Governance Forum
IGF ETHIOPIA 2022 ኢትዮጵያ
United Nations
IGF Internet Governance Forum

IGF 2022 Youth Track

The IGF 2022 Youth Track was composed of four capacity development workshops and a Global Youth Summit, all focused on unpacking the theme of digital transformation. It was designed and co-organized by the Youth IGF coordinators, IGF 2022 Host Country, IGF Secretariat and several youth-oriented international organisations.

Four capacity development workshops were hosted in conjunction with regional IGFs (EuroDIG, African IGF, Asia Pacific IGF and Youth Latin American IGF), exploring aspects of digital transformation such as policy challenges, education, AI and cybersecurity.

These workshops fed into the IGF 2022 Global Youth Summit, which sought to facilitate dialogue between young people and senior stakeholders. Youth from all five regions of the world engaged in a dialogue with senior experts from different backgrounds and countries. Messages from the IGF 2022 Youth Summit are presented further.

Messages from the Youth

Messages emerged from the IGF 2022 Global Youth Summit hosted in Addis Ababa on 28 November 2023.

Opportunities for social prosperity digital transformation provides

- Youth has always been an important driver of digitization, not only as technical innovators, but also through digital cooperation and policy development. In a multi-stakeholder environment of shared responsibilities, institutionalization is key to develop and maintain good practices, networks, and frameworks.

- Creative ways to problem-solving regarding the digital transformation is a responsibility that youth should embrace as their own, as current discussions have an impact on rules, policies and frameworks but also on opportunities for society at large.

- Youth has the opportunity to build on former developments, but also critically check if the frameworks and structures still apply in ever-changing digital environments. Youth therefore has to be recognised as a serious stakeholder in policy and regulatory development.

- Sustainable digital transformation requires a focus on the Internet as a public space that does not exclude marginalized communities (such as gender-diverse people, ethnic and race minorities, women), users in remote areas, and other underserved and underrepresented communities. Investments in meaningful access and accessibility shall benefit all users and communities, going beyond a focus on mere economic growth.

- Tools and processes for education and participation have to be accessible in order for youth to be a positive force in a sustainable digital transformation.

Challenges preventing from fully benefiting from digital transformation opportunities

- Modern technology is already present in our lives, but policy frameworks need to be adjusted to current risks. Higher levels of technical connectivity lead to increased vulnerability of digital infrastructures, data and services.

- Calculation of risk in cybersecurity looks at assets, vulnerabilities and threats. A stable governance structure to mitigate risks is holistic and requires the involvement of governments and regulators, the private sector, and the end-users themselves.

- Socio-economic obstacles to participation in digital transformation have to be recognised and addressed locally and regionally. High levels of youth unemployment, lack of Internet access, and inaccessible digital education hamper opportunities and especially exclude marginalized communities.

Toward a better digital future!

- Key points in the context of digital sustainability include social inclusivity of digital solutions, greener tech to reduce negative impacts on the environment, and open policy processes.

- Rebound effects, in which technology is made more sustainable, but resources use increases due to increased use of green tools, need to be avoided.

- Part of being digital natives means youth understand the impact of digital tech, and the inequalities present in digital connectivity and access. Thus, youth can act as both a driving force and a warning sign in tackling issues from green tect to privacy and human rights.

IGF 2022 Intersessional Work

In between annual meeting of the Forum, the IGF community works on a range of issues through three main types of intersessional fora – Policy Networks (PNs), Best Practice Forums (BPFs) and Dynamic Coalitions (DCs).

Policy Networks

Policy Networks, first established in 2021, are dedicated to identifying status quo and current issues including the policy gaps, existing capacity and conditions, local specificities, good and bad practices and possible ways forward through actionable activities led by identified implementation parties. Two PNs undertook work during 2022 and reported to the Forum in Addis Ababa.

- The Policy Network on Meaningful Access considered reasons why achieving meaningful and universal Internet access remains So challenging and ways in which the challenges identified might be addressed.

- The Policy Network on Internet Fragmentation explored different understandings of the concept of Internet fragmentation including technical, policy, legal and regulatory measures and actions that pose a risk to the open, interconnected and interoperable Internet.

Best Practice Forums

- The Best Practice Forums (BPFs) provide open, bottom-up and collective platforms for members of the IGF community to exchange experience – and to collect existing and emerging good practice – in addressing Internet policy issues. BPF outputs seek to contribute to an understanding of global good practice, and serve as a resource to inform policy discussions, standards development, business decisions, and understanding, awareness, and discussion. Two BPFs undertook work during 2022 and reported to the Forum in Addis Ababa.

- The Best Practice Forum on Cybersecurity continued its work to identify cybersecurity initiatives that bring to the fore voices of those most affected by cybersecurity events and to analyse the complex interplay between norms and cybercrime legislation.

- The Best Practice Forum on Gender and Digital Rights looked at the impact of regulations from a gender justice perspective. It generated conversations with people affected by these regulatory practices and assessed the impacts of intensive regulation on the privay and other experience of women and LGBTQI+ people online.

Dynamic Coalitions

Dynamic Coalitions (DCs) are open, multistakeholder and community-driven groups dedicated to an Internet governance issue or set of issues. They emerged at the first IGF meeting in 2006. There are currently 24 active dynamic coalitions concerned with topics such as Internet rights and principles, innovative approaches to connecting the unconnected, accessibility and disability, and child online safety. The activities of the DCs are coordinated by the Dynamic Coalition Coordination Group (DCCG) with support from the IGF Secretariat.

Twenty DCs held individual sessions at IGF 2022, presenting their work and discussing Internet policy issues within their areas of focus. A DC main session on the theme Our Digital Future: How IGF Dynamic Coalitions Support the Global Digital Compact showcased how DCs can contribute to the development of the IGF into an "IGF+", as suggested in the UN Secretary-General's Roadmap on Digital Cooperation, and to the principles of the Global Digital Compact.

National, Regional and Youth IGF Initiatives

National and Regional IGF Initiatives (NRIs) are organic and independent multistakeholder networks that discuss issues pertaining to Internet Governance from the perspective of their respective communities, while acting in accordance with the main principles of the global IGF. 155 NRIs are currently recognised by the IGF Secretariat.

At the 17th IGF in Ethiopia, over 100 NRIs co-organized seven sessions, including five thematic collaborative sessions, a main session and a coordination session. The main session focused on safeguarding and strengthening the core principles of a trusted Internet, while the coordination session emphasized the need for more sustainability in stakeholder engagement, cooperation and funding for the NRIs in order to build a more stable IG(F) ecosystem. The collaborative sessions unpacked local contexts and perspectives concerning access, data governance, child online safety, the forthcoming twenty year review of WSIS and the role of the Internet in democracy. More information about the NRIs sessions is available at the IGF website.

Other Sessions Accommodated in the IGF 2022 Programme

In addition to the tracks described above, the IGF programme included a range of other types of sessions. These included:

- Pre-events – sessions hosted on the day before the IGF official programme began, known as Day Zero (28 November).
- Open Forums – sessions dealing with Internet governance issues that were organised by governments, treaty-based international organisations, and global organisations with international scope and presence, with operations across regions.
- Town Halls – presentation and discussion sessions organised by entities dealing with Internet governance issues of international scope.
- Lightning Talks – brief, to-the-point, prepared presentations on specific Internet governance issues.
- Networking Sessions – including gatherings of stakeholders interested in specific or related issues, icebreaker sessions, social gatherings, and gatherings of people and organisations from particular regions, stakeholder groups, or areas of activity.
- Launches and Awards – sessions to present and discuss Internet governance-related academic and/or research initiatives or outputs such as research or think tank reports and book launches.

Best Practice Forum on Gender and Access

The IGF Best Practice Forums (BPFs) provide a platform for experts and stakeholders to collect community experiences and contribute to an understanding of global good practices. They also serve as a resource to inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse. Since its beginning in 2015, the BPF on Gender and Access has focused on the distinct aspects of women's meaningful access to the Internet. In 2021, the Forum was renamed the BPF on Gender and Digital Rights to encompass the broader protection of human rights online.

This year, the BPF explored the impact of regulations from a gender justice perspective. It assessed how regulations may undermine gender-diverse rights of women and LGBTQI+ people online – which might represent changes in ensuring freedom of expression, preservation of online identities, safety and civic spaces, and criminalisation of activities of historically marginalised groups. The goal is to raise awareness of how some regulations are pervasive and directly affect the wellbeing of said communities.

The BPF also aims to bring an intersectional perspective to the IGF agenda of urgent and necessary transformations for a gender-sensitive ecosystem, adding value to the overall democratic development. These efforts are associated with IGF 2022's Theme 1: "Connecting All People and Safeguarding Human Rights"; and on a smaller scale, to Theme 3: "Governing Data and Protecting Privacy", and Theme 4: "Enabling Safety, Security and Accountability". The policy focus was split into three areas, analysing the impact of regulation on:

- Privacy and Surveillance / Reproductive Privacy
- Freedom of Expression / Gendered Disinformation
- Freedom of Association and Religion

Throughout the year, the BPF Gender aimed at establishing outreach with like-minded experts and professionals, in order to set up learning/sharing sessions with the BPF community. Its members have also collected resources and analysed selected regulatory cases, highlighting their original goal and unintended impacts. The final product of 2022 BPF Gender work is set to be an informative report, showcasing the community discussions and cases' assessments.

