*Published on 10 January 2018*

# IGFREPORT

# FINAL REPORT FROM THE 12th INTERNET GOVERNANCE FORUM

dig.watch/igf2017

*IGF 2017 Report* prepared by the Geneva Internet Platform with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation

## Reflecting on IGF 2017: The values at the core of our digital future

If the Internet is a mirror of society, as Vint Cerf argued, the Internet Governance Forum is a mirror of global digital politics.

IGF 2017 reflected on a very turbulent year in global politics, with a number of issues resonating throughout the week: values on the Internet, digital future and frontier issues, dealing with data, cybersecurity and digital commerce, and the need for action and capacity development.

Perhaps succeeding better than in the real world, many convergences were created at the IGF, as the *Geneva Messages* indicate. However, differences emerged as the discussion moved from principles to concrete action and details. For example, while there is shared understanding of the need for action in cybersecurity, there are differences as to whether this should be done gradually through existing law, or through major action with the adoption of a cyber treaty.

Among the most frequently used words at this year's IGF, many relate to human values, such as 'community', 'democracy', 'trust', and 'freedom'. Values came into focus in many discussions on artificial intelligence (AI), fake news, the role of Internet companies, human rights, and others.

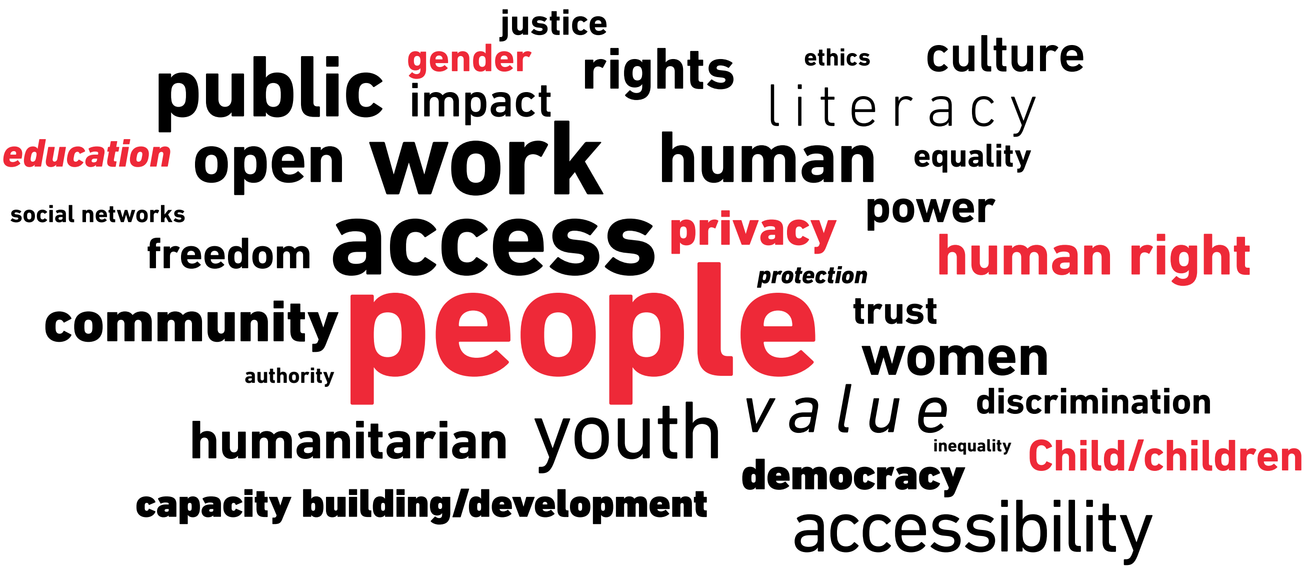
*Continued on page 2 and 3*

The opening ceremony of IGF 2017, on 18 December.

*Credit: UN Photo/Jean Marc Ferré*

## IN THIS ISSUE

Click on the icons in the digital version to access session reports and additional information.



*Values are at the core of our digital future. The tag cloud shows the prominence of terms related to values and society.*

Using the mirror metaphor, the values we relate to offline will apply online. If people are fair, generous, and peaceful offline, they are so online. But the reality is more complex. The Internet shapes our values and way of life.

For example, it amplifies political differences and reduces space for empathy across political, ethical, or social divisions. It also shapes behaviour, in particular that of younger generations. What can be done if our reality and perception are shaped by search-engine algorithms? Or if what we read is being affected by the spread of fake news or information disorder?

## The digital future and frontier issues

'Shape your digital future' was a well-chosen theme for the 12th IGF. In time of uncertainties, we turn to the future, which inspires with new possibilities. The future is both reassuring – if the possibilities become reality – and threatening – due to the uncertainties and unknown unknowns.

AI dominated the discussion on the digital future, which reflected its prominence in media and public debates. Discussions ranged from known unknowns – technological progress, the importance of data for AI, autonomous weapons and cars, the relevance of ethics – to unknown unknowns on the limits of AI's growth and its impact on the future of humanity.

## Dealing with data, cybersecurity, and digital commerce

Data, cybersecurity, and digital commerce were three of the most prominent issues in dealing with the known knowns in digital policy. Data was in the Top 5 most frequently used terms during the IGF. It featured in general debates, but also in very concrete discussions on what will happen on 25 May 2018, when the EU General Data Protection Regulation (GDPR) comes into effect.

Data was also the underlying theme of a series of open forums organised by Geneva-based organisations focusing on data in humanitarian, climate change, and trade and development activities.

