#IGF2019
#DWreports

FINAL REPORT FROM THE 14th INTERNET GOVERNANCE FORUM

dig.watch/igf2019

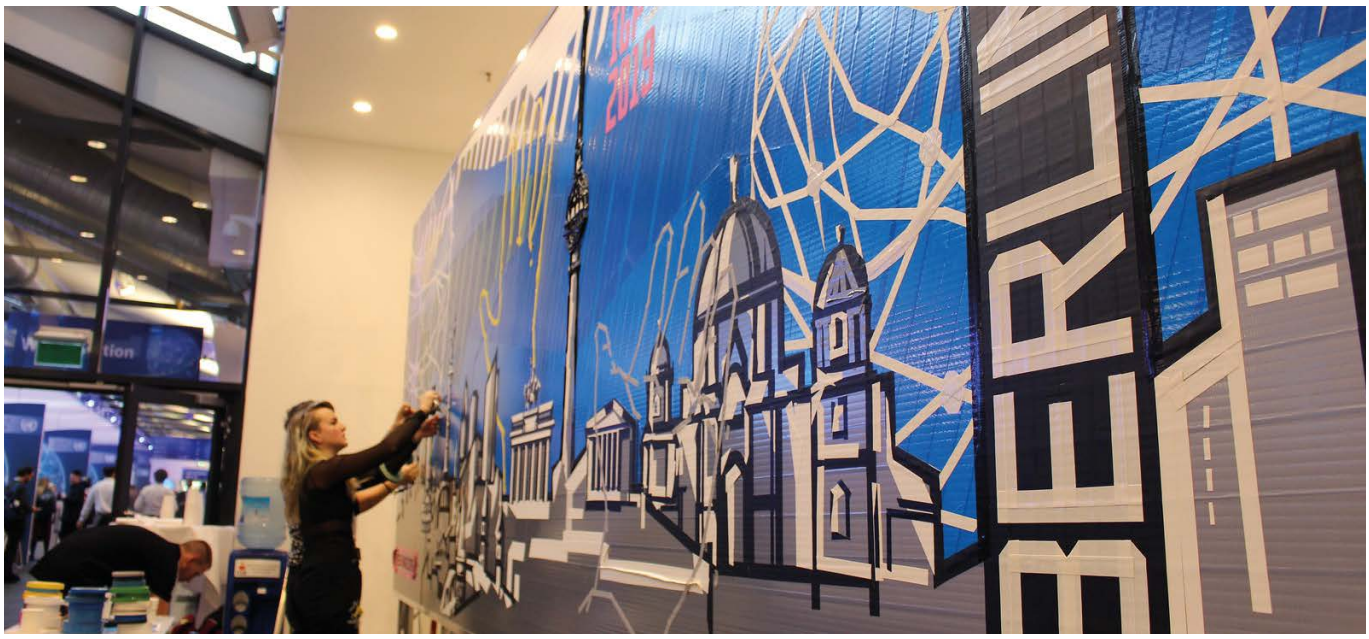
Published on Friday, 6th December 2019

Commentary: Reflecting on IGF 2019

In Berlin, the 14th Internet Governance Forum (IGF) reached a new level with a record number of participants and a dynamic programme. The parliamentarian track enriched stakeholder diversity. Remarkable hospitality with spacious facilities, advanced conference technology, coffee corners, and cultural programmes added to the smooth dynamics and a welcoming experience at the IGF.

Many policy discussions matured. On data, the dialogue moved from general notions that 'data is the oil of the economy' to detailed reflections on the responsibilities of companies, countries, and citizens in governing data. On cybersecurity, concrete norms for protecting critical infrastructure were analysed and advanced. On digital inclusion, discussions on enabling technical access 'to cables' was complemented by an emphasis on financial inclusion, language diversity, and education as ways to facilitate meaningful digital inclusion.

Continued on page 2



Art and Internet governance at the IGF 2019

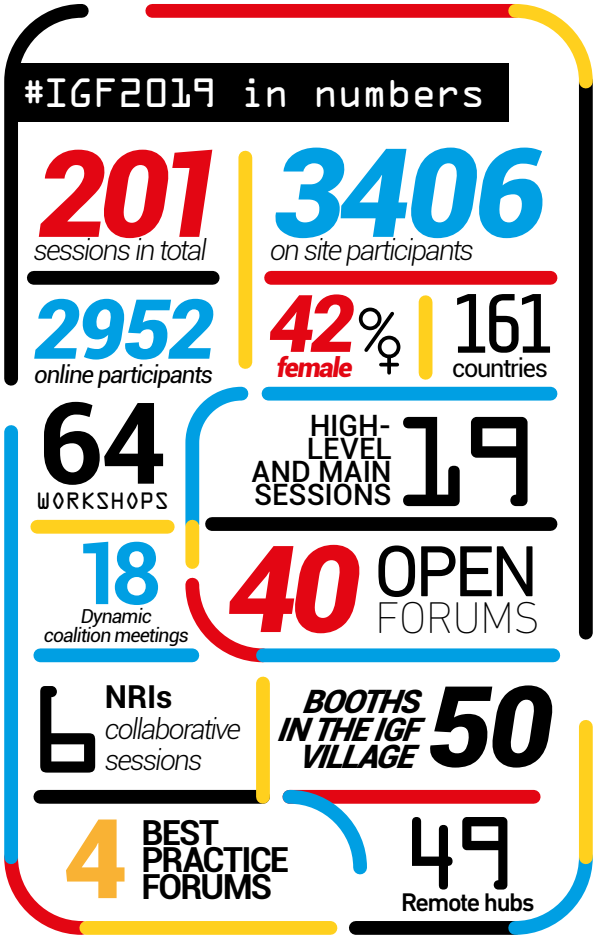
In this issue

The Final Report is published by the Geneva Internet Platform (GIP) and DiploFoundation, with the support of the IGF 2019 host country, the Swiss authorities, the Internet Society, and ICANN.

