Katowice IGF Messages

Sixteenth Meeting of Internet Governance Forum
6–10 December 2021
Katowice, Poland

https://www.intgovforum.org

1 IGF 2021 Introduction

The Internet Governance Forum (IGF) is a global multistakeholder platform that brings stakeholders together to discuss public policy issues related to the Internet. The Forum is convened by the United Nations Secretary-General, in line with the mandate set out in paragraph 72 of the Tunis Agenda for the Information Society.

In 2021, the Forum held its 16th annual meeting in a hybrid format, in Katowice, Poland and online. Under the overarching theme *Internet United*, the meeting featured discussions on some of the most pressing Internet and digital policy issues, from meaningful access, digital rights, cybersecurity, environmental sustainability and climate change to the challenges and opportunities offered by advanced technologies.

2 Katowice IGF Messages

The Katowice IGF Messages[1] provide an overview for decision-makers of current developments in and approaches to Internet governance and digital policy issues. They are sourced directly from the more than 300 sessions held during IGF 2021. Session organisers were invited to self-identify key takeaways and calls for action at the end of their session as input for these messages. A set of draft messages, curated by the IGF Secretariat, were published for community review. The comments received were considered in the preparation of the final Katowice IGF Messages, published as part of the annual meeting's outcomes.

Katowice IGF Messages are compiled for each of the six IGF 2021 issue areas:

- Economic and social inclusion and human rights
- Universal access and meaningful connectivity
- Emerging regulation: market structure, content, data and consumer rights and protection
- Environmental sustainability and climate change
- Inclusive Internet governance ecosystems and digital cooperation
- Trust, security, stability

3 Economic and Social Inclusion and Human Rights

- **Adequate enabling environments** (e.g. policies, legislation, institutions) need to be put in place at the national, regional and global levels to foster inclusive, just, safe, resilient and sustainable digital societies and economies.
- Stakeholders have a **joint responsibility in ensuring that digital transformation processes are diverse, inclusive, democratic and sustainable**. Commitment and strong leadership from public institutions need to be complemented with accountability and responsibility on the part of private actors.
- Digital IDs and financial inclusion solutions could contribute to fostering meaningful participation in the digital economy and society. **Public actors are encouraged to create or upgrade digital ID ecosystems and put in place normative frameworks** to ensure

[1] Messages produced during the 16th IGF meeting were subject for public consultations since the meeting ended on 10 December 2021, before updated and marked as final on 6 January 2022.

that these ecosystems are inclusive, human rights respecting, and interoperable. Regulators and the private sector are invited to support a **more extensive use of technologies as a way to achieve sustainable development and drive digital inclusion**.

- With the expansion of platform and digital work, regulators need to ensure that labour dimensions are added to broader digital policies and regulations, so that the **rights and interests of workers are adequately protected.**
- International organisations are invited to **develop definitions and tools to help countries measure digital transformation and its societal impacts** in an objective, effective and efficient manner.
- **Agile regulatory frameworks** – at the national, regional and, where possible, global levels – need to be put in place to outline rules, responsibilities and boundaries for how public and private actors behave in the digital space.
- **Artificial Intelligence (AI) needs to be developed and deployed in manners that allow it to be as inclusive as possible, non-discriminatory, auditable and rooted into democratic principles, the rule of law and human rights**. This requires a combination of agile self, soft and hard regulatory mechanisms, along with the tools to implement them.
- Policies implemented by Internet platforms to deal with **harmful online content** need to be transparent, acknowledge the limits of automated content moderation, and ensure a proper balance with the right to freedom of expression.
- A suggestion was made for states to consider **transposing the UN Committee on the Rights of the Child (UNCRC) General Comment 25 (GC25) on children's rights in the digital environment into national regulation and legislation, and to ensure compliance**. Another suggestion was for the UNCRC itself to tailor recommendations to individual countries during dialogue and review processes related to GC25.
- To ensure that human rights are enforced and upheld in the digital space, a careful reflection is needed on **how technology serves humanity, as opposed to simply putting in place safeguards around the edges and waiting until harms occur.** States' duty to prevent potential harm of human rights (e.g. through regulation and enforcement) needs to be complemented with (a) effective access to remedy when people are victims of human rights violation, and (b) responsibility on the part of relevant actors in integrating human rights due diligence and impact assessments throughout the entire life cycle of a technology.
- Mechanisms need to be put in place to **ensure that the rights-limiting measures put in place to cope with public health crises such as the COVID-19 pandemic are not prolonged indefinitely** and become instruments of mass surveillance.
- States and the private sector should **perform due diligence when it comes to the protection and promotion of digital rights,** including in the context of public-private partnerships.
- **Issues that were raised, but on which disagreement remains among stakeholders,** include (a) the possibility of introducing a moratorium for certain human rights violating technologies that are not (yet) regulated adequately (e.g. facial recognition and biometric data collection and analysis), and (b) the potential development of a legally binding agreement on technology and human rights, which would build on existing frameworks (e.g. the Universal Declaration of Human Rights and the UN Guiding Principles for Business and Human Rights).