Best Practice Forum on Cybersecurity

To enrich the potential for Internet Governance Forum (IGF) outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities.

Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics. In the last four years, the BPF on Cybersecurity started investigating the concept of culture, norms and values in cybersecurity.

In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analysing international and cross-stakeholder cybersecurity initiatives for commonalities. In

2020, the BPF took a wider approach and In explored what could be learned from norms processes in global governance in areas completely different than cybersecurity, and continued and further advanced the analysis of cyber norms agreements. Last year's BPF Cybersecurity investigated more deeply the drivers behind, and disablers of, cyber norms. A second work stream tested norms concepts against historical Internet events to understand how specific norms have or would have been effective at mitigating adverse cybersecurity events.

In 2022, the BPF Cybersecurity added new agreements to its assessment of normative cybersecurity agreements, explored the value of storybanking cybersecurity incidents, and produced an ad hoc mythbusting paper on the difference between cybercrime and cybersecurity from a policy perspective.

Work Stream I - Mapping International Cybersecurity Norms Agreements

The BPF added two new agreements - the Copenhagen Pledge on Tech for Democracy and A Declaration for the Future of the Internet - to its database, which now includes 38 international agreements between or among stakeholders, including voluntary, nonbinding cybersecurity norms. The analysis showed that "human rights" and "general cooperation" are the most commonly seen norms elements across the 38 agreements. Norms that relate to express restraint on what either government actors, private sector actors, or other actors will not do occur the least frequently, but have become more prominent over time. Interestingly, the new norms agreements included in the 2022 analysis have overlapping qualities as well as norms elements that set them apart. They are both led independently by foreign ministries and have emphasis on protecting democracy and on working to building democratic coalitions, of governments in one case and of broader multistakeholder actors in the other. There's a focus in both agreements on disinformation, misinformation, and influence operations related to the security of democracies. Lastly, the overall analysis of the 38 agreements showed a growing interest in combating ransomware as an action item.

Work Stream II - Exploring Historic Cybersecurity Events

Building on its work in 2021 that revealed a gap in understanding the roles of actors and stakeholders in mitigating cybersecurity incidents, the work stream 2 explored how storytelling can be an effective tool to listen and learn from the experiences of first responders and those most affected by a cybersecurity event. These insights are valuable input for those involved in cyber norm development. At the end of the day, cybersecurity norms must make a difference in the lived experiences of these people, past, present and future. The workstream 2 developed a framework for collecting stories from networks of first responders.

Work Stream III - Outreach and Engagement

Under its Outreach and Engagement work stream the BPF organised an outreach session during RightsCon 2022 and contributed relevant findings of its work on cybersecurity norms with the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 during the OEWG Chair's Informal Dialogue (BPF input) and Informal Inter-Sessional Meetings (BPF input).

Ad hoc paper - Mythbusting: Cybercrime versus Cybersecurity

The BPF created an ad hoc work stream to develop a paper to help stakeholders understand the key policy differences between cybersecurity and cybercrime such that their advocacy strategies can better align with a human rights centric approach to internet governance. In general the suggested strategy is to remove the policy decision making out of the criminal frameworks so as to balance the implications on human rights, while promoting cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and can be compatible with human rights. The paper is available online.

Policy Network on Meaningful Access

The Policy Network on Meaningful Access (PNMA) was launched in June 2021 with the goal of formulating impact-driven, concrete, actionable policy recommendations on how to achieve meaningful and universal Internet access, in alignment with the Secretary-General's Roadmap for Digital Cooperation and the Sustainable Development Goals. Its activities are facilitated through a multistakeholder working group of experts (MWG).

The PNMA provides an in-depth look at why achieving meaningful and universal Internet access remains so challenging, in spite of years of efforts by policy makers and other stakeholder groups. This policy network is associated with IGF 2022's Theme 1: "Connecting All People and Safeguarding Human Rights", and focused the year's work plan on:

- Connectivity (infrastructure and business models, analysed within the framework of the Roadmap for Digital Cooperation)
- Digital Inclusion (accessibility and multilingualism), with special attention to local contents in local languages, helping the digital transition of existing experiences
- Capacity Development (technical skills training)

To address gaps in these areas, the PNMA released a call for inputs to gather examples of good cases and practices from the community. Based on the information collected, the PNMA could identify whether policy actions have facilitated or encouraged increased meaningful access. The network has received contributions from academics, non-profit organisations, governments, and the private sector, mostly from the Global South. The intersectional partners ITU, WIPO, and WAN-Ifra have also made contributions. The network's output report features the most relevant practices as evaluated by the MWG. All complete inputs received by the PNMA will be added to a permanent repository of good experiences on meaningful access, to be made available at the PNMA's webpage. It is expected that similar calls will be promoted each year.

Policy Network on Internet Fragmentation

Internet fragmentation is a complex issue. The many views, diverse opinions, different conceptualisations and definitions of what is and what is not internet fragmentation, or what fragmentation - in the context of the UN Secretary General's Our Common Agenda - should be avoided or addressed can hinder an open and inclusive dialogue, and discussions on common guidelines or principles.

The proposal for a Policy Network on Internet Fragmentation (PNIF) was born out of a community initiative launched by a multistakeholder coalition of civil society, business and technical community organizations in 2021 to raise awareness of the technical, policy, legal and regulatory measures and actions that pose a risk to the open, interconnected and interoperable Internet. The IGF Multistakeholder Advisory Group (MAG) confirmed Internet fragmentation as topic for an IGF intersessional activity that aims to offer a systematic and comprehensive framework, complemented by case studies, to define Internet fragmentation, its causes, and its potential effects and it aims to establish recommendations or codes of conduct that prevent fragmentation. The PNIF proposal envisaged a two-year work plan with focus in its initial year on establishing a systematic and comprehensive framework to define Internet fragmentation, its intended and unintended causes, and its potential effects.

Towards a Framework for Discussing Internet Fragmentation

The PNIF webinars and discussions confirmed the diversity of opinions, and an attempt to deduct a common definition of internet fragmentation via a survey launched earlier in the year didn't prove successful. Through the discussions, however, emerged elements of a framework that could serve to guide and orient future discussions.

The draft framework for discussing internet fragmentation constructed by the PNIF was shared with the community ahead of and discussed during a PNIF session at the IGF annual meeting in Addis Ababa. The aim is to have a refined and more mature framework ready for a second phase of the PNIF, focused on identifying potential causes of fragmentation and defining solutions and policy approaches to avoid fragmentation.

A Framework for Discussing Internet Fragmentation

The overall goal of the framework is to serve as a general guiding and orienting tool for continuing the dialogue about fragmentation and bringing in more people and stakeholders. The framework should allow a more holistic and inclusive debate, and at the same time, create space for focused discussion and work towards concrete solutions, policy approaches and guidelines.

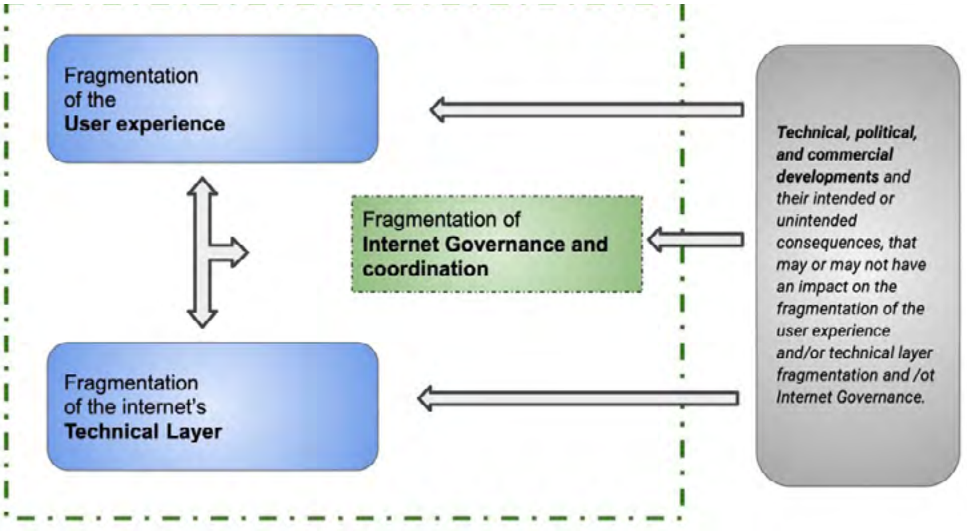
The Framework that emerged from the PNIF discussions conceptualises three key dimensions of fragmentation:

- *fragmentation of the user experience,*
- *fragmentation of the Internet's technical layer, and*
- *fragmentation of Internet Governance & coordination.*

The Framework indicates that **technical, political and commercial developments** and their intended or unintended consequences may or may not have an impact on fragmentation.

The Framework captures potential **relationships and overlap** between the dimensions, between technical fragmentation, user experience fragmentation, as well as governance fragmentation.