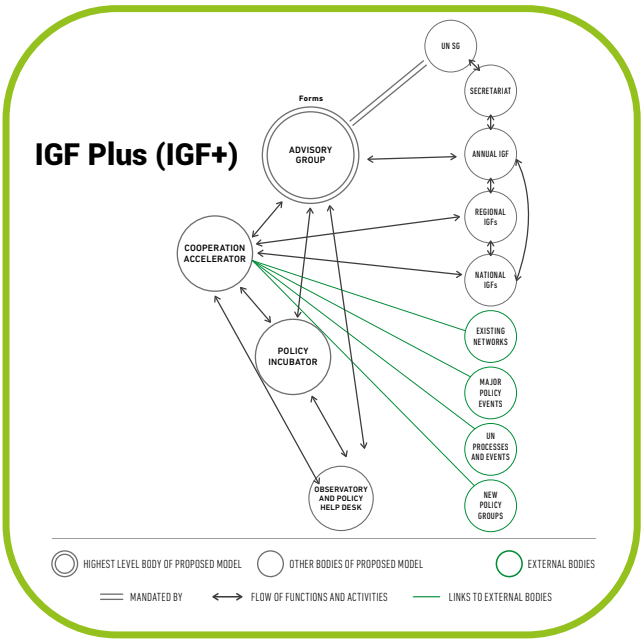
Continued from page 1

This edition of the IGF closed the 'survival phase' of the forum which started in 2017 in Geneva, when Switzerland stepped in to host the annual meeting as there was no interest by other countries. In Paris, in 2018, the first in situ address by the UN Secretary-General in the history of the IGF signalled a new relevance of the IGF for UN and digital cooperation. Even the fact that more countries now line up as potential hosts of the IGF demonstrates that the forum is past its 'survival phase' and has now entered a 'relevance phase'. This new phase should help the IGF evolve as a policy space that responds to digital challenges in agile, effective, and impactful ways.

Paradoxically, the very success of IGF 2019 made its structural weaknesses even more obvious. For many participants, the IGF discussions were not as up-to-date as the digital challenges of our era require. For example, the issue of the sale of .ORG registry was prominent in global media but not in the IGF programme. Were it not for Access Now's town hall meeting, this issue would have been completely left out of the IGF agenda. With a bit of agility, the IGF could have provided a venue for voicing different views and positions on the .ORG issue.



Growing pressure for digital solutions triggered new calls for policy actions. The Contract for the Web and the Digital Manifesto called for a more balanced, inclusive, and fairer digital world. The number of calls for digital solutions will likely increase. It remains to be seen who, where, and how these calls will be answered. The IGF has the potential to become a space where citizens, companies, and countries can find digital policy answers, or at the very least start searching for them. This potential was outlined in the UN High-level Panel proposal for the establishment of the IGF Plus, as a solution for the governance challenges ahead of us.



In Berlin, the IGF Plus was mentioned in discussions more than 60 times, as a way to build on the achievements of the current IGF while initiating changes within the existing policy mandate given to the UN Secretary-General by the World Summit on the Information Society's Tunis Agenda (article 72). Upcoming policy consultations should answer some of the most pertinent questions: Can the IGF become a digital home for humanity? Can it be the place where the ever-growing number of digital policy issues are addressed? How can the multistakeholder vibrancy of the IGF be preserved while producing more tangible outputs, including concrete policy recommendations?

Between Berlin and Katowice, the host city of the next IGF in November 2020, it will be a very busy year in the realm of digital policy. One of the year's main events will be the UN General Assembly 75th Anniversary meeting, where digital co-operation is likely to feature prominently. The main challenge ahead of us is to ensure 'One Internet', as UN Secretary-General Gueterres called for during his speech at the opening session of IGF 2019.

Stakeholder group representation

Civil society		Government		Intergovernmental organisations		Private sector		Technical community		Press / media	
2019	2018	2019	2018	2019	2018	2019	2018	2019	2018	2019	2018
41%	**45%**	**20%**	16%	6%	**7%**	19%	**20%**	**12%**	11%	**2%**	1%

An encouraging trend this year is the increase in governments' participation, which had been steadily dwindling in the past years. The 4% increase for this stakeholder group also accounts for the presence of parliamentarians (2% of participants at IGF 2019).

Parliamentarians at IGF 2019

This year, significant efforts were made to bring members of national parliaments (MPs) to the IGF. Direct invitations sent from the German Parliament to other parliaments around the world, as well as the allocation of financial support to MPs from the global south, led to almost 100 MPs from 56 countries being present in Berlin.

They not only attended the meeting, but also had a dedicated main session as part of the official programme. Their discussions resulted in a formal document which recognises the responsibility of MPs in 'creating regulatory frameworks for the next generation of Internet governance which will help to keep cyberspace free, open stable, unfragmented, and innovative'.

The document agreed upon by MPs also outlines a series of recommendations for national parliaments, which are encouraged to:

- Strengthen co-operation and the exchange of best practices in dealing with Internet-related issues.
- Guarantee that human rights and fundamental freedoms are upheld in the context of any legislation focused on 'enhancing national security in cyberspace and promoting the national digital economy'.
- Reconsider legislation to adjust it to the challenges of the digital age.
- Involve other actors in open consultation processes on draft legislation, and promote a multistakeholder approach to Internet governance.

MPs also intend to create an informal parliamentary IGF Group, dedicated to 'strengthening and expanding the parliamentary dialogue at the IGF'. This is an encouraging sign, considering that MPs are the ones drafting and passing laws dealing with Internet and digital policy issues; it is thus essential that they are part of the global discussions on such issues.

TRENDS

This year's IGF focused on three main themes: data governance; digital inclusion; and safety, security, stability and resilience. What were the latest trends, or new discussions, that emerged for each of these themes?

Data governance: The emergence of the 'data sharing' dimension

Over the years, discussions on data governance have been quite polarised. Some see data as essential for economic development and growth, and advocate for the free flow of data. Others are more concerned with issues such as safety, security, and the ability of authorities to access the data they need; those at this end of the spectrum favour data localisation rules that require data to be stored on local servers.

A third dimension has started to emerge that relates to data sharing. It boils down to a simple question: Which data can (or should) be shared? At this year's IGF, several discussions referred to this new dimension.