Cybersecurity was another frequently mentioned concept. The underlying question was how to fill the gap in global cybersecurity regulation, which appeared after the last United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) failed to reach consensus on a final report. Microsoft's proposal for a Digital Geneva Convention triggered many debates, including controversies. *More on page 5: Is there a need for a cyber treaty?*

The debate on digital commerce took place only one week after the World Trade Organization (WTO) Ministerial Meeting in Buenos

ARGENTINA
11ª CONFERENCIA MINISTERIAL DE LA OMC
BUENOS AIRES 2017
MC11
BUENOS AIRES
2017
UNDÉCIMA CONFERENCIA MINISTERIAL DE LA OMC
BUENOS AIRES, ARGENTINA | 10 - 13 DE DICIEMBRE DE 2017
CHAIRPERSON
SECRETARY

### In other parts of the world...

The WTO Ministerial Meeting in Buenos Aires, which took place a week before the IGF, failed to advance the discussion on e-commerce. The debate continued during the IGF.

*Credit: WTO/ Cuika Foto*

Aires, which failed to advance the discussion on e-commerce. Although it is too early to reflect on the next steps, a few issues emerged. These included a possible plurilateral agreement on digital commerce, and the risk that digital commerce regulation could be a back door for regulating issues of cybersecurity and data protection.

## A call for action

The risks are major and the future is uncertain. Problems will not be solved by themselves. The digital invisible hand does not work, as societal problems will not be solved just by technology.

A call for action resonated during the IGF, but differences emerge on what, by whom, how, where, and when policy action can be taken.

For example, there was consensus that cybersecurity is at risk and something has to be done. But the differences start with the next step. Many OECD countries argue that action should be careful based on implementation of existing law, as the UN GGE recommended. Microsoft proposed the adoption of a Digital Geneva Convention, which has generated controversial reactions.

Similarly, developing countries are far from enthusiastic about a multilateral arrangement on digital trade. Developed countries see it as one of the WTO's priorities.

## Capacity development and awareness building

Divisions about the immediate next steps converge on the need for capacity development and awareness building. Many debates picked up on the introductory remarks by the Swiss President. In addition to building physical bridges, she argued that development assistance should better reflect the digitally driven development, including the use of mobile and digital tools by many local communities in developing countries.

As a concrete step, the Geneva Initiative on Capacity Development in Digital Policy, launched during the IGF, will pool the expertise and experience available in Geneva to help communities worldwide deal with digital policy challenges.

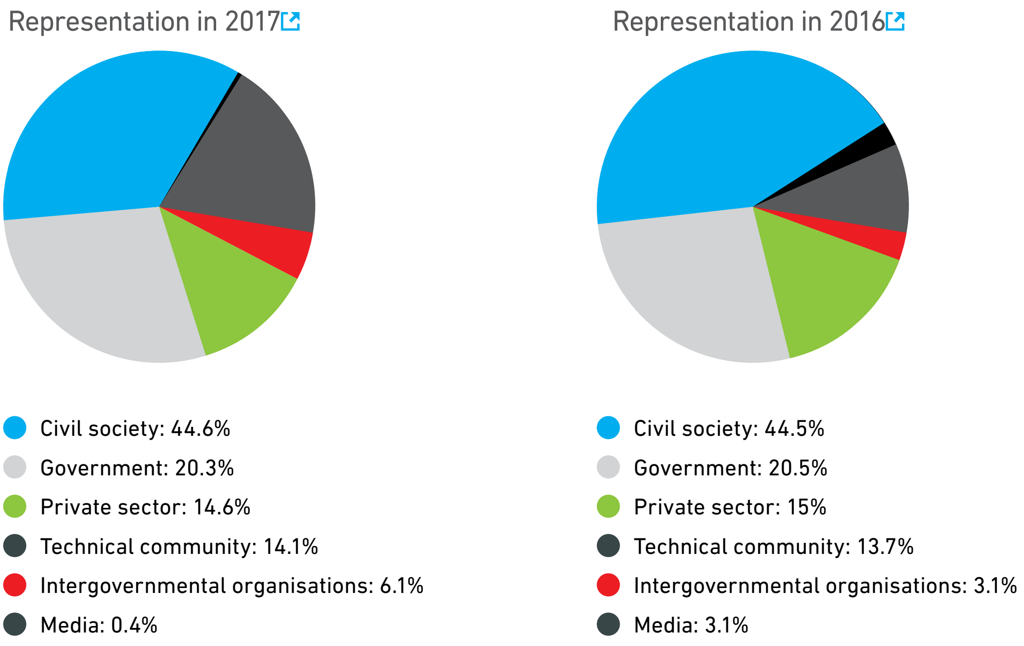
Although the IGF is not a panacea for solving our technology- and Internet-related problems, it succeeded in hosting frank and realistic discussions on our digital future. It also took steps towards concrete solutions, by publishing – for the first time – the *Geneva Messages*. The messages, which summarise the outcomes from the high-level and main sessions, and include many points of convergences from the discussions, show that the glass is half-full. If we build on convergences, we can shape a promising digital future and achieve a widely acceptable digital social contract.

### TOP 10 TERMS USED DURING IGF 2017

1. Internet
2. people
3. data
4. work
5. national
6. access
7. digital
8. information
9. cyber
10. law

### Stakeholder representation

The representation of stakeholder groups participating in situ at the IGF remained largely unchanged from last year:



## Summarising IGF 2017: The thematic issues that mattered the most

The 12th IGF took a bold step towards more tangible outcomes of the annual meeting. For the first time, it published messages – known as the *Geneva Messages* – summarising the key outcomes from high-level and main sessions. The outcome document was the first of its kind, and has repositioned the IGF as a discussion forum intent on producing tangible results.