The Human rights framework and the need to maintain a **free flow of data** could be used to evaluate measures that impact the user experience and assess if the measures enhance the user experience or have a negative impact and as such should be avoided. T**he interoperability of the global internet infrastructure** is proposed as reference framework to assess technical fragmentation. The internet governance dimension aims to capture the commitment to the **Multistakeholder management** of the technical layer of the internet and the existence or lack of a **global framework** across multilateral and multistakeholder venues, governments and stakeholders **to address global internet policy issues** from a human rights and free flow of data perspective.


Fragmentation of the User experience
Fragmentation of Internet Governance and coordination
Fragmentation of the internet's Technical Layer
Technical, political, and commercial developments and their intended or unintended consequences, that may or may not have an impact on the fragmentation of the user experience and/or technical layer fragmentation and /ot Internet Governance.

In a next phase, it is the PNIF's intention to populate the framework with concrete examples and facilitate focused dialogues on policy approaches and explore guidelines to avoid internet fragmentation.

NRIs Discussion Priorities in 2022

In 2022, 95 NRIs hosted their annual meetings. This is an increase of 6 meetings compared to last year.

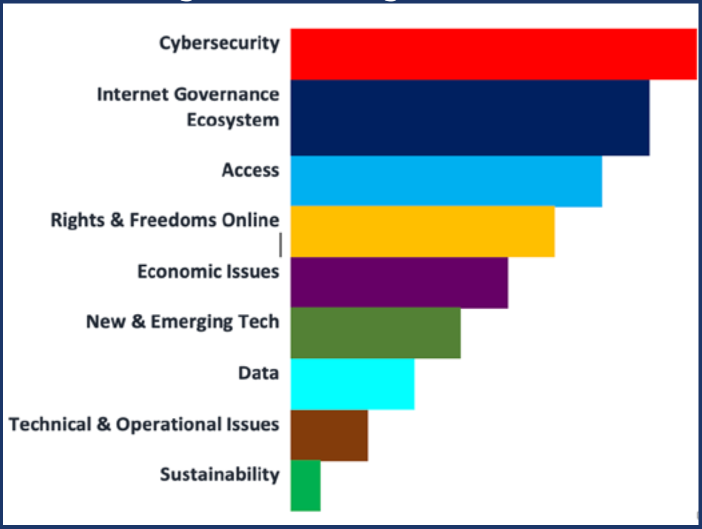
It is an established procedure that the NRIs annual programmes are developed in a bottom-up manner through public calls for inputs issued to all stakeholders of their targeted communities. Usually, issues received are clustered within thematic discussion areas, subject to further consideration by the NRIs multistakeholder organising committees. In order to understand global Internet governance issues' priorities, the IGF Secretariat analyses digital policy discussion areas through agendas of the NRIs annual meetings hosted during the mapped time period. Below is an overview of the 2022 discussion areas gathered across 95 NRIs annual meetings for the 2022 IGF cycle.

Internet governance discussion priorities

Comparing the substantive priorities to 2021, it is evident that the COVID-19 pandemic's impact on the shaping of digital agendas is on the decline. Unlike last year, when the discussions focused on access and connectivity, this year the narratives continued the trend from the pre-pandemic times prioritizing safety and security issues. However, it is important to recognize that the majority of the issues discussed under the thematic clusters are crosscutting and discussed in correlation with each other, depending on the context.

A more in-depth review of the particular discussion areas shows that cybersecurity areas focused on general issues countries in regions face combined with existing cybersecurity agreements and policies, to more specific ones which focus on cybercrime, protection of critical Internet infrastructure and vulnerable groups such as women and girls, young people and children.

Frameworks and procedures for discussion and deciding on Internet governance issues were central to close to half of the NRIs discussions that took place this year. Communities around the world looked into the state of affairs of their current Internet governance ecosystems, with many specifically focusing on the need for regulation of digital space, application of the multistakeholder model and overall opportunities the IGF spaces bring. The concept of cooperation and Global Digital Compact was also present on some of the NRIs agendas.



Looking into specific issues discussed under the access thematic cluster, many NRIs prioritized people's digital inclusion over technical layers of connectivity. In addition to generally wording the session panels as digital inclusion, many NRIs specifically oriented their discussions toward the inclusion of all users through the facilitation of access points with public libraries or the deployment of community networks. Some specifically discussed the inclusion of women and girls, migrants, and people with disabilities. Developing capacity and skills also featured prominently on the NRIs agendas.

Rights and freedoms continued to be highly prioritized by many NRIs. In addition, this area is cross-cutting other thematic clusters. More specifically, around 1/3 of NRIs 2022 discussions focused on discussing digital identity concepts, interpretation of digital rights and especially on combating misinformation and disinformation online. The role of social media was also discussed in the context of respect for human rights.

Unlike last year, topics related to the economy were much better represented on the NRIs agendas. Most of the discussions related to platform economy regulation, job market opportunities, consumer protection and the overall status of the digital economy at local levels.

Issues related to new and emerging technologies were also represented in the NRIs 2022 agendas. The most represented issues include those related to the development of concepts of digital transformation, regulation of emerging tech and governance of AI-based tools and services.

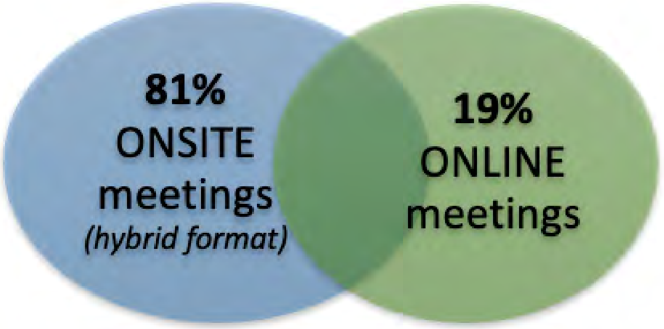
Discussions around data were cross-cutting many of the other analysed areas. However, some specific discussion subjects related to big data, data innovation and governance, to data privacy and overall data protection.

Less represented themes with unique session discussions related to technical and operational issues, but also sustainability. Unlike during the COVID-19 pandemic period, when environment and sustainability were among new emerging discussion areas, this year shows stagnation if not a decline in their representation. Nevertheless, the quality of the represented sessions was profound, brainstorming ways in which digitalisation can support sustainability, to the ways digital impacts and potentially strengthens the environment.

On a more technical side of the Internet, discussions touched upon routing security, DNS abuse and conditions necessary for universal acceptance.

Meeting Formats

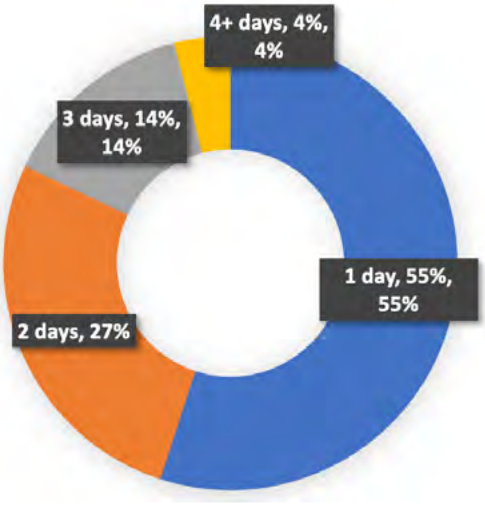
Last year, almost half of the NRIs meetings were hosted online due to the still present COVID-19 pandemic. However, this year saw a great increase in the number of meetings being hosted face-to-face with a meaningful channel for online participation, as well. Out of 95 NRIs meetings hosted last year, 77 were hosted onsite with an online participation component (hybrid format), while 18 were hosted online.



The majority of the NRIs annual meetings were hosted over 1 day. 26 NRIs meetings were hosted over 3 days, 13 over 3 days and 4 were hosted over five days. The latter were either hosted during consecutive days, or their components were spread throughout the year such as the case with Canada IGF or Guatemala IGF. However, this year illustrated a growing tendency for the NRIs to run activities intersessionally in between two annual IGF meetings. Over 24% of the NRIs which hosted their meetings in 2022 informed about the intersessional activities. These took the forms of schools on Internet governance and hackathons, dedicated capacity development programmes for children, youth and women.

- Growing tendency to host intersessional activities –

Schools on Internet governance, hackathons, programmes for inclusion of children, youth, women etc.



Most meetings were hosted in the capitals. However, there were the twelve NRIs meetings hosted outside of the capitals, with an aim to foster inclusion from outside of the capital cities. These are Italy IGF (Ancona), East African IGF (Arusha, Tanzania), Indonesia IGF (Bandung), Sierra Leone IGF (Bo City), India Youth IGF (Hyderabad), Polish IGF and Polish Youth IGF (Lubin), Brazil IGF (Natal), EuroDIG and YOUthDIG (Trieste, Italy), Nigeria IGF and Nigeria Youth IGF (Lagos).

The average participation across all 95 NRIs meetings in 2022, indicates that over 16,500 stakeholders directly participated in the IGF-like discussion processes around the world.