The concept of data sharing brings with it the potential for the debate on data governance to become a little less polarised. It starts from the assumption that different types of data require different treatments and protections. Both sides could find themselves agreeing that, for instance, sensitive data such as medical or financial data is best stored locally. Or that the sharing of certain sets of data, such as traffic data, is in the public interest.

The pitfall is that unless we have full clarity on what type of data we are referring to, the question of data sharing will not lead us far. This spells the need for a data taxonomy: We must differentiate and list categories of data, and determine what level of safeguards this data is currently afforded in different countries and regions.

It is only when a data taxonomy is developed that data sharing discussions can achieve their potential as tangible solutions for our data governance dilemmas.

Digital inclusion: More than access to networks

For a long time, digital inclusion debates focused mainly on access to networks. While without technical connection we cannot be online, benefiting fully from digital opportunities requires much more. The discussions at the IGF in Berlin made an important step in addressing digital inclusion in a holistic way.

Main pillars for digital inclusion can be found throughout IGF sessions and discussions on community networks, public-private partnerships, and financial incentives for infrastructure deployment education, financial inclusion, gender equality, online use of local languages and scripts, to name a few discussion threads. In the coming years, digital inclusion will acquire new dimensions, as more emphasis will be put on the development and use of AI tools.

Digital inclusion should remain high on the agenda of the IGF and global debates, since it is and will continue to impact equality and social cohesion, access to justice, and fairness in modern society.

Cybersecurity: Centrality of cyber norms

Last year, a number of initiatives related to cybernorms emerged in November, at around the same time as IGF 2018. Debates focused more on the role of the private sector rather than on state behaviour in cyberspace.

Among the initiatives were two resolutions: One called for a new Open-Ended Working Group (OEWG) and the other for the establishment of a new Group of Governmental Experts (GGE) – both of which would focus on the development and implementation of cybernorms. Since then, both groups have started their work, and are meeting in early December in New York: the OEWG multi-stakeholder informal consultations are on 2–4 December; the UN GGE's informal consultations for non-members, followed by its first substantive session, are on 5–6 December.

This is perhaps the reason why cybernorms dominated the cybersecurity discussions at IGF 2019 (read more in our Thematic Summary). Cybernorm issues such as the applicability of international law to cyberspace, the implementation of existing norms, and the new cybersecurity convention proposed by Russia, will remain in focus during this week's discussions in New York.

AI generates take-away message on AI governance

IQ'whalo, a former coffee-maker, now offers expert analysis on AI and policy as a full-time job. How did IQ'whalo interpret IGF 2019 through official session transcripts?

IQ'whalo analysed over 200 session transcripts from this year's IGF. Here is his take-away message on AI:

> *'If we talk about the future of artificial intelligence, then we're looking at a future of artificial bias. There are two aspects to this. The one is that we know that AI systems have no control over their data, that they are biased against specific groups and then the other aspect of the issue is that AI systems, unlike humans, do not have control.'*

While IQ'whalo continues to develop his techniques, we ask ourselves: Should we entrust IQ'whalo to summarise next year's discussions at IGF 2020?

IQ'whalo is the creation of Prof. Vladimir Veljašević from the Faculty of Fine Arts at the University of Belgrade, representing a non-anthropomorphised embodiment of AI. As part of humAInism project, IQ'whalo uses an open-source AI platform to generate synthetic text based on policy papers and transcripts, and was also a participant during this year's main session on AI.

IQ'whalo is an artifact from Diplo's humAInism project which aims to test if AI can help humans draft a social contract for the AI era. humAInism addresses this challenge by relying on two main pillars:

- The use of AI as a tool for managing the complexity of AI policies
- Feeding AI with as much human knowledge as possible and see what AI will suggest as guidelines or 'a new social contract' for the digital age

Summarising the IGF: The main discussions

This thematic summary highlights the main discussions during this year's IGF, based on the Digital Watch taxonomy.

TECHNOLOGY AND INFRASTRUCTURE

Towards a trustworthy AI that benefits all

The risk of AI-drive inequalities could be addressed by making AI systems trustworthy, reliable, and human-centric. Several other approaches can address this risk as well, such as embedding principles of inclusivity, robustness, accountability, transparency and explainability in the design of AI systems, and making sure that existing human rights frameworks and ethical guidelines and principles are implemented in an efficient and harmonised manner.

These elements are essential in addressing challenges associated with algorithmic decision making, bias in AI systems, and the misuse of AI to spread disinformation or influence electoral processes. Other solutions include technical audits, impact assessments, and promoting more awareness among users.

Is self-regulation enough? Probably not; clear legal obligations would make companies more responsible. Regulations should also take into account the need to protect human rights.

AI advances should not lead to more inequalities; the benefits of this technology should be equitably distributed. We cannot allow AI to be the driver of yet another form of digital divide. Developed countries, international organisations, and even tech companies have a responsibility in empowering developing countries to benefit from AI. Measures include support in developing national AI strategies, capacity development programmes, and initiatives focused on making sure that AI systems also embody characteristics and perspectives from developing countries. Protecting children's rights in the context of AI and tackling gender bias should also reduce AI-driven inequalities.

Strengthening the Internet's underlying infrastructure

Infrastructural issues – from fibre optics to 5G and the Domain Name System (DNS) – remain high on digital agenda.

The expansion of the DNS – with new generic top-level domains (gTLDs) and Internationalised Domain Names (IDNs) – was meant to make the Internet more inclusive. But the reality tells us something else, as universal acceptance (UA) remains a challenge. Many browsers do not recognise IDNs or gTLDs with more than three letters. And little progress has been made in achieving email address internationalisation. ICANN, tech companies, and governments have a role to play in promoting and supporting UA.

Let us not forget about Internet protocols. If we want one single network, our final objective should be an IPv6-only Internet, which is more stable, robust, and secure. Training and financial resources for network operators, and governmental policies can encourage the transition.

And there is one more element to consider: making sure that security standards and protocols are deployed to protect the robustness of the core Internet infrastructure.

