IGF Summary / Published on 16 November 2015

IGF SUMMARY

JUST-IN-TIME REPORTING FROM THE 2015
INTERNET GOVERNANCE FORUM
dw.giplatform.org/igf

PUSHING THE BOUNDARIES AT IGF 2015

The 10th Internet Governance Forum (IGF) was held in João Pessoa, Brazil, on 10-13 November; in a month's time, the UNGA High-Level Meeting on WSIS+10 will decide on the future of the IGF. Although the continuation of the IGF is almost certain, there are many open questions about its future *modus operandus*. In this context, the IGF has had a very vibrant discussion on past and future developments.

The creation of the IGF at the World Summit on the Information Society (WSIS) in Tunis in 2005 pushed the boundaries of how the United Nations previously worked. When people attended the first IGF in Athens in 2006, they had no idea what to expect. They were a little bit defensive and a little bit suspicious as to whether this new type of meeting was needed or could achieve anything. Gradually, trust was built, new processes were introduced, and the IGF developed its unique profile in digital policy.

The past ten years of the IGF's existence have seen the rapid development of the Internet, from an academic network to a critical communication infrastructure of modern society. The number of Internet users increased, in particular in developing countries. And while in 2005, Facebook was still being developed in Zuckerberg's Harvard dormitory, and Twitter did not exist, the IGF was becoming the policy forum capable of dealing with issues which were arising during the most rapidly developing phase of the Internet. It would be too far-fetched to give credit for the Internet's fast growth to the IGF. However, the IGF did provide quite a few building blocks. If nothing else, the IGF has been the place where, through discussion and engagement, traditional geopolitical tensions have been diffused.

Today's digital world is different from the one in 2005, and is likely to be even more different from the digital world which will emerge in the next decade. From predominantly an academic network in 2005, the Internet has become a global critical infrastructure with high strategic, economic, and political relevance.

The IGF needs to adjust to a new reality in order to remain relevant. The multistakeholder approach, as a core IGF principle, is undergoing change. From a nominal and 'good to do' principle, it is becoming part of the *realpolitik*. Namely, it is very difficult to envisage effective digital policy on cybersecurity, human rights, and critical infrastructure without the involvement of every stakeholder – governments, business, academia, and civil society – in their respective roles and responsibilities.

Would the IGF be able to provide the adequate answers to, let's say, a minister from a small and developing country who is searching for digital policy solutions, for example, to introduce e-payment systems in his/her country, or to ensure the protection of critical infrastructure, or to many other issues?

Continued on page 2

PREFIX MONITOR

Cyber (security) and online (human rights) dominated IGF 2015 discussions. Digital (development) and net (technology) had lower prominance.

The percent of all characteristically prefixed terms in the IGF 2015 session transcripts compared against the baseline IGF 2006-2014 results.

IN THIS ISSUE

Anytime you see this icon, there is more background material in the digital version. Alternatively, visit **dw.giplatform.org/igf** for more in-depth information.

PUSHING THE BOUNDARIES AT IGF 2015

Continued from page 1

Not likely. It is unlikely that the minister would be able to find hes/her solution at the IGF – or any other venue – simply because these issues can be very complex. For example, enabling e-payments is a decision for private companies such as PayPal, albeit influenced by many public policy issues (the security of payment system, legal remedies, etc).

So what can the IGF do? The search for a place where the proverbial minister can find a digital policy solution could start with the IGF. Article 72 of the Tunis Agenda gives the IGF a broad enough mandate to coordinate activities and, where appropriate, issue policy recommendations.

And this is how the discussion in João Pessoa matured. The IGF community pushed itself further on one of the main critical points: a lack of tangible outcomes of the IGF. It embraced the outputs of the intersessional work which began shortly after the last IGF in Istanbul. Until very recently, the community has not felt it 'appropriate' for the IGF to develop recommendations as an official output. Reluctance to move in this direction stems from the specific nature of the IGF. The argument used to maintain the *status quo* has always been that recommendations require negotiations and that such formal negotiations could endanger the forum function of the IGF where information and ideas are exchanged freely and with little formality. Discussions took a new turn with the NETmundial meeting in 2014, when an outcome document was negotiated and agreed on in a multistakeholder setting.

This year's IGF considered six Best Practices documents, a number of Dynamic Coalition outputs, and one very detailed *Policy Options for Connecting the Next Billion* compilation consisting of over 80 contributions from national and regional IGFs as well as interested individuals and organisations. What was telling about the IGF community's attitude to these documents, unlike traditional intergovernmental negotiations over texts, was the desire to keep these outputs as living documents, to be updated on an ongoing basis in order to respond to changes in the Internet and in the larger world.