IGF 2022 Parliamentary Track

Building on the past years' experience, the IGF focused on further strengthening its Parliamentary Track, in particular through expanding a set of intersessional activities dedicated to fostering inter-parliamentary dialogue and cooperation on key digital policy issues. With the IGF 2022 meeting scheduled to be held in Ethiopia, the focus was placed on engagement with parliaments and parliamentarians on the African continent. Below is an overview of activities undertaken in 2022.

On 18–19 July 2022, 30 parliamentarians from 20 African countries got together in a dedicated digital policy symposium to discuss challenges and opportunities related to the digital economy and society and explore their role in shaping an inclusive and human-centric digital future. The two-day event was held in the context of the annual meeting of the Africa Internet Governance Forum (AfIGF) and also marked the launch of the African Parliamentary Network on Internet Governance (APNIG). The discussions are summarised in an output document.

During the IGF meeting in Addis, over 80 parliamentarians from more than 35 countries, as well as the European Parliament and the Pan-African Parliament, got together - on site and online - to exchange experiences and interact with other stakeholders on issues related to addressing cyberthreats. Over four very rich and engaging sessions, parliamentarians highlighted the importance of whole-of-government and whole-of-society approaches to strengthening cybersecurity and combating cybercrime, as well as the need to advance effective and efficient regional and international cooperation in these areas.

A strong call was made for parliamentarians to continue and strengthen their engagement with the IGF, take part in national and regional IGF initiatives, and consider the work carried out in these fora as resources to inform their parliamentary discussions and activities.

These and other messages are reflected in an output document which is intended to inform parliamentary action in the years to come.

The IGF Secretariat published a Guide to Key Digital Policy Issues and Related Processes and Organisations: Toolkit for Parliamentarians, intended to:

- Provide MPs with an overview of the IGF ecosystem and its relevance for parliamentary activities.

- Serve as a toolkit to assist MPs navigate several key Internet and digital policy issues (i.e. focus areas) – envisioned to be covered by the GDC and discussed at IGF 2022 – as well as related processes and organisations.

IGF 2022 Parliamentary Track Ouput

Addressing cyberthreats: national, regional and international approaches

We, parliamentarians taking part in the Parliamentary Track at the 17th UN Internet Governance Forum,

*Coming together i*n the context of the 17th United Nations Internet Governance Forum (IGF) and discussing issues relating to national, regional and international approaches – State-led, multilateral, and multistakeholder – to addressing cyberthreats,

Welcoming the continuation and strengthening of the IGF Parliamentary Track, and building on the recommendations of the 2019, 2020 and 2021 editions that national parliaments cooperate and exchange good practices in dealing with digital policy issues,

Acknowledging the role of the United Nations Department of Economic and Social Affairs (UN DESA), the Inter-Parliamentary Union (IPU) and the House of Peoples' Representatives of Ethiopia in co organizing the IGF 2022 Parliamentary Track, as well as the support provided by the IGF Secretariat,

Recalling United Nations General Assembly resolution 74/304 of 9 September 2020 which encourages strengthened cooperation between the United Nations, national parliaments and the Inter-Parliamentary Union,

Taking note of the United Nations Secretary-General's Roadmap for Digital Cooperation and Our Common Agenda report, which emphasize the importance of strengthened multistakeholder cooperation in ensuring online safety and security,

Noting that, as the Internet and digital technologies increasingly shape our economies and societies, they also create vulnerabilities for individuals, public and private entities, critical infrastructures, and much more,

Recalling that "cybersecurity" and "cybercrime" are related but distinct issues, "cybersecurity" being something that needs to be improved and "cybercrime" being something to be prevented,

Noting the importance of international instruments such as the Council of Europe's Convention on Cybercrime (Budapest Convention) to which there are currently 68 State Parties, and of regional instruments such as the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention), and the role that such instruments can play in furthering international and regional cooperation,

Acknowledging that geopolitical concerns are never absent from discussions on cybersecurity, while affirming that all countries share a common interest in enhancing cybersecurity and combatting cybercrime,

Acknowledging also that the cyber landscape is complex and that countries are at different levels of readiness to deal with cyberthreats, *Noting* that cybersecurity and cybercrime issues have cross-organizational and cross-border dimensions, and that tackling them requires:

a. Whole-of-government and whole-of-society approaches involving strong partnerships and coordinated efforts between relevant authorities and agencies, the private sector, the technical community, academia, and civil society,

b. Efficient and effective regional and international cooperation, both intergovernmental, multilateral and multistakeholder,

1. Call upon parliaments, governments and all other stakeholders to work together to develop policy, regulatory and legislative frameworks for enhancing cybersecurity and tackling cybercrime and recommend that such frameworks:

a) Are developed in an open and transparent manner, with the involvement from the onset of all relevant governmental and non-governmental actors;

b) Embed a human-centred security approach and incorporate the principles of rule of law, judicial oversight, proportionality, accountability, and transparency;

c) Provide sufficient funding to ensure that the authorities tasked with the implementation of those frameworks are adequately equipped – in terms of financial, technical, and human resources – to perform their tasks;

d) Clearly define the roles and responsibilities of relevant public and private actors in a manner that allows meaningful and effective collaboration towards a more secure cyberspace;

e) Draw upon internationally agreed technical standards for cybersecurity;

f) Are coherent with existing legislation developed for the analogue world, for example, legislation to combat hate speech or fraud;

2. Also call upon parliaments to ensure a proper balance between measures to enhance cybersecurity and tackle cybercrime, on the one hand, and the protection of internationally recognized human rights and fundamental freedoms, on the other hand, and in particular to:

a) Ensure that cybersecurity frameworks are complemented by strong data protection laws;

b) Encourage effective cooperation between the intelligence services and other government departments, and seek transparency and accountability from intelligence services tasked with cybersecurity;

c) Avoid the use of cybersecurity measures for political purposes, for example to target opposition politicians;

3. Further call upon parliaments to:

a) Engage in regular dialogue with relevant ministries and agencies, ensure that the government is paying appropriate attention to addressing cyberthreats,uthorities to account for progress in enhancing cybersecurity and
b) Consider the most appropriate institutional mechanisms for addressing cyberthreat-related issues in parliaments,

including by clarifying the mandate of existing parliamentary committees or creating dedicated committees;

c) Encourage effective cooperation between public authorities and the private sector in strengthening cybersecurity and the creation of an environment of trust conducive of such cooperation;

d) Examine the potential for digital technologies such as artificial intelligence to be used in the fight against cybercrime, and the appropriate human rights safeguards needed to avoid misuse of such technologies;

4. Call upon parliamentarians to:

a) Contribute to efforts to raise awareness, build capacities and develop a culture of cybersecurity across society;

b) Translate cybersecurity issues into concepts that are accessible to people, help the public to understand what is at stake, and build political will to address cyberthreats;

c) Use every opportunity to encourage members of the public to practice good cyber-hygiene;

d) Focus attention on encouraging women to take up careers in the field of cybersecurity, as well as on combatting cybercrime incidents that have women as targets;

e) Find ways to bring the conversation on cyberthreats into the mainstream political debate, attract media attention and increase pressure for governmental action;

f) Consider organizing special events in parliaments to focus attention on cyberthreats, such as dedicated "cybersecurity days" or a question time with relevant ministries and agencies;

5. Encourage parliaments, considering the **potential of regional and international instruments in fostering harmonization of legal and regulatory frameworks for cybersecurity and cybercrime, as well as strengthening international cooperation, to:**

a) Consider the ratification of existing international instruments such as the Council of Europe's Convention on Cybercrime (Budapest Convention) and regional instruments such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention);

b) Ensure that ratified conventions are reflected in national policies, regulations and legislation, and are properly implemented at national level;

c) Encourage their governments to participate in the negotiation of new instruments on cybercrime at the United Nations level, and in international processes on norms for responsible state behaviour in cyberspace;

d) Also encourage their governments to ensure that their positions in such processes are informed by a multistakeholder dialogue and that any new instruments work in partnership with existing standards on the rule of law and human rights instruments;

6. Call upon international development partners to:

a) Involve parliaments at all stages in initiatives dedicated to supporting the development of policy, regulatory and legislative frameworks for enhancing cybersecurity and tackling cybercrime;

b) Build the capacity of parliamentarians to work on issues related to cybersecurity and cybercrime, as well as on broader digital policy topics, including through training and skills building;

7. Invite parliaments to strengthen dialogue and exchanges of experiences with other parliaments and parliamentary bodies, including sharing information about existing and new legislative initiatives related to cybersecurity and cybercrime at a national and regional level;

8. Call upon parliaments and parliamentarians to:

a) Contribute to the strengthening of national multistakeholder dialogue on policy issues pertaining to the Internet;

b) Continue and strengthen their engagement with the IGF, take part in national and regional IGF initiatives, and consider the work carried out in these forums as resources to inform their parliamentary discussions and activities;

c) Engage in global processes dedicated to strengthening digital cooperation, such as the development of the Global Digital Compact proposed by the United Nations Secretary-General;

9. Acknowledge with appreciation the publication by the IGF Secretariat of the Guide to key digital policy issues and related processes and organizations: Toolkit for parliamentarians, and

a) Encourage parliamentarians to make use of this toolkit to inform, as relevant, their work on digital policy issues;

b) Encourage also the maintenance of the toolkit as a living, evolving document;

10. Call upon the IGF to further institutionalize the Parliamentary Track and to facilitate regular exchanges between parliamentarians and other IGF stakeholders.