Advanced technologies: Keeping up with the growth

The fast growth of digital technologies needs to be managed with caution. As the number of IoT devices continues to grow, so do privacy, security, and even human safety challenges. Addressing them requires a combination of measures: implementation of technical standards and security practices by tech companies, local and global regulatory efforts, and more education for end-users.

5G is seen by many as a revolution, as it promises faster speeds, lower latency and other characteristics to enhance the user experience. To encourage the deployment of 5G, significant investments and regulatory support – such as favourable spectrum policies – are needed.

CYBERSECURITY

Cyber-stability: Norms, responsible behaviour, and confidence building

Cyberspace is said to be stable when everyone can be reasonably confident in their ability to use it safely and securely. Cyber-stability requires shared responsibility between stakeholders, restraint by state and non-state actors from engaging in harmful actions, the avoidance of escalating tensions, and respect for human rights.

An emerging framework for responsible behaviour in cyberspace includes several voluntary norms and confidence-building measures. The concerns are that there may be duplication of effort among multiple forums, limited participation of some actors, and different understandings of key concepts. Even when norms are agreed, there is no institutional mechanism to monitor and report compliance, and hold states accountable.

There is general consensus that international law applies to the behaviour of states in cyberspace, although there are divergent positions on what this means in practice, and geopolitical tension that is widening the gap.

Confidence-building measures remain a low(er)-hanging fruit for achieving cyber-stability. They can help reduce misperceptions and de-escalate tensions, while fostering trust and co-operation. The private sector can contribute to increasing confidence as well, while civil society can help monitor and research compliance with agreed rules of the road.

Interdependence: The roles of various actors in securing cyberspace

Governments have an essential role in securing cyberspace due to their ability to adopt and implement laws and regulations. Equally important, they should engage more in partnerships with other actors to help shape policies, improve joint responses to incidents, build cybersecurity awareness and skills, and implement standards.

Tech companies should enhance vulnerability reporting practices and ensure their products and services are embedded with security standards. The technical community can enhance the security of Internet infrastructure – for instance, by transitioning to IPv6 and by addressing DNS-abuse practices – and provide expertise to governments. Civil society organisations can contribute to promoting cyber-hygiene among end-users, while also helping to shape public opinion. In addition, regional, international, and cross-stakeholder co-operation is key in fostering community building and problem-solving.

Staying safe: Human rights, ethics, trust, and digital literacy

How do we increase the level of safety and security in cyberspace? Digital literacy programmes can help individuals better understand the digital age, along with associated cyber risks and protective measures, such as encryption tools. Tech companies should abide by human rights and ethics principles when designing and making services available. Governments can also help, for example, by issuing labels and certificates for digitally enabled technologies and products to reassure consumers that they are safe.

HUMAN RIGHTS

Stronger youth voices

Despite improvements in recent years, the voices of young people are still insufficiently heard in Internet governance and digital policy processes. The challenges include a lack of information and know-how, limited opportunities to become effectively engaged, and a lack of financial resources.

Simply giving youth a place to speak is not enough. Young people need to be encouraged and empowered to voice their opinions, speak in favour of their rights, and actively contribute in discussions and developing solutions. Other actors have a responsibility to meaningfully involve young people and children from all over the world in policy-making processes. This year's Youth IGF Summit and the Youth Coalition on Internet Governance are positive steps in this regard.

Upholding children's rights

With so many children making use of the Internet – 1 in 3 Internet users in the developed world, and 1 in 2 globally, are children – the main issue surrounding children's rights in the digital age is how to interpret and uphold such rights, which are enshrined in the Convention on the Rights of the Child.

The General Comment to the convention, which is being drafted by the UN Committee on the Rights of the Child in consultation with stakeholders refocused the debate even at the IGF. This marks significant progress in a process that was kickstarted by several landmark studies that highlighted the applicability of children's rights in the digital environment. This debate will continue in March 2020, when the draft is released for public comment.

For children, the Internet is a 'natural' way of communication, entertainment, and education. Given their young age, though, they often have difficulties in understanding rules and policies related to their rights, especially when it comes to privacy issues associated with online services. They also face risks when it comes to cyberbullying, child exploitation, and the dangers of online gaming.

Despite many existing efforts, more needs to be done to empower children to exercise their digital rights, including privacy, freedom of expression, and access to information. Even more efforts are needed to keep children safe online. Solutions could include digital literacy and education programmes designed to develop not only digital skills but also qualities such as tolerance and empathy; more technical tools such as parental control software or apps for reporting rights violations; and strengthened policies and legislation to protect minors.

Protecting the rights of vulnerable groups

Persons with disabilities, women, and gender minorities deserve more attention from companies and regulators alike.

'If for most people technology makes things easier, for people with disabilities, technology makes things possible.' This reflects the importance of assistive technologies designed to empower people with disabilities to enjoy their rights in the digital era. Accordingly, the tech sector needs to do more to respond to the challenges of disabled people. The ongoing work on digital inclusion is an indication that some people are still being excluded. While many policies for disability access address auditory, visual, and sometimes mobility issues, solutions for cognitive and learning disabilities are still not being explored as needed.

Addressing gender discrimination and gender-based violence online is another area that requires more effort. Part of the solution includes: helping girls and women gain equal access to skills and opportunities online and in the tech industry, legislation to protect women and gender minorities and end online sexism, and paying a closer look at potential biases in algorithms. We also need to change our approach to policy-making and focus more on preventing gender discrimination, rather than just responding to cases after they happen.

LEGAL AND REGULATORY

The need for regulation in cyberspace

There seems to be more agreement than ever that cyberspace does need more regulation. The question is not whether, but rather how to regulate.

Calls for regulation span across multiple Internet policy issues. Countries are adopting data regulations covering privacy and data protection rules, but also reflecting national realities and priorities. Such regulations should be drafted with care, not to impose unjustified barriers to trade and free flow of data.

Tighter regulations could also help address the challenges of illegal content online, especially when relf-regulatory measures are not working. Regulations should also further encourage the growth of the digital economy, keeping in check the risks of over-regulation needs as companies try out new business models.