4 Universal Access and Meaningful Connectivity

- Ensuring that all people everywhere have meaningful and sustainable access to the Internet must be a priority. **Access to the open Internet is key for bridging the digital divide, as well as fostering democracy and human rights**.
- The open Internet can be considered a multistakeholder domain, fostering dialogue. There are three main elements that structure **the concept of meaningful access:** (a) affordable access (e.g. to connectivity, devices); (b) social environment (skills, education, content, multilingualism); (c) meaningful, permanent, and quality connectivity (including the technical foundation that allows meaningful access to become a reality).
- Public access through institutions such as libraries can help deliver on all of the components of access that help drive development – **equitable and inclusive connectivity, content and competences**. The COVID-19 pandemic has demonstrated that countries had to prioritise the massive development of connectivity infrastructure to connect the unconnected to an increasingly digital world.
- Regarding online education and learning, **many countries are faced with a lack of devices, weak infrastructure and low levels of digital literacy and digital skills**. Increased support and international collaboration and partnerships to tackle these issues are key. Individual actors at local and regional levels should also take responsibility in finding solutions together.
- For all stakeholders working on connectivity and access in community contexts, it is **vital to map out their community networks**. Data from these exercises can feed into building participatory training curriculums or refining existing curriculums. Community networks are also struggling to have a financial sustainability model. Some countries are reviewing their Universal Access Funds requirements to allow small cooperatives or community networks to access those programmes and increase rural and remote connectivity. In addition, regulatory measures and public policies should consider the sustainability of private sector investments, in order to help strengthen infrastructure coverage globally.
- Multiple different **actions are needed to fight against illiteracy, in particular in the Global South. There is insufficient common language between stakeholders, inadequate participation and lack of critical assessment of whether engagement is meaningful.** There is a need to improve coherent use of terminology which can impact the effectiveness of Internet policy debates. For example, having better translation between languages, but also exchange within and between regions.
- **Multilingualism** is a foundational component of Internet inclusivity. The development of local language content, the widespread adoption of **Universal Acceptance (UA), and the promotion of Internationalized Domain Names (IDNs) are key** to creating a truly multilingual Internet – a driver of peace. All stakeholders should promote policies that support the development of local language content and the adoption of UA; governments in particular can drive multilingualism on the Internet by incorporating these policies in their procurement contracts.
- While access to the Internet must be supported, it also **must be ensured that the open Internet access goes hand in hand with infrastructure deployment** - especially needed in the least developed countries, landlocked developing countries and small island developing states.
- **Competition was identified as a highly desirable characteristic** of the Internet across the various participants representing diverse stakeholders. Competition was welcomed in every aspect from connectivity, creation of inclusion, accessibility, small-players, geographically (Global South) etc.
- There is an **urgent need to understand why policy solutions already known and proven to be effective are not being more widely implemented**.

5 Emerging Regulation: Market Structure, Content Data and Consumer Rights and Protection

- The **complex interplay between the market and society** is being reshaped by online platforms. Online platforms continue to gain power in the digital world, generating high impact throughout the globe, especially in the Global South. There is **no one-size fits all approach as** impacts may be positive or negative, depending on the local reality.
- Suggested **underlying principles to guide policy approaches** towards strengthened market competition and consumer protection include: (a) transparency; (b) global taxonomy of service providers; (c) emphasis on rights application; (d) proportionality; (e) acknowledging the complexity of platforms, content and behaviours and jurisdictions; (f) harmonization - ensuring that the Internet remains a global, unified platform that enables the exercise of human rights.
- There is a **necessity to strengthen the multistakeholder approach**, in order to be truly inclusive and to develop effective policies that respond to the needs of citizens, build trust and meet the demands of the rapidly changing global digital environment. The most powerful stakeholders - governments and private companies - are responsible for **ensuring that civil society actors are able to meaningfully contribute to these processes**.
- All stakeholders must work together to **foster digital growth and development at the local level,** within different countries and regions; approaches could include governmental grants or investments from large companies to foster local small and medium-sized enterprises (SMEs).
- More awareness should be raised about the interplay between big platforms, competition, and consumer rights, among both consumers and global, regional or national antitrust regulators. **Antitrust regulation could incorporate the concept of public interest**, addressing the issue of market power and concerns about fundamental rights such as the right to freedom of speech. Tailored approaches like pro-ethical design in regulation should also be considered.
- In the debate on digital sovereignty and digital autonomy, more **focus needs to be placed on the individual autonomy of Internet users within the digital realm**.
- New technologies incorporated in video games are also likely to become an object of discussion around questions on intellectual property. Examples include non-fungible tokens, metaverse and user-generated content. As **video games are likely to incorporate cutting-edge technologies for user engagement,** governments are called to pay further attention to this innovative sector for inspiration.