IGF
Forum

Annex A: Statistics

Breakdown of Registrations

The 17th annual IGF meeting gathered 5,120 participants out of which 2,520 in Addis Ababa and 2,600 online. The following tables illustrate the breakdown of participants by stakeholder grouping, region, gender and other factors.

By stakeholder (percentage)	
Government	29%
Intergovernmental Organisation	11%
Civil Society	32%
Private Sector	16%
Technical Community	11%
Press/Media	1%

By region (percentage)	
African Group	44%
Asia-Pacific Group	15%
Eastern European Group	4%
Latin American and Caribbean Group (GRULAC)	8%
Western European and Others Group (WEOG)	21%
Intergovernmental Organisation	8%

Compared to IGF 2021, this year's IGF saw an increase in representation of Governments (+10%), intergovernmental organisation (+3%); in representation of stakeholders from Africa (+25%), Asia Pacific (2%); and GRULAC (+2%). The number of stakeholders from Eastern Europe decreased (-28%).

By gender (percentage)	
Female	43%
Male	56%
Other	1%

Newcomers (percentage)	
Newcomers	64%

19% od all participants are below age 19. 2% of all participants are members of parliaments coming from 35 different countries.

Remote Hubs

34 remote hubs from 21 Countries

- Represented 5 regions
- 67% from Africa
- 9% from Latin America and Caribbean
- 9% from Asia Pacific
- 12% from WEOG
- 3% from Eastern Europe

IGF 2022 preparation

- 40 Members of the Multistakeholder Advisory Group (MAG)
- 2 Open Consultation and MAG Meetings
- 38 Virtual MAG meetings
- 4 MAG Working Groups

Sessions

293 sessions at IGF 2021

- 1 Opening session
- 1 Opening Ceremony
- 5 Main Sessions
- 79 Workshops
- 29 Town Halls
- 45 Open Forums
- 10 Launches and Awards
- 31 Lightning Talks
- 11 Networking Sessions
- 20 DC Sessions
- 7 NRI Collaborative Sessions
- 31 Pre-Events (Day 0 Sessions)
- 5 High-level Leaders Track
- 4 Parliamentary Track
- 1 Global Youth Summit
- 2 BPF sessions
- 2 PN sessions
- 1 Closing session
- 1 Open Mic

Media

YouTube

Live stream	10,000+ views
Social media posts	212,500

Over 2,300 media articles were produced on IGF 2022. Major coverage came from the US (39%), followed by Ethiopia (23.4%) and India (15.8%). The press briefing hosted on 29 November resulted in 229 media articles, garnering 14.8 million unique visitors.

Top media coverage included articles featured in AP News, VOA News and UN News. Full media coverage is available at the press page of the IGF website. In terms of the language, the biggest number of press coverage was in English (96,9%).

There were 212,500 social media posts on the IGF 2022 and its themes. This is a significant increase from the 11,000 posts seen last year. Engagement (clicks, shares, likes, etc.) was close to 300,000, significantly higher than the 27,000 recorded for IGF 2021. The cumulative potential reach across all platforms was 3.5 billion, up from 744 million last year.

Most of the social media engagement came from female users (58.8%). The majority of the social media interactions were among stakeholders of age 18 to 34 (+90%).

Close to 250 thousands of users interacted with the meeting's official hashtags #IGF2022 and #ResilientInternet.

The livestream over IGF YouTube channal recorded close to 10,000 views. The users were mostly male (66.1%) between 25 and 44 years old (64%). Over 27% of viewers were up to age 35. Livestream was mostly viewed i Ethiopia (+45%), followed by the US, Russia, Brazil and India

Annex B:
Documentation and Process

Outputs

IGF 2022 outputs, including IGF 2022 messages, session reports, press releases, and IGF participant statements, can be found at: https://www.intgovforum.org/en/content/igf-2022-outputs

Session Reports, Transcripts and Recordings

Reports:	https://www.intgovforum.org/en/igf-2022-reports
Transcripts:	https://www.intgovforum.org/en/igf-2022-transcripts
Recordings:	https://www.youtube.com/user/igf/videos

IGF ETHIOPIA
2022
ኢትዮጵያ
The 17th Annual Internet Governance Forum
United Nations
IGF Internet Governance Forum
Federal Democratic Republic of Ethiopia

Intersessional Work

The community-led intersessional activities that occur throughout the year offer the IGF community the opportunity to work on substantive and concrete longer-term projects in the field of Internet governance:

Best Practice Forums (BPFs):

- Cybersecurity
- Gender and Digital Rights

Policy Networks (PNs):

- Internet Fragmentation (PNIF)
- Meaningful Access (PNMA)

Dynamic Coalitions (DCs):

The Activities of the 24 DCs are coordinated by the Dynamic Coalition Coordination Group (DCCG):

- Accessibility and Disability
- Blockchain Technologies
- Children's Rights in the Digital Environment
- Community Connectivity
- Core Internet Values
- Data and Trust
- Data Driven Health Technologies
- Digital Health
- DNS Issues
- Environment
- Gender and Internet Governance
- Innovative Approaches to Connecting the Unconnected
- Internet and Jobs
- Internet of Things
- Internet Rights & Principles
- Internet Standards, Security and Safety
- Internet Universality Indicators
- Network Neutrality
- Platform Responsibility
- Public Access in Libraries
- Schools of Internet Governance
- Small Island Developing States in the Internet Economy
- Sustainability of Journalism and News Media
- Youth Coalition on Internet Governance

National, Regional and Youth IGF Initiatives (NRIs)

National, Regional and Youth IGF Initiatives National, Regional and Youth IGF Initiatives (NRIs) are organic and independent formations that are discussing issues pertaining to Internet Governance from the perspective of their respective communities, while acting in accordance with the main principles of the global IGF.

The status of NRIs in 2022:

- 155 NRIs recognised in total
- 100+ NRIs represented at IGF 2022
- 14 more countries/regions have established IGF processes since IGF 2022

Below are the sources where to find more information about the NRIs and their work.

About the NRIs

National IGFs

Regional IGFs

Youth IGFs

Preparatory work of the NRIs

IGF 2022 Preparatory Process

The IGF meeting programme is prepared by the MAG and the IGF Secretariat over the course of the year. Key decisions on the programme are taken in the face-to-face

Following a traditional approach, the process was triggered by a public call for inputs which helped identification of the main themes. These were developed by the MAG based on input and contributions submitted by the community. The programme for IGF 2022 was then built around the five main themes which were prioritised through the public call and aligned with the themes of the Global Digital Compact.

Key elements of the preparatory processes included:

- A call to Take Stock of IGF 2021 and Suggest Improvements for IGF 2022 was open until 20 January. The contributions were summarised in a synthesis output document.
- A call for thematic inputs was open until 14 February. The list of received inputs and an analysis are available.
- The MAG identified main themes during its first MAG meeting and open consultations.
- A call for session proposals was open until 10 June, inviting all stakeholders to consider applying for the type(s) of session that best fit their interests.

In addition to the overall collective work, the MAG worked on particular segments of the Forum's preparations to advance the overall process through four working groups:

Working Group on Outreach, Engagement and Communications Strategy (WG-OEC)

Working Group on Hybrid Meetings (WG-Hybrid)

Working Group on IGF Strategy (WG-Strategy)

Working Group on Workshop Process (WG-WSP)

IGF ETHIOPIA 2022 ኢትዮጵያ
The 17th Annual Internet Governance Forum
IGF ETHIOPIA 2022 ኢትዮጵያ
The 17th Annual Internet Governance Forum
United Nations
IGF Internet Governance Forum
IGF ETHIOPIA ኢትዮጵያ

Annex C: IGF 2022 Donors

The IGF project and its Secretariat is funded through donations from various stakeholder groups. While host countries bear the majority of the costs associated with holding the annual IGF meeting, the IGF Secretariat's activities are funded through extra-budgetary contributions paid into a multi-donor Trust Fund administered by the United Nations Department of Economic and Social Affairs (UN DESA).

IGF 2022 was primarily funded by the Host Country – the Government of Ethiopia, as well as the Trust Fund and in-kind support.

In 2022, the following donors supported the IGF:

FORMIN.FINLAND.FI MINISTRY FOR FOREIGN AFFAIRS OF FINLAND	Government of Finland	Internet Society Foundation	The Internet Society (ISOC) Foundation
European Commission	European Commission	giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH	GIZ
ICANN	Internet Corporation for Assigned Names	Department for Culture Media & Sport	Government of the United Kingdom
NRO	Number Resource Organization (NRO)	Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Government of Switzerland
iGFSA Internet Governanc Forum Support Associatic	IGF Support Association	Google	Google
EURid	European Registry for Internet domains (EURid)	cisco	CISCO
Microsoft	Microsoft	Meta	META
AT&T	AT&T		

HIOPIA
ኢትዮጵያ
Governance Forum

IGF ETHIOPIA
2022
ኢትዮጵያ
RESERVED

INTERNET GOVERNANCE FORUM 2022

Addis Ababa IGF Messages

This document is a summary of points raised during the 17th annual Internet Governance Forum meeting hosted in Addis Ababa on 28 November - 2 December 2022.