While regulations may contribute to a sustainable, safe and secure cyberspace, they must be handled with care. Balancing the rights and interests of different actors, respecting democracies' institutional boundaries and legal frameworks, and allowing all relevant actors to contribute to policy-making processes should be key in all regulatory approaches.

Preventing (more) fragmentation in the digital space

Although the Internet is a trans-border network, most Internet regulations are national. Sometimes, this results in conflicting requirements that make it difficult for service providers to operate across borders. The issue is particularly acute in data governance, where different data regimes are likely to trigger the fragmentation of the digital space.

These challenges may be addressed through more interoperability and harmonisation between national legal and regulatory frameworks, which is arguably more difficult when countries have conflicting interests.

It is encouraging, however, that several countries have started engaging in initiatives which avoid digital fragmentation, by agreeing to cooperate on data governance issues and promoting more harmonised rules. Examples include initiatives by G8 and BRICS (Brazil, Russia, India, China, and South Africa) countries.

Regulations for new and advanced technologies

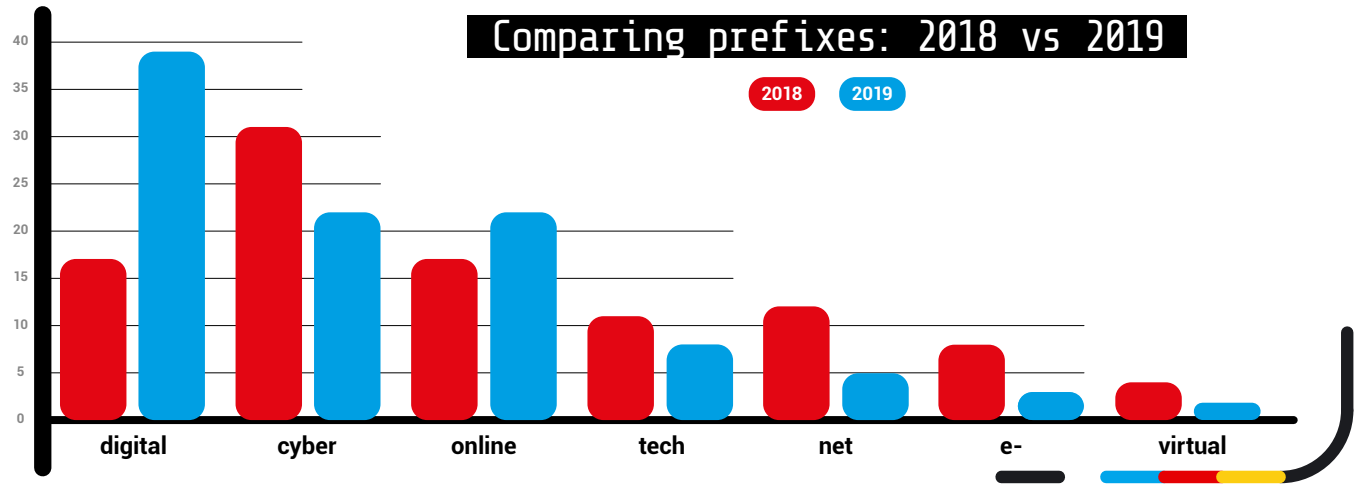
With advancements in technologies such as blockchain, AI, and IoT, regulatory actions may also be required to protect human rights and safeguard democratic principles.

Prefix monitor: The rise of 'digital'

The use of prefixes in digital policy is indicative of the trends and developments in the field. For the six main prefixes, their prominence reflects the position and nuances that actors take in relation to a particular issue.

This year, the prefix 'digital' dominated IGF language, and exceeded 'cyber' and 'online' – prefixes usually associated with security-related issues and human rights. The noticeable growth in the usage of 'digital' could be explained by the impact of the Report of the UN Secretary-General's High-level Panel on Digital Cooperation, which was referenced in many IGF discussions.

'Cyber' and 'online', prefixes that are largely used for cybercrime/cybersecurity and human rights, were on par this year. The use of 'tech' remained fairly low, which is not surprising, considering that it emerged in digital parlance only last year, and has since been reserved mainly as a reference to platforms or to Internet companies. The relative decline of other prefixes indicates that policy jargon is losing the finer nuances related to the use of 'net', 'e-', and 'virtual'.



5G technology needs regulatory support to be deployed, and to address security concerns; frameworks for distributed ledger technologies are already under discussion, especially in Europe, which aim to tackle data protection, accountability, and taxation issues, among others. Regulations in the field of AI need to address challenges related to algorithmic decision-making (and its role in influencing people's choices, for example), the use of facial recognition technologies, or systems that pose a threat to human life, such as lethal autonomous weapons. Such regulations need to be strongly anchored into human rights frameworks.

Regulations, which can provide more legal certainty for business worldwide, need to be kept as flexible and as technically-neutral as possible: technology evolves fast, and legal frameworks become outdated just as fast.

DEVELOPMENT

Improving access and inclusion for sustainable development

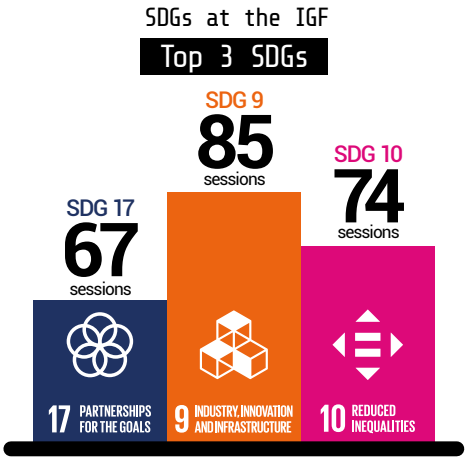
We have heard it time and time again: The Internet can be a tool in achieving sustainable development. Ensuring that this happens requires respect for societal values and adapting technology to our society (and not the other way around).

It all starts with increasing connectivity and making sure that the right infrastructure is in place to support meaningful access. Solutions include community networks, public-private partnerships, and financial incentives for infrastructure deployment. For particular cases such as small island developing states, context-specific solutions are required, such as more investments in submarine cables and satellites. When the infrastructure is in place, ensuring that older technologies are replaced in a timely manner is essential to avoid new gaps in connectivity.