Inspired by the *Geneva Messages*, the following summary focuses specifically on tangible recommendations, outcomes, or solutions. While daily summaries have been featured in our *IGF Daily* 1, 2, 3, and 4 – published during each day of the 12th IGF – this thematic summary focuses on the most pressing issues for each of the seven baskets from our taxonomy.

### Infrastructure

**1. Automation: With the rapid advancements in automation, AI, and other data-driven technologies, how do we prepare for the future?**

We might not be able to predict with certainty what our digital future will look like, but there are a few things we can do so it does not take us by surprise.

First, focus on education and make sure that future generations are prepared for the new skills required on the job market. Second, ensure that, as technologies continue to evolve, no one is left behind, and their benefits can be enjoyed by all society. And, third, keep ethics and humanity at the core of both technological progress and policy approaches.

**2. Net neutrality: How will the US FCC's decision on net neutrality affect policies worldwide?**

In the USA, the Federal Communications Commission (FCC) repealed the 2015 Open Internet rules, which had until now offered strong net neutrality protection. The vote took place a few days before the 12th IGF.

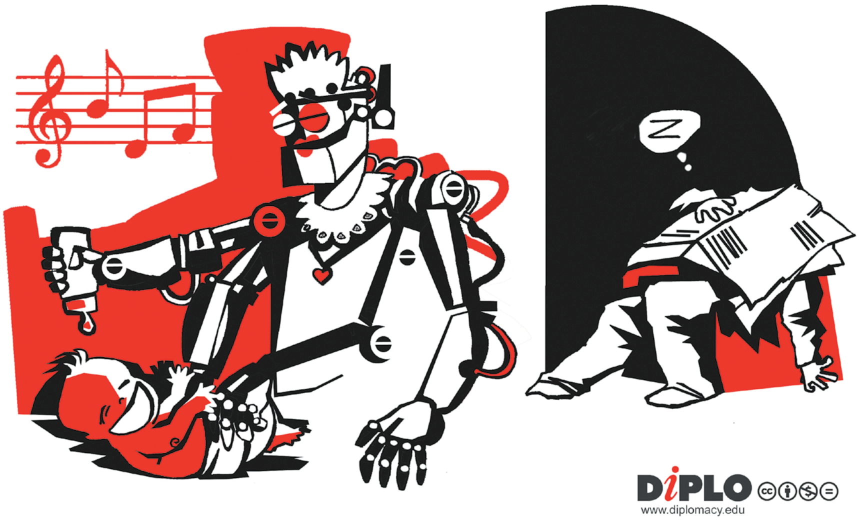
The FCC's decision is unlikely to affect net neutrality protection in other countries or regions. In the EU, net neutrality rules enjoy strong backing by the 28 European countries. The legal framework in the EU contrasted with the way the rules were enacted, and later repealed, by the regulator in the USA. In addition, the statement by the Vice-President of the European Commission gave clear indications that the EU rules will remain unaffected by the FCC's decision.

Although the IGF did not trigger many discussions related to the FCC's recent vote, it is unlikely that this will challenge the strong positions adopted in other countries such as India, which has recently adopted recommendations in favour of net neutrality, banning also the so-called zero-rating practice.

**3. The 5G network: There is a lot of talk about 5G being the network of the future. Why is it so?**

The Internet of the future is described as one in which not only people connect to one another via the Internet, but objects interact as well. The Internet of Things (IoT) is continuously evolving. More and more objects, from refrigerators to self-driving cars, are connected to the Internet. With this, large amounts of data are produced and need to be processed.

5G networks are seen as better suited for all this. They would not only provide better connectivity for end-users (e.g. increased speeds allowing movies to download in seconds), but also facilitate the expansion of the IoT and enhance the ability to collect data from connected objects and machines. This data, in turn, would facilitate progress in fields such as cloud computing and AI. Low latency services could also be enhanced through the use of 5G, thus allowing the development of more user-friendly services in areas like augmented and digital realities.



# Security

**1. Cybersecurity: Is there a need for a cyber treaty?**

This has been a much-asked question since Microsoft proposed a Digital Geneva Convention at the start of 2017. The search for the answer featured in quite a few workshops and corridor discussions.

One of the main questions is whether there is a need for a cyber treaty at all. The main argument against a treaty is that international rules already exist. Since international law applies also on the Internet, it is a matter of applying and enforcing these existing rules, rather than creating new ones.

Even among those who argue that there is a need for a cyber treaty, the predominant view is that it would be very difficult to negotiate new rules. There is generally a feeling of fatigue for multilateral treaties, and divisions on cyber matters run deep.

**2. Tackling cybersecurity: What other ways can help us address the challenges?**

While a new cyber treaty is unlikely, other ways of addressing cybersecurity challenges were suggested:

- Build the capacity of governments to participate in international policy processes such as the UN GGE.
- Identify a venue for debates on cyber-norms: suggestions included a GGE continuation in 2018/19, the creation of an open-ended group within the UN, a (possibly multistake holder) UN body on cybersecurity, a Special Advisor(s) to the Secretary General, or even a Conference on Disarmament.
- Continue regional discussions on confidence-building measures, such as those within the OSCE, the ASEAN Regional Forum, and the OAS.
- Explore technical solutions for cybersecurity problems before they escalate into major policy and diplomatic issues.

**3. Security of IoT: Smart devices and applications are more prevalent in our lives, but as we have seen in the past year, they remain highly vulnerable to cyber-attacks. Can these vulnerabilities and risks be addressed by regulation?**

At the IGF, some argued that principles and minimum baseline requirements for the industry are a better option than regulation, given that regulation tends to lag behind technological progress. Such principles could be defined through standardisation efforts, within organisations such as the IEEE, ISO, and the ITU.