6 Environmental Sustainability and Climate Change

- **Climate change, biodiversity loss and pollution** have catastrophic consequences for humans and other species. Human activities have caused around 1.1 °C of global warming to date, causing scientists to sound a “code red for humanity” (IPCC, 2021).
- As another megatrend of the 21st century, digitalisation has a significant environmental footprint. Urgent action is needed with regard to: (a) **The digital world’s carbon footprint,** amounting to about the footprint of the aviation industry, is expected to increase in the

years ahead; (b) The main source of impact stems from emissions related to the **manufacturing and powering of user equipment**; (c) **Extraction of resources (also critical for digitalisation)** - with it are associated about 90 percent of total biodiversity loss and water stress (d) **End of life resource loss and e-waste**: E-Waste is the fastest growing waste stream within our already very wasteful society. In 2020, a record number of 53.6 million tons of electronic waste was released into the environment.

- **However, digitalisation can also provide us with the tools and devices to combat and adapt to climate change** - e.g. by using digital technologies to help us evaluate consequences of actions already taken and develop new ones that benefit the global community. Areas of beneficial application of digitalisation include (among others) **environmental data, food and water systems and circular economy**.
- Faced with the realities of anthropogenic climate change, it is clear that the **environmental impact of technology needs to be further investigated and adequately addressed**.
- There is also a growing need to **tackle emissions from mineral extraction**. The digital devices we use today are host to a complex mix of materials (screens alone being made up of 14 different elements), many of them produced in developing countries. **Many extraction sites are correlated with negative impacts on the health of the local human population as well as surrounding fauna and flora**. As renewable energy technologies are also heavily reliant on the same minerals, challenges associated with mining and extraction could lead to supply disruption, slowing down a successful transition to clean energy.
- **Encourage circular economy and tackle e-waste**: Whenever a digital device is bought, significant environmental damage has already occurred. It is thus crucial to strive towards circular business models, keeping the devices and resources in use as long as possible.
- When devices are finally taken out of the cycle, proper disposal is key. It is advocated for **raising awareness for the problem of e-waste and making use of public-private partnerships to replicate good practices for reducing e-waste**, building on the latest pollution data. Targeted capacity support (financial resources, infrastructure and knowhow) is needed especially for developing countries, who carry the burden for many of the disposal sites.
- **Acknowledge and encourage the contribution of youth:** Young people play a key role in the achievement of sustainability and environmental conservation, and their actions need to be supported by providing necessary infrastructure and connectivity.

7 Inclusive Internet Ecosystems and Digital Cooperation

- A **positive vision for the future of the Internet** has to draw together the strands of core values across technical principles, human rights, access and openness, transparency, and rule of law, as well as economic considerations. This can only be done in an inclusive multistakeholder manner, where the interests of all actors can be addressed.
- While the Internet contributes to social, cultural and economic growth, questions of governance, accountability, misuse, trust and access still exist. As the Internet cannot be dealt with from a one-dimensional perspective, **collaborative, equitable and inclusive Internet governance** is imperative and requires well-structured coordination and consolidation.
- There is a need to think about the **sustainability of the Internet governance ecosystem**, including the empowerment of youth - the next generation of experts and leaders. Given the

rapid pace of technologies, there is a need to build the capacity of the generations to come. One of the concrete ways this could be done relates to creating educational curriculums based on competencies and skills in the local languages of targeted groups. Similarly, the ‘’train the trainer’’ concept could be a quick, feasible and effective way to ensure educational professionals, such as teachers, are equipped with knowledge and skills to pass on to massive numbers of multiple generations.