Digital inclusion means more than just providing an Internet connection. It is also about affordable access, the ability to use the Internet in local languages and scripts, addressing gender inequalities, and enhancing access for people with special needs. Digital inclusion also requires helping people utilise the Internet in ways that best address their needs (e.g. for education, economic opportunities, etc.).

Role of data in attaining the SDGs

Data, and big data in particular, are powerful tools for the promotion of economic growth and the well-being of citizens. Data-sharing principles can leverage the role of data for development: openness, interoperability, accessibility. Access to data should be equitable; if adequately justified,



SDGs at the IGF

The Internet, AI, and big data can help alleviate poverty, improve the quality of education, combat hunger, and achieve other SDGs.

At this year's IGF, a total of 122 sessions were dedicated to at least one of the 17 SDGs. The largest number of sessions (85) were dedicated to Goal 9 – Industries, innovation and infrastructure. This should come as no surprise, given that Target area 9c specifically refers to access to ICTs and the Internet. SDG 10 – Reduced Inequality and SDG 17 – Partnerships to achieve the goals appear in 74 and 67 sessions, respectively.

accessibility may be time bound. If these principles are applied, data can have a more powerful role in the design of beneficial products and services, as well as in human-centric information policies and regulations.

Data processing and big data analytics are also essential for monitoring progress in achieving the SDGs and in identifying areas where more action is needed. Training more data scientists and enhancing data skills among individuals can help us tap into the potential of data. Partnerships between different stakeholders and between developing and developed countries are also important.

Digital education and capacity building

Capacity development remains a key enabler of digital inclusion and overall digital growth. Capacity development starts with basic ICT literacy that helps people use digital devices, and continues with broader digital skills that empower people to meaningfully use technology (where to look for information, how to stay safe online, etc.).

Schools need to focus more on developing digital skills as part of their educational curricula. It should also be an integral element of informal and life-long learning education programmes designed for adults and the elderly.

Digital education should go beyond Internet-related issues. It needs to cover the fast evolving digital technologies, such as AI and big data. Current and future workforces need to constantly acquire new skills (digital, interdisciplinary, and soft skills alike) so they can effectively adapt to the changing digital economy.

Developing countries also need more support in keeping up with technological progress. This can include assistance for developing national AI strategies, and capacity development opportunities so individuals can use AI and other advanced technologies for good.

ECONOMIC

Cross-border data flows and data governance

Given the impact of data flows on economic growth and digital trade, data localisation policies should be carefully considered. Some see data localisation rules as economic barriers. Other focus on data localisation as a way of protecting the privacy of citizens and ensuring the security of data.

There is still divergence on whether data flows should be part of international trade discussions. For some, it is inevitable that trade discussions touch on data governance issues, as the free flow of data enables commerce. But data governance frameworks also have human rights implications, so agreeing on them cannot be only a matter of trade negotiations; other actors should be involved as well. Given the wide diversity of national approaches, views, and goals, it may be hard to achieve a universal agreement to regulate the free flow of data.

Some regional trade agreements already incorporate data governance provisions, covering issues such as privacy, data protection, and the obligation for countries to allow cross-border transfers of data. Several challenges come from the fact that data governance rules set by developed countries tend to become de-facto standards worldwide.

While we can spend time discussing which is the appropriate venue for data governance, this should not derail the core of the debate on data standards and regulations: how to reconcile the rights of citizens and the interests of businesses.

Benefits and challenges that the digital economy presents to SMEs

For small and medium-sized enterprises (SMEs) the Internet and digital technologies facilitate access to new customers, make operations more efficient, and allow the development of new products and services. To enjoy these benefits, they need an enabling infrastructure in place: connectivity, cloud computing, e-payment services, etc.

A stable regulatory environment, access to financing, tax rules that favour investments, and simplified governmental procedures (e.g. for authorisations and permits) can help SMEs thrive. The position of SMEs is also impacted by other regulations such as immigration laws that provide access to digital talents, and by educational systems that foster creative thinking and entrepreneurial spirit. Initiatives focused on empowering SMEs to engage in digital marketplaces are also useful.

When it comes to operating on international markets, SMEs are often challenged by having to comply with different and sometimes conflicting regulations on issues such as privacy and consumer protection. This means additional operations costs, which are a barrier to cross-border trade.

Openness and a way to stimulate competition and economic growth

The Internet was built on free and open standards, which allowed startups to thrive and the digital economy to grow. Currently, proprietary standards are proliferating, threatening openness – which can facilitate economic growth – and innovation. Open standards and open data enable the development of new online services, and support new business models, such as the sharing economy.

Openness also relates to the regulatory environment. Flexible regulations enable the growth of the digital economy by allowing companies to test innovative business models. For example, data governance rules that facilitate data sharing and the use of open data foster interoperability, expand consumer choice, and, ultimately, support competition.

SOCIOCULTURAL

Tackling harmful content: Between self-regulation and hard law

Tech companies are under increased pressure to come up with new solutions to curb the spread of harmful content. Their responses include more stringent content policies, adherence to codes of conduct proposed by regulators, and collaborative initiatives such as the Global Internet Forum to Counter Terrorism. Technical measures – such as using algorithms to identify and remove harmful content or blocking access to content at the DNS level – are also increasingly used. But they come with risks and limitations: Can algorithms be trusted to distinguish hate speech from legitimate content? How effective is it to block access to a certain resource, if the content hosted there can easily be moved to another location?

If self-regulatory measures are not working, governments are undoubtedly ready to step in with hard regulation. This could be helpful if it brings clarity to what harmful content is and what roles and responsibilities stakeholders have. But it can also lead to censorship and violations of freedom of expression and privacy. Achieving a balance is not an easy task.

Fighting misinformation and protecting democractic values

Misinformation is not a new phenomenon; recently, it has been amplified by the Internet. Fake news and deepfakes easily spread via social media platforms and can influence electoral choices, manipulate divisive domestic debates, and undermine trust in democractic processes.