The views and opinions expressed herein 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.

Discussions at the 2022 IGF focused on five key themes that have been identified for the Global Digital Compact (GDC) which was proposed in the United Nations Secretary-General's 2021 report on the 75th anniversary of the United Nations, Our Common Agenda, and will be considered by the UN General Assembly in 2023. This will form part of the development of the Summit of the Future which is scheduled for 2024.

The themes considered by the IGF were:

- *Connecting All People and Safeguarding Human Rights*
- *Avoiding Internet Fragmentation*
- *Governing Data and Protecting Privacy*
- *Enabling Safety, Security and Accountability*
- *Addressing Advanced Technologies including Artificial Intelligence (AI)*

The IGF's multistakeholder community expressed support for the Secretary-General's proposal for a Global Digital Compact. The messages set out in this document represent contributions from the IGF towards development of the Compact. IGF Dynamic Coalitions which are already addressing specific challenges and opportunities that are relevant to the thematic areas proposed for the GDC have also expressed their intention to contribute to the UN's preparatory and implementation phases of the GDC process.

Connecting All People and Safeguarding Human Rights

Theme

The UN Secretary-General's proposed Global Digital Compact (GDC) has as its first principle to "Connect all people to the Internet, including all schools." This recognizes that Internet connectivity and access have become prerequisites for ensuring the livelihoods, safety and education of people all around the world – and that Internet in schools provides crucial points of access, makes informational resources available to all students, and builds digital literacy from the earliest stages of life. Yet 2.7 billion people remain unconnected today, with those in least developed countries and rural communities most disadvantaged.

Meaningful access reaches beyond mere connectivity and is inextricable from the safeguarding of human rights online. Access that contributes to the wellbeing of societies must have human rights at its centre. This includes, among many others, the ability for users to express themselves freely, for the unfettered exercise of democratic and political participation, for persons of all backgrounds to experience the Internet without fear of harassment or discrimination, and for children to enjoy the same rights and protections online as they do offline. The Internet is both an enabler of rights and must seamlessly incorporate established human rights, as we increase our digital dependence for routine functions, and as boundaries between life "online" and "offline" are becoming less significant.

Messages

Digital Divides

- **The digital divides between different countries and regions remain powerful factors affecting national and international development**, including progress towards the Sustainable Development Goals (SDGs). Of particular concern are least developed countries and small island developing states (SIDS). Digital divides are much more than connectivity divides. Meaningful access includes issues of accessibility, affordability, content, services, digital literacy and other capabilities as well as connectivity. Affordability is a particular problem for many people, especially in the Global South.

- **The COVID-19 pandemic demonstrated the Internet's role in enabling individual and economic resilience, but also illustrated the extent to which those who lack connectivity or meaningful access are disadvantaged**, potentially exacerbating other inequalities. It will take time to understand the full impact and implications of COVID-related interventions concerning access, use and human rights.

- **Some groups within all societies experience deeper digital divides or have less meaningful access than others.** Women in many societies are less connected than men and make less use of connectivity. Digital disadvantage is greater among vulnerable and marginalised communities, and many people experience multiple disadvantages through the combination of factors related to age, gender, ethnicity, language, social class and other factors. Targeted initiatives in infrastructure, devices and services can help to improve the access rates for less-connected social groups, but need to be accompanied by measures to address other deficiencies in meaningful access and should be associated with other measures to address disadvantage and discrimination.

- **Resilient and secure digital infrastructure is crucial for digital inclusion. Governments should protect and promote required infrastructure, including grid and off-grid power as well as communications networks.** In parts of Africa and other continents, large distances between rural and remote communities, including those in SIDS, make last-mile connectivity commercially unattractive to the private sector. Connectivity, speed and reliability are important aspects of infrastructure provision. It will take time and investment to improve the capacity of infrastructure and address regional imbalances, especially in rural areas.

- **Cooperation amongst stakeholder groups is important in ensuring and enabling access. Governments, and multistakeholder partners, should support the establishment and work of effective regulatory agencies and frameworks, address challenges in commercially unattractive areas, and encourage innovative approaches to connectivity** including community networks, appropriate spectrum allocation, access delivered by low earth orbit satellites and the availability of local content, including content in local languages.

The Gender Digital Divide and women's rights

- **Men are significantly more likely to be online or have mobile connectivity than women.** The gender digital gap is particularly wide in Least Developed Countries. SDG target 9c, which seeks to achieve universal, affordable Internet access, cannot be met until this gap is closed.

- **The threat of violence and harassment is a deterrent to women's online participation.** Online gender-based violence is an important factor driving and reinforcing gender inequality in Internet access and usage, leading to some women leaving online spaces. The role of technology services and platforms in propagating gender-based violence should be acknowledged and addressed. Women should be supported by guidance to resist and redress online gender-based violence, including through community-led helplines. Resources, community guidelines and reporting on platforms should be made available in local languages.

- **Concepts of gender equality, inclusion, and women's rights and protection should be incorporated into the Global Digital Compact (GDC)**, as has been proposed by UN Women.

Human Rights and digital development

- **Universal access should respect human rights, to ensure the Internet is both accessible and safe for all.** These include freedom of expression and association, the right to privacy and other civil and political and economic, social and cultural rights set out in international rights agreements. Internet governance structures and the design of digital technologies should respect these rights. Standards development organisations should consider inviting participation by experts in online human rights, from all stakeholder communities, in their work.

- **Transparency, accountability and due diligence regarding human rights are the responsibilities of all stakeholder groups, including intergovernmental and international organisations, governments, the private sector, the technical community and civil society.** This will require alignment of business practices with digital rights and cooperation between stakeholders to address issues such as disinformation, discrimination and hate speech, especially at times of political unrest, elections and transfers of power.

- **Access to the Internet provides a crucial opportunity for access to information and expression.** Governments should avoid recourse to Internet shutdowns because of their negative impact on both human rights and economic welfare. Social media and technology companies should support citizens in their advocacy efforts concerning shutdowns.

- **It is important to improve the monitoring and implementation of digital rights.** A number of suggestions have been made to establish international monitoring arrangements within the UN system, with multistakeholder engagement. These could complement and build on existing mechanisms, including both those concerned with digital development and rights and those in other spheres such as climate change.

- **The internet provides opportunities for enhancing rights to education,** as part of broader policies for educational improvement. The quality of education in the Global South, particularly during the pandemic, has suffered due to a lack of connectivity. While ICTs can enable meaningful access for students, differences in global and local adoption rates have exacerbated pre-pandemic inequalities. Experience during the pandemic can be used to improve the use of digital resources in the future.

- **Efforts should be made to help smaller and local businesses take maximum advantage of the Internet.** Use of digital tools by small and medium-sized enterprises has increased greatly since 2020, but micro-enterprises still face significant challenges in their ability to digitalise their businesses.

- **Labour market changes built around online platforms present both opportunities and challenges for job creation and job quality**, especially for women who play a greater part than men in the informal sector in most countries. Lack of training remains a barrier for many people in maximising their employment potential.

- **Digital competencies must be improved, and adaptations in teaching, learning and training methodologies are needed to adapt to new paradigms** in both education and employment. It is important to identify and close the gap between the needs of the industry and tertiary education.

Avoiding Internet Fragmentation

Theme

The maintenance of a global, open and interoperable Internet is a core value of the IGF. This implies that common technical standards and protocols continue to be deployed to achieve a network of interconnected networks across countries and regions, and that standards for content and services are consistent with human rights and with the rule of law. The call for this – applying a framework to the Internet that prioritises the rights and freedoms of users as well as, and through, infrastructural, end-to-end coherence – has been echoed in plans for the GDC.

The risk of fragmentation is real and mounting. While technical and commercial fragmentation – where the functioning of the Internet is impacted by a mix of voluntary and involuntary conditions and business practices – needs to be addressed, fragmentation by government policy that affects the open and interoperable character of the Internet is also of concern.

Messages

Understanding the issues

- The Global Digital Compact provides an opportunity to reassert the value of an open interconnected internet for the realisation of the UN Charter, achievement of the Sustainable Development Goals and exercise of human rights. There is widespread agreement within the Internet community about the value of a global, unfragmented Internet as a platform for human activity.

- The issues raised in discussions of Internet fragmentation are multi-layered, and different stakeholders give a variety of meanings and interpretations to the term. Some are most concerned with technical and infrastructural aspects of the Internet, while others focus on public policy issues including access, rights and impacts on user experience. These are explored in a draft framework prepared by the IGF Policy Network on Internet Fragmentation. Respect and understanding for different people's perceptions and experience of fragmentation is essential if we are to reach effective and coordinated responses.

- A wide range of political, economic, and technical factors can potentially drive fragmentation. However, diversity and decentralisation should not be mistaken for fragmentation. These are fundamentally positive aspects of the Internet's architecture and operations.