Others believed that users remain the weakest link; more education is needed to make them aware of the risks inherent to connected devices and of the cyber hygiene rules they need to follow. Yet others argued that we cannot trust the industry to act responsibly; users would make safer choices themselves. Instead, we should be looking at ways to develop and enforce transnational regulations concerning the safety and security of IoT devices.

One point of convergence was that there are different layers of IoT security – security of devices and security of data – and they must be given equal importance.

## Is technology a mirror of society?

Technology is a mirror of society, as eloquently argued by Vint Cerf during the IGF opening session. If people are aggressive and selfish offline, they are likely to be aggressive and selfish online as well. But the metaphor is limited. Internet companies impact society, too. They change our habits. Recent research shows that they accentuate our characteristics. Extroverts become more extroverted on social media. Introverts withdraw more into their cocoon of fake online socialisation – being connected without interacting. The mirror metaphor therefore becomes more complicated. But for starters, we should not break the mirror. This would be too simple and would not solve the problem. What would? Share your views on Facebook via #mirrorofsociety.

## Human rights

### 1. Countdown to GDPR: How will the new regulation, which will come into effect on 25 May 2018, affect businesses operating in Europe?

Dubbed as one of the earthquakes we can expect in 2018, the GDPR will affect every business handling the data of EU citizens, regardless of where it is based. However, it will affect businesses differently.

Companies within the EU have already been implementing the privacy rules which have existed in EU countries for a long time. While it is expected that the implementation will be challenging in some aspects, the regulation is based on rules which have existed in the EU for the past 20 years.

The regulation will therefore pose a greater challenge for companies based in other jurisdictions. While privacy rules exist in many other countries, the contexts vary.

The GDPR will also affect large and small companies differently: the implementation may pose a challenge for small and medium enterprises (SMEs) especially in developing countries; it is nonetheless a major challenge for multinationals whose business models revolve around data.

### 2. Gender rights online: The gender digital divide and online gender-based violence continue to be a reality. What can be done to address these issues, and by whom?

Statistics continue to show that fewer women than men are online, and that the gender digital divide is increasing. Thus, a first step for overcoming the divide is to provide women and gender minorities with equal opportunities to access the Internet and the digital economy.

Governments' responsibility derives from international human rights frameworks: since the gender digital divide limits the participation of women and girls, addressing it becomes a human rights concern. Actions need to focus on multiple dimensions, from facilitating access to infrastructure and devices, to promoting education and digital literacy, and empowering women and girls to become contributors of the digital economy.

The cooperation of other stakeholders is equally important. The industry, for example, is encouraged to consider gender diversity issues when new technologies are designed. Fighting gender-based abuse and violence is also a shared responsibility.

At the same time, when devising policies and tools to tackle the divide, other human rights, such as freedom of expression, should not be jeopardised. Gender issues are not only about women's rights, but also about the rights of those in subgroups, and the rights of gender minorities.

### 3. Tools for inclusion: What features should devices and tools have, in order to be used by everyone, including persons with a disability?

Devices and tools need to be reliable, safe, and customisable to foster inclusivity and use by everyone. Tools need to be available for use across different devices.

A main challenge is that devices do not always take cross-disabilities and interlinked uses into account. Assistive technologies also face a challenge of interoperability between devices, which was considered more critical than reliability. Narrowly categorising disabilities should be avoided. Devices should instead be easily customisable and interoperable, and reviewed by persons with disabilities, possibly at the design and development stage.

Tools for online participation, including the tools used during the IGF, also need to be improved. The Webex platform created a challenge for visually impaired participants who were unable to actively and equally participate. Microphones lacked a 'beep' signal, indicating when the mic was on or off. As one participant stated: 'Just as much as we can't see people, people are not seeing us.'

Winners of the 2017 Equals in Tech award, which recognises outstanding women who work to overcome social bias and stereotypes, and empower role models.

## Legal

### 1. Internet intermediaries: To what extent are Internet companies liable for online content that goes through their networks?

When it comes to liability and role of intermediaries, there is a visible trend of putting more burden on Internet intermediaries in this regard, especially in the era of fake news.

On the one hand, there is significant regulatory work that is dealing with this question and which is trying to define more specific obligations of intermediaries, like the work by the Council of Europe and the European Union (especially in the area of copyright). On the other, there are some mechanisms, like algorithms, that platforms themselves are implementing in order to tackle the problem of illegal content.

The main challenge is in how to balance conflicting interests: going forward with regulatory trends that should put more responsibility for content regulation on platforms, but also avoiding the risk of private companies stepping into a judicial role, which may be detrimental to freedom of speech.

### 2. Cross-border data flows: What are the predominant trends and concerns, and how can they be addressed?

Cross-border data flows are seen by many countries – especially developed countries – as essential to digital economy and trade. In advocating for free flows, they argue that the global digital economy can only thrive if data can circulate freely across borders. Interruptions to data flows can lead to the fragmentation of the Internet.

Other countries, mostly developing countries, are more in favour of data localisation policies. These range from requesting that data is stored within national borders, imposing restrictions on the cross-border movement of certain categories of data, or introducing the requirement of prior consent for certain data transmissions. Such policies are often motivated by data protection and security concerns, but there is also a protectionist dimension.

International frameworks (such as trade agreements) that facilitate the free movement of data while addressing data security concerns could hold the answer to striking a balance between legitimate concerns. As demonstrated by the recent WTO Ministerial Meeting, however, trade agreements can be difficult to reach.

### 3. Regulating new technologies: Should blockchain technology be regulated, and how?

While there are countries that have introduced or are exploring the introduction of regulations covering cryptocurrencies, a main question is whether blockchain should be regulated as a whole – if it should be regulated at all – or whether specific rules for issues such as security and privacy, consumer protection, and taxation, should be introduced.