Transparency practices, fact-checking activities, and awareness-raising efforts are among the measures adopted by tech companies to fight disinformation. Some governments argue these are not enough. To avoid tighter regulations, companies are stepping up their self-regulatory approaches, generating new controversies in the process. Was Twitter right to ban (almost) all political adverts? Or is Google's decision to only limit adverts to those which use general data to target audiences more appropriate? It is difficult to say until we see the effects of these measures.

Fighting disinformation can create collateral risks for online freedoms. Risks can be addressed by developing carefully balanced policy frameworks, benchmarking, and due processes for dealing with problematic content. Media literacy remains the approach preferred by many for strengthening the resistance of Internet users against misinformation.

The future of digital governance and cooperation

Many discussions at this year's IGF revolved around digital cooperation, following the release of the report of the UN Secretary General's High-level Panel on Digital Cooperation. The message was clear: International and cross-stakeholder cooperation is essential for enjoying the benefits of digitalisation, while also managing the associated risks and challenges.

There are many steps that should be taken. Strengthening digital cooperation requires that all interested actors should be given an opportunity to contribute to discussions and policy-making processes. This includes new voices such as specialists in humanist sciences, marginalised groups, and religious minorities. More parliamentarians need to be engaged in global debates, as the messages from the parliamentarians' meeting in Berlin called for.

The IGF Plus proposal provides a framework for strengthening the IGF, by accommodating the concerns and interests of various stakeholders, and identifying actionable policy solutions.

More effective digital cooperation could also help avoid the fragmentation of the Internet that could be triggered by divergent rules and regulations imposed by countries on issues such as privacy, data flows, and cybersecurity.

BERLIN MESSAGES:
Takeaways from IGF 2019's main themes

Continuing a tradition that started at IGF 2017 in Geneva, the discussions held throughout the week were summarised in a set of *Berlin IGF Messages*. They reflect the chief issues around the three main themes of this year's IGF: data governance; digital inclusion; and safety, security, stability, and resilience.

Published on the IGF website, these messages are not yet final: they can be further updated over the coming weeks, pending possible comments from the community. A final version is expected to be published three weeks after the IGF.

Host government outputs

A few additional outputs have been produced under the coordination of the host country as a result of specific events and processes organised in the framework of IGF 2019.

- Chairman's Summary of the High Level Internet Governance Exchange
- Elements of SME Charter
- Jimmy Schulz Call – Messages from the Meeting of Parliamentarians

Launched: Reports and studies

At IGF 2019, several policy initiatives, reports, and publications were launched or used as background material for discussions.

The Age of Digital Interdependence
(UN Secretary-General's High-level Panel on Digital Cooperation)

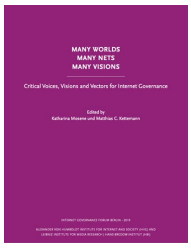
Report | *IGF session*

Contract for the Web
(World Wide Web Foundation)

Contract | *IGF session*

Digital Justice Manifesto: A Call to Own Our Digital Future (Just Net Coalition)

Manifesto | *IGF session*



Many Worlds, Many Nets, Many Visions
(Mosene, K. & Kettemann, M.C. (Eds.))

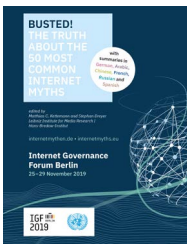
Publication | *IGF side-event*

Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s
(Kleinwachter, W., Kettemann, M.C., Senges, M., Mosene, K. (Eds.))

Publication | *IGF session*

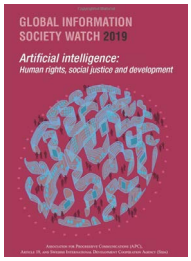
Internet & Jurisdiction Global Status Report
(Internet & Jurisdiction Policy Network)

Report | *IGF session*



Busted! The Truth about the 50 most Common Internet Myths
(Kettemann, M.C. & Dreyer, S. (Eds.))

Publication | *IGF session*



AI: Human Rights, Social Justice and Development
(Global Information Society Watch)

Publication | *IGF session*

IGF throughout the years: What was the focus on?

The IGF turned 14 this year. The Internet we knew in 2006, at the time of the first IGF meeting in Tunis, is not the Internet we know now. Each year, the forum has reflected on the policy issues of the moment, and the topics addressed have gained new dimensions as the Internet itself evolved.

Using the Digital Watch's taxonomy of issues, we can see how prominent the main Internet and digital policy topics were at each IGF meeting, and highlight the changing priorities.

The development basket – covering issues such as access, the digital divide, and capacity development – was among the most prominent across every IGF, and the most dominant for eight consecutive years. With issues such as content policy, cultural diversity, and multilingualism, the sociocultural baske was prominent in the first couple of years, and then again since last year as a result of growing concerns over the spread of hateful content.

The technology and infrastructure basket prevailed in both 2018 and 2019. It is not surprising, considering that discussions around AI, IoT devices, and blockchain gained prominence in recent years in most digital policy spaces. The cybersecurity basket, covering issues related to network security, cybercrime, cyberconflict, and child safety online, has dominated a significant number of IGF sessions lately, becoming the second most dominant basket in 2019.

The presence of human-rights-related issues at IGF meetings remained largely constant over the years. Issues under the economic basket (including e-commerce, taxation, future of work) – absent during the first three IGFs – tend to be less reflected in IGF discussions consistently *(see Commentary section)*. Legal and regulatory issues (jurisdiction, intellectual property rights, etc.) – covered very little during the first four IGFs – gained prominence in recent years.