Addressing the risk of fragmentation

- Effective multistakeholder governance mechanisms are essential for the governance of a global unfragmented Internet. There is a need to reinforce trust in these mechanisms, to ensure that they are robust and sustainable, and to foster coherence across governance structures as they evolve to meet new challenges.

- There is a need for vigilance concerning new or developing risks of fragmentation. Global cooperation and coordination will be essential in identifying early warning signs, mapping the impact of policies and other developments, and preparing to address the implications of these changes. A multistakeholder approach is best suited to assess, evaluate and monitor the potential unintended consequences of measures that affect the Internet and to suggest effective alternatives that avoid or mitigate the risks of fragmentation. The IGF Policy Network on Internet Fragmentation is a positive example of this approach.

- Internet openness is instrumental in fostering the enjoyment of Internet users' human rights, promoting competition and equality of opportunity, and safeguarding the generative peer-to-peer nature of the Internet. Debates about net neutrality and non-discriminatory traffic management are only part of broader discussions in this context. Net neutrality is necessary but not sufficient to guarantee Internet openness. Infrastructural and data interoperability, and platform and device neutrality, are also necessary.

- While legal, regulatory and policy approaches will 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. Maintaining the integrity of the global network requires international regulatory collaboration and consensus on basic principles.

- Many different factors affect the experience of the Internet in different jurisdictions, including different social, demographic, economic, cultural and political contexts as well as technical and infrastructure issues. The pursuit of some forms of digital governance at national level can increase the risk of fragmentation at the technical level of the Internet. However, regulatory frameworks must also consider different requirements in different contexts and keep pace with rapid change in technology and services.

- There is a need for greater knowledge- and information-sharing among stakeholders, to further discussion of cyber-diplomacy as an evolving phenomenon, and to consider the scope for appropriate interventions. Standard-making bodies should continue to improve outreach and engagement with stakeholders and to improve understanding between policy and technical communities. Technical decisions that bear policy implications should be discussed by standardisation bodies through the direct involvement of all affected stakeholders.

Governing Data and Protecting Privacy

Theme

Data are the key resource of the globalised digital age. The movement of data drives economies, while data analysis, including big data analytics, has been the basis for remarkable innovations across disciplines, from finance, to health and law enforcement.

But the widespread use, routine flow across borders and fungibility of data remain sensitive and unresolved topics. As a transnational, commercial asset, data flows operate in an environment in which there is little consistency between national legal regimes and where there are significant enforcement challenges. The privacy of personal data is too often sacrificed over the course of data exchanges, from the point of collection to application and storage, with deep consequences for trust and security.

To harness the significant promise of data, economically and for research purposes, discussions need to be relaunched around governance, integrity and the protection of peoples' privacy.

Messages

The centrality of data

- **Data have become a critical resource in an increasingly digital age.** Data flows are crucial to international cooperation in many fields including scientific research, law enforcement, and national and global security. Data, data security and data protection are critical enablers of sustainable development. 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.

- **Data can generate both profit and significant social value.** The benefits of the data-driven economy, however, have so far been unevenly distributed. Many people are concerned that they may become primarily providers of data rather than beneficiaries.

- **The relationship between those who generate and those who use data is important.** Data poverty is a significant problem, especially in local communities and among vulnerable segments of populations. Lack of data privacy and inadequate data protection undermine trust in data management. It is important to build data literacy and data capacities across levels of government, in educational curricula and for the general public.

- **Data management and governance are complex issues in both national and international governance.** Developments in data – including big data analytics, innovations in artificial intelligence and machine learning, and innovations across public policy dimensions and the SDGs – demonstrate the need for appropriate consideration of political, economic and social impacts and for nuanced policy interventions. Government and regulatory institutions need the infrastructure and capacity required to implement effective, integrated national data governance frameworks. Application developers have a responsibility to ensure ethical and safe design.

Data privacy and data justice

- **Data privacy is not a matter of convenience or good practice but of human rights.** As well as the rights to privacy, equal treatment and non-discrimination it affects access to other human rights such as those to healthcare, education and public services, as well as democratic rights such as free expression and association. Privacy laws should be substantial, evidence-based and capable of clear enforcement. Those affected by them should be able to understand their implications clearly.

- **Data flows and data exchange should take place without compromising data privacy.** The privacy of personal data has often been sacrificed in the processes of data exchange, between the gathering of information and its application, with intentional and unintentional risks to trust and security. Internet access and use should not be dependent on data-tracking: users should have the right to choose the extent to which their information is shared, including information derived from their online activity.   Personal data should not be exported into jurisdictions which do not provide adequate guarantees.

- **Policies should reach beyond data protection to data justice in which people have choices over how personal data are used and where they can share the returns and benefits of innovation** brought by datasets derived from their data. Privacy protections should thereby contribute to a safer and more prosperous digital economy.

- **Governments and regulators should ensure that personal data are protected,** identifying the differentiated responsibilities of different stakeholders and without imposing undue burdens or responsibilities on individual users. Data governance policies should be developed with multistakeholder input to ensure that implementation challenges are understood.

- **Privacy and data protection are particularly significant for the governance of artificial intelligence and machine learning.** All stakeholders in the AI supply chain have a role to play in upholding privacy rights.

There is a need for independent oversight bodies equipped with appropriate resources. Data protection offices should have a mandate to manage data registration, provide guidance, implement investigations and resolve complaints from data subjects.

Data governance

- **Issues concerning data governance should not be treated in silos or in isolation from their impacts.** The current data governance landscape is a fragmented patchwork of national, regional, and international rules involving responsibilities for national governments, private sector businesses and individuals.

- **Greater coherence is needed on a global level to achieve a balanced approach in which data work for people and the planet.** Existing legislation and regulatory frameworks at national, regional, and international levels are often insufficient and fail to keep up with the pace of change in technology and applications. They should seek to ensure high security standards by businesses and other organisations responsible for holding data.

- **Different contexts and challenges, histories, cultures, legal traditions, and regulatory structures mean that there cannot be one rigid set of rules for all.** Different individuals and organisations also interpret broadly similar approaches in different ways. However, while countries and regions must develop their own tailored approaches to data governance there should be consistency and interoperability to facilitate data flows and ensure a level playing field.

- **Transparency, participation and accountability are important aspects of good data governance.** Important considerations in governing data include (but are not limited to): data standards and classification; data sharing, exchange and interoperability; data security and data privacy; data infrastructure; data and digital identity; data justice and fairness; data traceability, transparency and explicability; data minimization and data limitation; data accuracy and quality; data bias, marginalization and discrimination; the data life cycle, specificity and retention of data use; data accountability and data ethics; data harms, data security and data protection

- **Many stakeholders have roles within this context and should exercise their power and influence to promote effective data governance,** including regulators, researchers, standards organizations, consumer organisations and end users. Policies for data governance should be developed with input from this multistakeholder community which has expertise in both legal debates around privacy and the "real world" challenges of implementing effective data privacy solutions.

- **Developing economies need to enhance their institutional capacities to govern, use and manage data in a comprehensive, objective and evidence-based manner, including through regional and global cooperation.** This requires improved understanding of the institutional capacities of government officials and stakeholders.

Cross-border data flows

- **Cross-border data flows are essential to many aspects of e-commerce and digital trade.** Efficient intra-regional trade and supply chain management relies on the smooth flow of data as well as goods, services and capital. However, all of these require complex cross-cutting considerations for regulatory convergence, harmonisation of legal frameworks, Internet governance, information and communications technology policy reform and strategic regional infrastructure implementation.

- **Current multilateral, regional and bilateral trade agreements are insufficient for current and future cross-border data flows.** These operate in a largely unregulated environment with little consistency between national legal regimes. Approaches differ and are contextual, generating barriers to trade, while many countries do not currently have adequate legislation or enforcement capacity. There is a growing need to develop and harmonise measures to manage cross-border flows that facilitate development and economic value generation, in different contexts, while respecting national sovereignty and user privacy.

Enabling Safety, Security and Accountability

Theme

The security of the Internet is under threat in several ways. Traditional cybersecurity deals with the protection of networks, devices and data from unauthorised access or criminal use. This encompasses the ongoing problem of cyber-attacks, whether they are perpetrated by individuals or state-sanctioned, and whether the targets are civic, commercial or governmental. Factors such as the absence of broad and binding cybersecurity agreements and insufficiently secure networks contribute to the loss of opportunities to capitalise fully on the economic benefits of digital technologies, particularly for developing countries.

Issues of safety, security and accountability are multifaceted, including distinct issues concerning infrastructure, services, content and other aspects of the Internet. Our understanding of safety and security, for instance, now includes persistent challenges of online misinformation and disinformation. In recent years, these have been factors in aggravating the effects of the COVID-19 pandemic as well as posing significant risks to electoral processes around the world. This has emphasised the need for accountability and clear criteria for misleading content.

The concept of 'safety' may be further widened to include environmental safety, considering efforts to 'green' the Internet and reduce carbon emissions associated with digital consumption. The need to address the environmental impact of digitalisation is an increasingly important theme in IGF discussions.

Messages

The role of policymakers

- **Cybersecurity should be seen as a central challenge for Internet policy.** Considerations of trust and security should be integral to the development of safe, secure access, including respect for human rights, openness and transparency in policymaking, and a multistakeholder approach that serves the interests of end-users.