- Violation of the rights of youth and minors on the Internet are a growing concern. One approach to protecting young people against online threats (e.g. data breaches, cyberbullying) could be to **establish a global network of Youth Digital Ombudspersons** to act as mediators between the youth and all stakeholders.
- Digital inequalities have become much more visible during the COVID-19 pandemic, calling urgently for actions to resolve them. It has been raised as a concrete example to prioritise digital cooperation. Through collaboration, partnerships and cooperation, stakeholders can exchange good practices and attract investment to **ensure an affordable and accessible Internet for all**.
- **Inequalities** are multi-layered nuanced areas and **require dedicated assessments and tailored solutions**. Women and girls are especially affected. The inclusion process should be designed and implemented in a multistakeholder manner through capacity development, empowerment and awareness raising and building common understanding across stakeholder groups.
- **Digital cooperation requires trust, and the IGF can help build that**. To adapt to the future, the IGF has to boldly embrace the policy controversies that face the Internet.

8 Trust, Security, and Stability

- The **development and implementation of cyber norms** should include the views of all stakeholders (including victims, first responders, and frontline defenders) and address meaningfully their needs and responsibilities. Processes need to be based on research and analysis which include these communities.
- **Industry sets of good practices, standards that are globally recognised, norms and principles** (such as those under the United Nations’ (UN) Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG)) that call for states to focus on the security of supply chains and reducing vulnerabilities, and regulatory instruments – like labelling and certification schemes – are also emerging. However, **more stakeholders should be aware of best practices** and base their work on them. Initiatives and forums, along with standardisation organisations, play an important role in gathering actors together.
- Different forums, at the UN and beyond, need to have distinct roles, but multiple dialogues are not necessarily a bad thing. The multistakeholder community should take advantage of the **upcoming opportunities, to contribute to and participate** in the new OEWG dialogues on cybersecurity. The IGF may need to have an expanded role in facilitating either implementation or multistakeholder inclusion in cyber dialogues at UN.
- It is too early to celebrate **cyber norms; they must be implemented**! An effective implementation, e.g. through Security by Design, must respect core basic principles such as openness and decentralisation that have made the success of the Internet.
- **The norm to protect the Public Core of the Internet** should not be interpreted as enabling or encouraging control over the Internet, but as a norm of restraint that is largely oriented towards moderating malicious state behaviour. Actors around the world need to better understand and further define what is meant with “public” and what constitutes a

violation of the norm. To this end, civil society and other non-governmental actors should continue in calling out violations of the public core norm.

- **Addressing cyberterrorism and violent extremist content** is a complex and important problem. Human-rights-based multistakeholder approaches on cybersecurity lead to better outcomes but are also harder to achieve. Transparency and inclusiveness are vital to their success. It takes time to build trust and relationships in which challenging conversations can take place. It is vital that such approaches succeed as the alternative is a cacophony of incoherent and less effective approaches.
- **The dialogue on industry security standards** needs to be broadened with more stakeholders, including industry, regulators, standardisation organisations. Places like the Geneva Dialogue or the IGF provide a platform to bring them together.
- **Neutrality holds significant potential as a force for stability** in cyberspace and - in times of lively global discussions - can advance the understanding of key conditions for implementing rules of responsible behaviour. Greater clarity about state views, which have been the traditional focus under the law of neutrality, has the capacity to create safe spaces for non-state actors that assist vulnerable groups.
- **A responsible use of AI algorithms** ensures the preservation of human rights and avoids biases that intensify inequality. Policies to deal with misuses should be developed where needed.
- Women and girls are disproportionately victimised online and find it difficult to obtain support. Governments need to **harmonise legislation to protect victims** of non-consensual intimate image abuse, and ensure easy access to redress. Network and platform policies need to accommodate a spectrum of global cultures. Peer support networks for girls who are victims of online gender-based violence, such as Safer Internet Centers, must be strengthened, while digital literacy should be improved through school curricula and start from a young age, before they venture online.
- Discussions on Internet of Things security should involve all stakeholders (i.e. private, public, technical, academic and civil society) include more youth representation, pursue a user-centric approach, and work towards **a unified set of open security standards,** while leaving space for users to customise to what is appropriate for their needs.
- Cybersecurity has become even more important in times of hyper-digitalisation as a result of the COVID-19 pandemic. **Cybersecurity measures put in place must be designed to evolve with the rapid digital transformation,** including enabling important social services to function online instead of physically. Cross-silo collaboration is essential to strengthen cybersecurity.