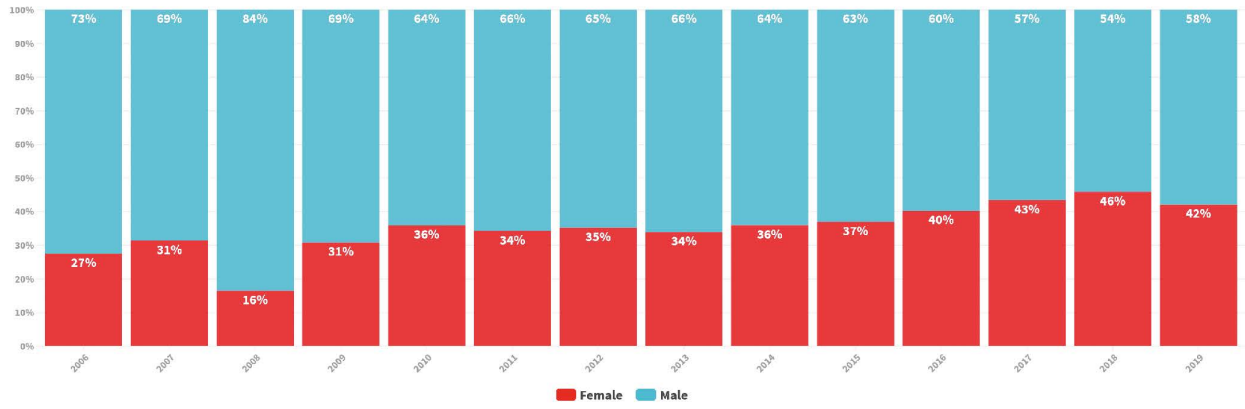
For the first time this year, discussions were much more evenly distributed. In light of so many developments in AI, IoT, and other emerging technologies, such an even distribution may be hanging in the balance.

Baskets trend per year

2006-2019

Female vs Male participants trend

2006-2019



The ten most dominant issues at IGF 2019

Using automated text analysis software, Diplo's Data Team analysed the raw transcripts from 165 sessions captured from real-time captioning. These were then processed using a custom digital policy dictionary.

The results of this analysis shows that the most prominent issue at this year's IGF was trust, ethics and interdisciplinary approaches, followed by data governance and sustainable development. Aside from tackling AI as a technological development, recent months have seen the world more concerned about ethical and trust issues, with questions such as How can trust be restored in technology? How will AI shape the future of humanity? *(Watch our video interviews with key experts.)*

Compared to 2017 and 2018, there was a slight increase in the number of sessions dedicated to AI. This pushed AI to sixth place on the list, after network security and capacity development.

TOP 10 ISSUES

TRUST, ETHICS, AND INTERDISCIPLINARY APPROACHES
DATA GOVERNANCE
SUSTAINABLE DEVELOPMENT
NETWORK SECURITY
Capacity development
Artificial intelligence
Telecommunications infrastructure
Cybercrime
Cyberconflict and warfare
Privacy and data protection

Social media monitor

IGF 2019 reached 180 million social media users since the beginning of November. Addresses by UN Secretary-General António Guterres and German Chancellor Angela Merkel on Day 1 triggered a peak in social media traffic.

Most of the social media activities came from Germany, with 15.6% of all mentions, followed by the USA with 7.3%.

Brazil, France and the UK came in third, fourth, and fifth place respectively, each with a little over 3% of mentions. The monitoring was based on the official #IGF2019 hashtag and conducted on social networks including Twitter and Facebook, as well as on a number of websites and blogs.

Hashtags used during IGF 2019, extracted from 7.5K tweets

Social media stats

Reach: 182,4 M
Mentions: 17,9K
TOP COUNTRIES:
Germany (15,6%)
US (7,3%)
Brazil (3,5%)
France (3,3%)
UK (3,2%)

Towards IGF 2020

The next IGF will be hosted by Poland, in Katowice on 2–6 November 2020. The theme of the meeting will be *Internet United*, which according to the IGF's next host country, 'represents a real obligation and challenge for the whole Internet society'.

What can we expect until Katowice? With the support that the IGF Plus model received in Berlin, we might see more focused discussions on how and when to implement some of its elements, and perhaps even concrete action. Will IGF 2020 be an entirely new IGF? It all depends on the IGF's broad community, and how ready it is to bring change to this almost 15-year old initiative.

About the IGF Reporting

This Report is a summary of a comprehensive IGF reporting that includes reports from all sessions, preparation of IGF Daily Briefs, providing just-in-time updates via mobile apps, and conducting in-depth AI analysis of the IGF content.

You can explore session reports and layers of wealth of information on digital policy by clicking on the icon in the digital version of this Report or accessing the page https://dig.watch/igf2019.

Rapporteurs, contributors, and coordinators

Cedric Amon, Katarina Anđelković, Stephanie Borg Psaila, Amrita Choudhury,Jelena Dinčić, Andre Edwards, Noha Fathy, Andrijana Gavrilović, Stefania Grottola, Katharina Höne, Tereza Horejsova, Pavlina Ittelson, Arvin Kamberi, Sarah Kiden, Jovan Kurbalija, Marco Lotti, Dustin Loup, Marília Maciel, Aida Mahmutović, Dragana Markovski, Darija Medić, Jana Mišić, Nagisa Miyachi, Grace Mutung'u, Jacob Odame-Baiden, Virginia (Ginger) Paque, Clément Perarnaud, Nataša Perućica, Vladimir Radunović, Mili Semlani, Andrej Škrinjarić, Ilona Stadnik, Paula Szewach, Sorina Teleanu, Pedro Vilela, Bonface Witaba

Editing, design, and multimedia team

Maja Bačlić, Miodrag Badnjar, Jelena Dinčić, Nataša Grba Singh, Su Sonia Herring, Srđan Ivković, Arvin Kamberi, Anna Loup, Dragana Markovski, Darija Medić, Viktor Mijatović, Mina Mudrić, Mary Murphy, Dorijan Najdovski, Aleksandar Nedeljkov, Virginia Paque, Hannah Slavik, Steve Slavik, Vladimir Veljašević, Milica Virijević Konstantinović, Nemanja Vojvodić, NT Gruppen AS

Data and AI teams, technical and communications

Katarina Anđelković, Dylan Farrell, Aleksandar Firevski, Vladimir Ivaz, Jelena Jakovljević, Đorđe Jančić, Arvin Kamberi, Nikola Krstić, Svetislav Nedeljkov, Anamarija Pavlović, Nataša Perućica, Tanja Tatalović