- **Ensuring cybersecurity and preventing cybercrime are both important areas of policy that require serious attention and the development of expertise.** They differ in purpose, however, and the approach required for each is different. An approach that is effective in one will not be effective in the other without adaptation and

  reformulation.

- **Cybersecurity and cybercrime issues have cross-organisational and cross-border dimensions. Tackling these requires:**

a) **whole-of-government and whole-of-society approaches** that include strong partnerships and coordinated efforts, involving parliaments, regulators and other relevant government authorities and agencies, the private sector, the technical community, academia, and civil society; and

b) **efficient and effective regional and international cooperation** that is intergovernmental, multilateral and multistakeholder.

- **Governments, the private sector and the technical community should take care to avoid adopting cybercrime laws and establishing standards that negatively affect the work of cybersecurity defenders.** They should invite all stakeholders to engage in policy development and facilitate interaction and sharing of experience and expertise between their different communities.

- **Civil society should participate in both cybercrime and cybersecurity discussions.** To do so effectively, civil society stakeholders should educate themselves on the different approaches and issues involved, and work with other stakeholders to gather the information and resources required to participate fully in making policy.

Cybersecurity

- **The international community should explore practical ways to mainstream cybersecurity capacity-building into broader digital development efforts.** 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. While doing more to increase the resilience of digital infrastructure is necessary, it is not sufficient. Translating existing international agreements into feasible actions is long overdue.

- **Standards that enable cybersecurity are essential for an open, secure and resilient Internet that enables social progress and economic growth, and are particularly important in protecting those who are not yet connected.** Such standards have been developed, but their use needs to grow significantly to make them fully effective. The United Nations could help accelerate the global adoption of key standards by including their promotion in the Global Digital Compact, by supporting advocacy and capacity building and by encouraging initiatives to test and monitor deployment. Early awareness raising and capacity building on standards should not be forgotten as priorities in areas where many still have to get connected and the internet is growing.

- **More needs to be done to improve national policymakers' and other stakeholders' awareness of the challenges of cybersecurity and of international norms and principles.** This should include awareness and capacity-building concerning the links between sustainable development and cybersecurity, bringing diverse stakeholders together to mobilise effective, sustainable and inclusive stewardship of international cooperation for cyber-resilience. A number of international initiatives have been established to support this. Opportunities to finance cyber resilience also need to be addressed by funding agencies and other stakeholders.

- **Cybersecurity norms must make a difference to the personal experiences of Internet users past, present and future.** Listening to the experiences of individual and organisational victims of cybersecurity attacks, and those of first responders, is important in this context, particularly when developing new norms.

Cybercrime

- **Cybercrime poses an increasing threat to many Internet users.** Regulations countering cybercrime should be sensitive to the size, capacity and resources of platforms. Legal obligations should consider the diversity of the technical sector, and acknowledge the needs and circumstances of smaller businesses in adhering to their legal obligations, for instance in countering terrorist and violent extremist exploitation of their services.

- **Governments and policymakers should ensure that legal responses to criminal and terrorist use of the Internet safeguard both the rule of law and human rights,** taking freedom of expression fully into account and ensuring transparency and accountability in the implementation of measures against cybercrime.

Content and disinformation

- **Disinformation can and should be addressed through mechanisms that address the risks faced by individuals and societies while protecting freedom of expression, pluralism and democratic process.** Support for professional journalism and media plays an important part in efforts to address disinformation, including commitment to established journalistic norms.

- **Media and digital literacy skills empower citizens to take a more critical view of the content or information they encounter, helping to identify disinformation and misinformation and strengthen democratic participation.** Digital literacy education can help to increase online safety awareness, especially for more vulnerable individuals and communities. Initiatives need to be sensitive to the needs and risks associated with different demographic groups. Different approaches for young people and older generations, for example, must respond to different usage patterns.

- **Educational curricula should include digital literacy skills that help children to be safe online.** Initiatives should involve parents, teachers and guardians. Lawmakers and digital platforms should take responsibility to ensure children's safety within a framework of children's rights online consistent with international rights agreements including the UN Convention on the Rights of the Child.

- **The domain name system has limited technical capacity in this context.** Continued stakeholder dialogue should clarify when and how it may be used to remedy specific content problems, and should strengthen due-process norms.

- **Encryption plays an important role in building an open, safe and democratic Internet** and helps users to achieve safety, privacy and freedom of speech. Issues concerning law enforcement and user's ability to manage access in areas such as child protection need to be addressed.

- **Translation issues present significant barriers that can inhibit end-users' meaningful engagement with platforms' community standards and guidelines.** Key terms are sometimes poorly translated, resulting in ambiguous interpretations. Engagement with different language communities to improve the accuracy and relevance of translation, including the communication of concepts without direct equivalents in different languages, is an important part of enabling platforms and users to understand what is expected of them.

Addressing Advanced Technologies, including Artificial Intelligence (AI)

Theme

Advanced digital technologies increasingly shape our economy and society, including artificial intelligence (AI) systems which guide our online experiences, power smart devices, and influence our own decisions and those that others take about us, as well as robotics and Internet of Things applications that are deployed in areas as diverse as manufacturing, healthcare, and agriculture. Beyond their promises, these technologies come with pitfalls. Algorithmic decision-making, for instance, can result in bias, discrimination, stereotyping and wider social inequality, while AI-based systems can pose risks to human safety and human rights. Internet of Things devices come with privacy and cybersecurity challenges. Augmented and virtual reality raises issues of public safety, data protection, and consumer protection.

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 and cooperation – involving governments, intergovernmental organisations, technology companies, civil society, and other stakeholders – are required to ensure that these technologies are developed and deployed in a manner that is human-centred and respectful of human rights.

Messages

Governance

- **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.** They should benefit people and the planet by driving inclusive growth, sustainable development and well-being. Oversight and enforcement mechanisms should follow principles and rules, with AI actors being held accountable for any damage caused.

- **The assumption that technology necessarily enhances equality is flawed.** Those who design machine learning technologies and the data used to train AI applications are often unrepresentative of their societies. Technologies can amplify inequalities and cause harm, particularly to vulnerable and marginalised groups.

- **Societies need to adjust to the transformation that AI will bring about through changes to their cooperation framework and governance model.** Building a human-centred intelligent society requires the full cooperation of government, enterprises, social organisations and academia. Ongoing human control remains essential, to ensure that algorithms do not lead to outcomes that are undesired or uncontrolled. Breaking down silos between engineers and policy experts is critical to achieving this.

- **Global agreement on AI norms cannot be achieved in one straightforward process.** While there are some existing norms, these are mostly soft laws rather than binding principles. The development of meaningful global standards will require effective participation from all countries, including developing and developed countries, and inputs from regional initiatives, as well as the engagement of all stakeholders.

- **Capacity-building is important in efforts to address advanced technologies.** Policies for AI literacy, skills development and language resources for minority languages are needed in order to formulate a truly global approach to advanced technologies.

Trust, security and privacy

- **Regulatory frameworks should include principles to help social media and other platforms fulfil due diligence obligations for the management of content that could damage democracy and human rights.** Frameworks should contribute to the global conversation on online content moderation to empower users, including the most vulnerable groups and users of minority languages. Emerging technologies such as affective computing, which consider how computers may recognise, interpret and simulate human emotions, require substantive ethical assessment.

- **Transparency in the operation and reporting of algorithmic systems is essential for human rights.** AI facilitates the constant observation and analysis of data to personalise and target content and advertising. The resulting personalised online experiences run the risk of disaggregating online information spaces and limiting individuals' exposure to diversity of information. Lack of information pluralism can foster manipulation and deception – furthering inequalities, undermining democratic debates, and potentially enabling digital authoritarianism, hatred and violence.

- **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 that foster trust in AI systems.

- **It is important to recognise and respect the different institutional and cultural backgrounds of diverse countries and communities**, as well as promoting inclusivity and enabling international cooperation in AI.

Rights and content moderation

- **It is essential that policies for content governance by online platforms, and their enforcement, are in line with international human rights standards.** Artificial intelligence and machine-learning technologies are already being used to decide whether content should be posted or removed, what content is prioritised and to whom it is disseminated. These tools play a significant role in shaping political and public discourse in ways that affect both individual and collective human rights, including social, economic and cultural rights and rights to global peace and security. They are often deployed with little or no transparency, accountability, or public oversight. This should be rectified.

- **The same technologies that can be used to promote human rights can also be used for surveillance, to promote violent agendas and in other ways that infringe those rights.** Unintended consequences of automated content management can be particularly detrimental in times of conflict or crisis when they may silence critical voices at a time when they are most crucial.

- **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. They may also have powerful impacts on human rights.** Yet the technical standard-setting processes within standards development organisations do not take human rights concerns fully into consideration. These processes are often opaque, complex, and resource-heavy for civil society and other stakeholders to access and follow systematically. This should be addressed.

IGF ETHIOPIA
2022
ኢትዮጵያ
The 17th Annual Internet Governance Forum
United Nations
Internet Governance Forum
ENGLISH CHANNEL 1