Some believe that we should not be rushing into regulating a technology that is still new and evolving, but rather wait for it to be better anchored into the economy. Others argue that it should be regulated at international level since blockchain itself is 'inherently global in every aspect of it'. As blockchain is a distributed technology, so should be its governance. Moreover, any attempts to regulate blockchain need to be carefully handled so as to avoid stifling innovation.

## Economic

### 1. The sharing economy: How will the CJEU's recent ruling affect Uber and other companies operating in the sharing economy?

On 20 December, the Court of Justice of the European Union (CJEU) ruled that Uber is a transport company, rather than a provider of information society services.

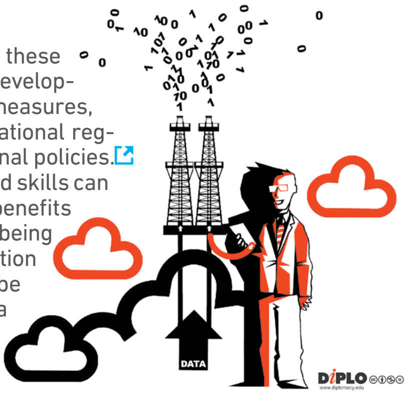
Some expect that the ruling will have a major impact on the digital economy, as it will force a change in the business models of Uber and other companies operating in the so-called sharing economy. In the case of Uber, for example, EU countries will be able to regulate Uber's conditions of operation based on the rules applicable to taxi and other transportation companies.

Beyond the EU, the ruling may trigger similar decisions in other jurisdictions, with significant economic implications for the company. As for other companies in the sharing economy, the ruling spells even less regulatory predictability.

### 2. Data: The oil of the economy, or a threat to privacy and social justice?

New forms of data could theoretically generate enormous opportunities, but this does not come without its share of threats. Privacy violations and surveillance are on the rise, up to the point that even our own bodies may be 'perceived and used as valuable political data'. Democratic and social justice mechanisms might even be under pressure, as governments have unprecedented access to personal information and could use it for less legitimate reasons.

Suggestions to address these challenges included the development of data protection measures, as regional initiatives, national regulations and organisational policies. Advancing data literacy and skills can help citizens capture the benefits that data provides, while being aware of the data protection measures that need to be taken to keep their data secure.



### 3. Economic implications: Internet disruptions continue to take place around the world. What is the economic cost of such disruptions?

Voluntary Internet disruptions, imposed by governments, are a reality in many countries. Apart from limiting the exercise of human rights, the disruptions have economic consequences, both for telecom and Internet companies directly affected by the measures, but also for the economy at large, given the increasing dependency of many services on connectivity.

Due to the significant economic and social consequences stemming from Internet disruptions, the Internet needs to be protected from shutdowns through mechanisms that ensure transparency, proportionality, and due process.

# Development

### 1. Community networks: A value-added solution for addressing the digital divide?

Last year's IGF placed community networks at the forefront; the discussions helped raise the point that there are other connectivity models than those provided by telecom companies.

This year, attention turned to the added value that community networks provide. Such networks are not only about building physical infrastructures. Although they help provide sustainable access to the Internet, especially in remote areas where service providers feel less incentivised to invest, community networks also empower communities to actively contribute to their own digital development. Communities should be aware of the benefits of connectivity, and should be empowered to use the technology.

Some argued that community networks are also an illustration of a 'right to network self-determination'. This is described as the right of communities to associate freely; their right to define the ways and means for the development, implementation, and management of infrastructures as public goods, which can be freely accessed and used to share and impart information.

Policies are required in three main areas: adequate spectrum availability (needed for connecting remote areas, where wireless connectivity tends to be the most optimal solution), licensing (so that community networks function within a legal framework), and funds allocation and financial sustainability (such as the use of universal service funds to support the development of community networks).

### 2. New technologies: Promoting sustainable development, or creating new forms of digital divides?

ICTs and the Internet are crucial for the 2030 development agenda, both for reaching specific SDG targets, but also for achieving many of the goals not directly related to ICTs. New tools and technologies, such as big data, AI, and the IoT, are also important for achieving the goals.

Mobile data can fill gaps in existing statistics and census data. AI and IoT solutions can help solve some of the humanity's most pressing problems, such as poverty, hunger, and climate change. New technologies can help developing countries accelerate their progress towards sustainable development, by leapfrogging certain development stages.

However, a new form of digital divide may be emerging since developing countries may not have the capacities to take advantage of these opportunities. This can lead to new forms of global inequality and unbalanced distribution of wealth. AI is one example: while countries such as the USA and China elaborate AI development plans and strategies to support research and integrate AI into the economy, other countries still struggle with Internet connectivity and other related problems, keeping AI development out of their immediate reach.

While it may be impossible to completely avoid this risk, minimising it should be a priority for stakeholders in developed and developing countries. Solutions could include technology transfers, foreign investments, and support for education, and capacity development.

### 3. SDGs: Cybersecurity is often mentioned as an important factor for fulfilling the goals. What is the link?

Human rights are an important component of the success of SDGs, in particular Goal 16 which promotes peace, access to justice, and strong institutions. Security is intrinsically a human right; states have a responsibility to protect human rights, particularly for vulnerable groups. Even though cybersecurity is often framed as a national security issue, states need to openly discuss the human dimension, and reconcile the two framings.

Development and growth are heavily impacted by cyber-attacks. Economies are increasingly dependent on ICT, and cannot develop in an insecure environment. The peace and stability of the interconnected society are very dependent on cybersecurity, as cyber-attacks can undermine public trust in democratic processes, while cyber-armament can endanger international stability. More investment should be made in defence than in offense, with increased transparency and accountability around cyber-armament; the role and responsibility of world leaders is crucial.

The IGF Best Practice Forum on Cybersecurity can play an important role in discussing the ways to contribute to SDGs, particularly by building a culture of cybersecurity and identifying shared values, as well as by shaping the 'duties of care' – responsibilities of individual stakeholders. National and regional IGF initiatives have the potential to involve new voices on local and regional levels, and to facilitate comprehensive discussions through the exchange of views among national and regional IGFs.

## Towards inclusive and comprehensive capacity development

One of the main points of convergence throughout IGF 2017 was the need for inclusive and comprehensive capacity development.

Inclusiveness cannot be taken for granted: A whole-of-government approach can rope in the various sectors, as would a multidisciplinary approach that extends to those working in economic and human rights sectors, among others.

Comprehensive capacity development, consisting of various components and formats (including schools, camps, online courses, and high-level events) and facilitating the exchange of knowledge and experience, also helps bring in various stakeholders and professional levels.

## Sociocultural

### 1. Fake news and 'information disorder': How can they be tackled effectively?

Fake news, and how to respond to it adequately, was a prominent topic in a number of sessions and reverberated around the IGF 2017 corridors.

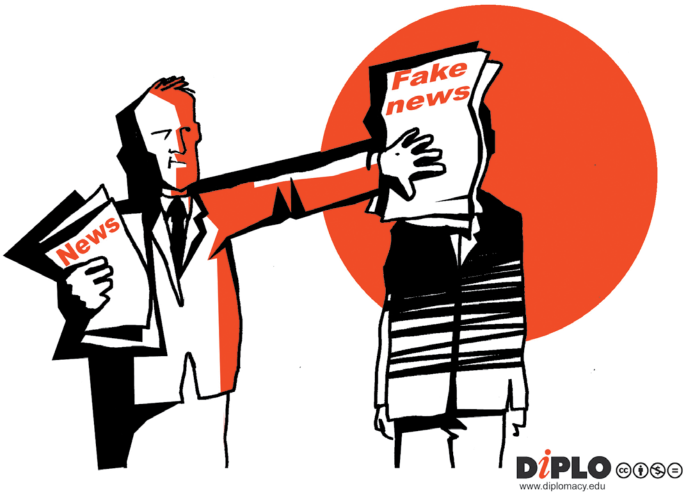
Some questioned the usefulness of the term and argued that the hype around the problem should not lead us to forget that the question of relying on and trusting news has always been with us, as have filter bubbles.

While fact checking and counter narratives were highlighted as important, there were reminders that fake news cannot be countered simply by presenting the 'correct' facts.

Rather, critical thinking needs to be encouraged, digital literacy needs to be included in school curricula as early as possible, and the public needs to be engaged through storytelling and other devices.

The role of critical journalism and the much needed support for the profession were also highlighted. Some voices also called for technological solutions to counter fake news and encouraged the exploration of these.

Generally, there was a lot of caution when it came to content regulation of online platforms and policy-making in general, as many expressed fear that such regulation or legislation would negatively impact freedom of speech. This balance between freedom of expression and countering fake news was identified as one of the key challenges for the years ahead.



### 2. Content policy: Where and how do we draw the line between what is appropriate and what is not when it comes to online content, and how can this line be properly drawn and enforced without limiting freedom of expression?

Beyond fake news, content policy discussions raised questions about the roles and responsibility of intermediaries for the content on their platforms, including issues such as extremist content, child safety online, sextortion and gender-based violence, domain names, and intellectual property.

With these rising challenges, companies are increasingly using automated systems to flag and remove content, which could be of great help in identifying harmful material among the massive amount of content continuously generated online. At the same time, the move towards automation has intensified calls for companies to be more transparent about what they allow and do not allow online, and how these decisions can be challenged.

To ensure that legally and ethically sound decisions are made, governments have started to collaborate with Internet companies to find solutions, while others are resorting to existing or new law. Ultimately, however, these issues are not created by the Internet, but technology online amplifies offline behavior, as pointed out by one speaker.

### 3. Local content: A multilingual Internet can help bring more people online. But how can we facilitate this multilingual Internet?

Bringing the next billion(s) of people online is not only a matter of deploying infrastructures and making connectivity affordable. The Internet needs to be relevant also, and relevance often comes with local content, in local languages.

There are several actions that can be taken to support the development of local, multilingual content. Governmental policies to facilitate access to information, ideally in an open, reusable format, allow developers, journalists, and bloggers to develop local digital content. Digital literacy is key to empowering users to become creators of content themselves.

Promoting a culture of entrepreneurship and innovation, among the young generation especially, is important in fostering the development of projects aimed at creating local content that responds to local needs. And not to forget tools and technologies that can promote a more inclusive and multilingual Internet. Internationalised Domain Names (IDNs), facilitating the registration and use of domain names in local languages and scripts, enable online multilingualism.

More efforts are needed to solve technical challenges, and ensure the universal acceptance of IDNs across infrastructures and services. We also need to consider the integration of local content into the global Internet; and here constant improvements in AI-based translation tools come to hand.

# Highlights from the 4th Day

**If you have read our highlights from each day, you will not want to miss the highlights from the fourth and last day of the IGF. Although there were fewer workshops, the discussions focused on some of the most pressing issues in digital policy.**

## Jurisdiction: Tackling digital policy incoherence

The Internet knows no national borders, but the international system does. Tensions between the cross-border nature of the Internet and the territoriality of national jurisdictions pose a challenge to Internet companies operating across jurisdictions, which need to adapt to the different legal frameworks. This also creates complications for governments, especially in criminal investigations which involve data stored in other countries, and in cases of illegal content, often hosted in foreign jurisdictions.

This creates uncertainty as to what rules apply, when, and where. For example, the GDPR will pose an implementation challenge to registries and registrars of generic top level domains, whose contractual obligations to collect data of domain name registrants seem to be in conflict with the new regulation. The same applies to the right to be forgotten, introduced by a decision of the CJEU, with applicability beyond European shores.

This legal uncertainty and lack of digital policy coherence at international level is increasingly tackled by courts. A recent example is the CJEU's ruling declaring Uber a transportation company, and which will impact the business models of the sharing economy.

Ensuring digital policy coherence and making sure that the international system is 'legally interoperable' remains a challenge. Addressing it requires coordination among the actors to reach a common understanding on the issues and methods for tackling them.

## Threats to freedom of expression online

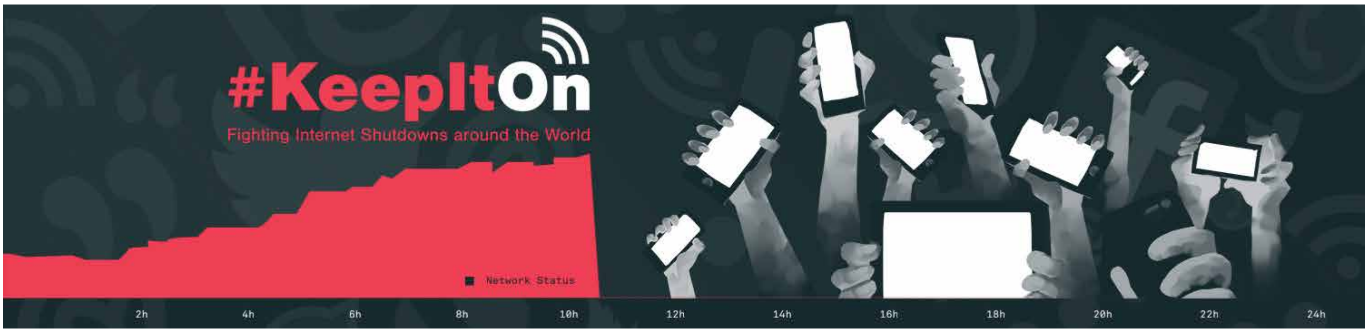
Digital rights have come up in many discussions, from tackling cyber threats and extremist content, to dealing with Internet shutdowns. Many issues concern freedom of expression: how various policies imposed by governments or self-developed by Internet intermediaries affect this right, and what can be done to safeguard it further.

What are the global trends on protecting this right? A recent report by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) notes a growing positive trend of enacted freedom of expression laws across the globe. But there are worrying negative trends for media freedom, safety of journalists, legal restrictions on access to information, and Internet shutdowns. Internet shutdowns, which hinder the enjoyment of human rights, and in particular freedom of expression, have increased around the world. So have the initiatives – such as the Keep It On campaign – which aim at countering the negative effects.

When governments impose Internet shutdowns, they often motivate such action by the need to protect public order or national security. Remedies are needed to allow the public to challenge these actions, and have them reviewed by judicial bodies.

Pressured by governments to take measures to deal with problematic online content, Internet intermediaries have started using algorithms and AI to identify and take down such content. An open question is whether these algorithms are reliable and can be completely trusted to not lead to unintended consequences. As for tackling fake news, measures cannot be used to censor free speech. The principles of necessity and proportionality come into play, which also need to be kept in mind generally when dealing with content monitoring, blocking, and take-downs.

Online violence and harassment against women, gender minorities, marginalised groups, journalists, and others, also discourage and prohibit individuals from exercising their freedom of expression in the online space. Both governments and Internet platforms have responsibilities in curbing these phenomena.



The Keep It On campaign spreads awareness about global Internet shutdowns, and urges governments to act.

## READ MORE HIGHLIGHTS:

**Day 0: https://dig.watch/igf2017-day0**
**Day 1: https://dig.watch/igf2017-day1**
**Day 2: https://dig.watch/igf2017-day2**
**Day 3: https://dig.watch/igf2017-day3**

## Youth: Engaging the younger generation in Internet governance

Many times throughout the IGF week it was said that Internet governance processes need to be inclusive. There was much debate about ways and means to ensure that all stakeholder groups have a seat and a voice at the table. What about young people, the generation that will live in the digital future we are now trying to shape? What is being done to better integrate them into these processes?

These were some of the questions raised in the context of a discussion on Youth IGF initiatives. As outlined in a publication produced by the IGF Secretariat, there are several initiatives focusing on the involvement of youth. Some are organised by national, subregional, and regional IGF initiatives (such as the Netherlands Youth IGF and the Asia Pacific Youth IGF), while others are set up independently (such as the Youth German IGF, the Youth IGF Turkey, and the Youth Latin American and Caribbean IGF).

In some cases, the voices of the younger generation are integrated into the planning processes and the programmes of existing IGF initiatives. This is the case, for example, with the SEEDIG Youth School (an initiative of the South Eastern European Dialogue on Internet Governance), the youth-dedicated workshops and training organised by the IGFs in Brazil, Nigeria, Sri Lanka, and the USA, and the YouthDIG Programme of the European Dialogue on Internet Governance (EuroDIG).

There are also schools on Internet governance which focus on youth, as well as youth-targeted capacity development programmes, such as those run by ICANN and the Internet Society.

As these initiatives share the common goal of empowering youth to help shape digital policy, they need to interact with and learn from each other. The Youth Coalition on Internet Governance is one potential forum.

Mentoring programmes for young participants, more youth panellists, and a better representation on the Multistakeholder Advisory Group (MAG) could have positive effects. Additional funding for youth fellowships, greater outreach to local communities, and setting quotas for youth participation at the IGF were other suggestions made during the tacking stock session.

## The IGF as a process: Dynamic Coalitions, Best Practice Forums, and National and Regional IGF Initiatives

Dynamic Coalitions (DCs), Best Practice Forums (BPFs), and national and regional IGF initiatives (NRIs) continued to hold meetings on the last day of IGF 2017.

In a collaborative session on barriers to Internet access, NRIs from Afghanistan, Colombia, Georgia, Malawi, Sri Lanka, Latin America and Caribbean, and West Africa discussed challenges and good practices in making the Internet available to those who do not yet have access. Insufficient infrastructures, lack of private investments, and high costs of access were some of the issues identified as causes of the existing digital divide. While governments develop policies to address these and others challenges, they have more chances to succeed if they also involve the private sector.

Policy approaches identified by the DC on Connecting the Unconnected included developing programmes aimed at encouraging young people to study technology topics, supporting community networks, promoting digital literacy, and developing clear regulations to encourage private investments. As the BPF on Local Content noted, the availability of local content, in local languages makes the Internet more relevant and attracts new users, especially in rural and developing areas. As the NRIs in China, Japan, Kenya, and the Netherlands explained, the deployment of Internet protocol version 6 (IPv6) is a prerequisite for access and growth, as more people and devices connect to the Internet.

In their joint session, IGF initiatives in Brazil and Panama and Youth LAC IGF discussed issues related to data protection and data retention, converging on points: (1) the processes of developing regulations over personal data collection, processing, and retention should be transparent and inclusive; and (2) more awareness can help people better understand the need for protecting their privacy and personal data.

Privacy issues were also the focus of the DC on Publicness, which raised a few questions: While privacy is a relevant topic in the digital era, what is it that we really want to protect, to what extent, and what is the border between private and public spaces in the digitalised world?

The need to strengthen youth participation in Internet governance processes, at global, regional, and national levels, was underlined by the Youth Coalition on Internet Governance.

## Our IGF 2017 reporting initiative: Under the bonnet

A team of 48 rapporteurs, 9 technical and social media gurus, 8 editors, and 4 designers is what it took for the GIP to successfully carry out another just-in-time reporting initiative. This year marked our third reporting initiative from the IGF.

We prided ourselves on publishing reports from most of the 200+ sessions within hours of the end of each of them. By the following morning, the *IGF Daily* – a daily newsletter published throughout the IGF and distributed at the Palais des Nations and online – summarised the discussions from the previous day.

We cannot be in more than one place at the same time (or at least, we can multitask only to a certain extent), but our rapporteurs can each report from parallel sessions. For every reporting initiative, therefore, our aim is simple: to help participants stay current with what is happening simultaneously.

At the same time, our initiative brings the discussions closer to local communities. By involving rapporteurs from so many different countries, the GIP is contributing to building the capacities of actors, and strengthening participation across local and global levels.

This final report rounds up what we believe are the issues that mattered most during this IGF. It is based on our session reports, and on the text analysis of IGF verbatim transcripts. While experts provide human reflections, text analysis provides a machine X-ray of the IGF debates.

The thematic summary is based on DiploFoundation's taxonomy of Internet governance issues, which is continuously being updated to reflect the shifts in policy. It is also the underlying structure of the *GIP Digital Watch* observatory, home to our reports and newsletters, and to continuous analysis of the developments in digital policy.

Follow the links in this report for additional resources, including the reports themselves. In 2018, we hope you can make dig.watch your one-stop-shop for all things digital policy.

**The IGF 2017 reporting initiative was supported by the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation.**

**Rapporteurs:**

Manyi Arrey, Radek Bejdák, Stephanie Borg Psaila, Natoya Cassius, Amrita Choudhury, Tamar Colodenco, Guilherme Cooper Vicente, Ana Maria Corrêa, Efrat Daskal, Foncham Doh, Noha Fathy, Carlos Guerrero, Su Sonia Herring, Ines Hfaiedh, Katharina Höne, Tereza Horejsova, Pavlina Ittelson, Sarah Kiden, Robert Kikonyogo, Krishna Kumar, Jovan Kurbalija, Nazgul Kurmanalieva, Shita Laksmi, Marco Lotti, Cláudio Lucena, Marília Maciel, Aida Mahmutović, Anju Mangal, Adriana Minović, Jana Mišić, David Morar, Grace Mutung'u, Michael Oghia, Clément Perarnaud, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, Mohit Saraswat, Nathalia Sautchuk Patrício, Ilona Stadnik, Kevon Swift, Noemi Szabo, Sorina Teleanu, Leila Ueberschlag, Arto Väisänen, Pedro Vilela, Deirdre Williams, Bonface Witaba

**Contributors to this report:**

Stephanie Borg Psaila, Katharina Höne, Adriana Minović, Aye Mya Nyein, Virginia Paque, Barbara Rosen Jacobson, Jovan Kurbalija, Vladimir Radunović, Sorina Teleanu.

### Art in times of digital uncertainty

Art is known to flourish during times of uncertainty, when core ethical issues are open. This year, Diplo, the IGF Secretariat, HEAD and the Geneva Internet Platform organised Art@IGF, an exhibition, curated by Diplo's Darija Medic which invited IGF participants to step away from routine discussions and reflect on the broader issues of society. Digital artists displayed installations depicting core issues related to security, privacy and data protection, sociocultural, infrastructure, and more.

*Credit: Aleksandra Virijević*