It is clear that over the past 10 years, not only has the IGF developed a vibrant community, it has started experimenting with new practices (such as 'lessons learned'). These can evolve into recommendations, which would be in line with Article 72 of the Tunis Agenda. The IGF tackles digital issues in a multidisciplinary way unlike many other digital specialised agencies organisations. Although much more needs to be done, when comparing the IGF to other policy spaces, we can conclude that the IGF is far ahead in addressing digital policy issues in multidisciplinary and comprehesive ways.

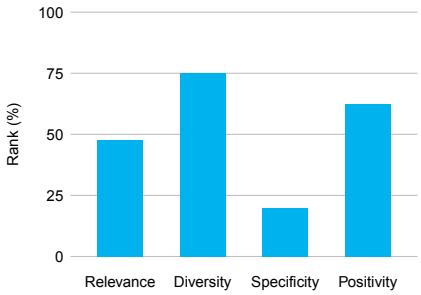
IGF SUMMARY REPORT IN THREE LAYERS

On the **1st layer** you can find summary text and click on an icon that will lead you to...

...the **2nd layer,** where you can find more detailed information, including session reports, graphics, and information about the various actors. Click on the icon to go to...

...the **3rd layer,** where you can find primary sources, transcripts, legal instruments, raw data, and statistics

SECURITY, ENCRYPTION, AND TRUST



IG Barometer Scores. The rank (%) of each score is computed relative to 40 IG issues from Diplo's IG Taxonomy. The analysis was performed on 147 session transcripts from IGF 2015. To learn more about the GIP IG Barometer scores, visit www.giplatform.org/barometer. The four IG Barometer scores are:

Relevance. The relevance score describes the relative importance of each IG issue in the IGF 2015 transcripts. This score is computed from two components: explicit relevance, which relies on the exact count of issue-specific keywords and phrases in the transcripts, and implicit relevance, which is based on the presence of terms related to the issue-specific keywords in the transcripts. Thus the IG Barometer can 'sense' associations to a particular IG issue in the source documents even if issue-specific keywords and phrases are used less frequently or avoided altogether (e.g. mentioning Interpol implies cybercrime; mentioning zero-rating implies net neutrality).

Specificity. The most important words and phrases used in the debate on each IG issue are studied in respect to their overall frequencies of use. The more unique their usage in a particular IG issue relative to the whole IG debate, the more specific the language used to discuss the respective IG issue is considered to be. The specificity score describes the degree of linguistic, semantic specialisation of the debate in a particular IG issue.

Diversity. Imagine a debate in which all stakeholders use the same or similar terms in a more or less similar manner, and a parallel debate where one can detect two or more groups that differ in the way they make use of the most relevant words and phrases. While the later debate is considered to be diversified, the former is said to be less diversified. The diversity score measures the variation in the way the most specific IG relevant words and phrases are used to discuss a particular IG issue. Diversity often follows professional diversity (e.g. a discussion on cybersecurity involving security, human rights, and technical communities would likely have high diversity).

Positivity. Sentiment analysis is a psychologically-based automated method of considering the presence of emotionally charged words in a collection of text documents to estimate the overall affective tone of the discourse. The positivity score indicates the degree to which the debate in question is charged with more positive emotions.

With a rise in cybercrime and a sharper focus on cybersecurity by policymakers worldwide, it is no surprise that the issue was discussed at great length last week.

Cyberattacks, which are on the rise and are evolving with the growth in infrastructure, mobile money transfers, and social media, affect the economic growth and sustainable development of many countries. The real economic cost of cyberattacks is considerable. However, as the discussion during **Managing Security Risks for Sustainable Development** (WS 160) concluded, it was hard to identify and calculate the cost of each cyberattack due to multiple tangible and intangible effects, with one of the consequences being the limited availability of global statistics on cyberattacks.

With regard to cybersecurity strategies, the speakers made reference to the OECD's recommendation on *Digital Security Risk Management for Economic and Social Prosperity* which seeks to ensure that risk management is considered an important facet when decisions are made on digital issues. They said, however, that existing cybersecurity strategies are too focused on technology and are missing the human element.

In **Commonwealth Approach on National Cybersecurity Strategies** (WS 131), the speakers agreed that cybersecurity should be tackled by governments in partnership with the private sector, regulators, and other governments. It requires legal frameworks, the use of technology to enforce cybersecurity, harmonisation of regional laws, and cooperation among states to tackle cross-border cybercrime.

The issue of trust (as well as other issues, such as privacy and freedom of expression, which are discussed below) was a main theme that intersected with security. Discussed predominantly during the main session dedicated to **Enhancing Cybersecurity and Building Digital Trust**, the panel agreed that multistakeholder approaches and private-public partnerships should be used to address the challenges. 'If you want total security, go to prison', said one panellist. On the other hand, surveillance and censorship cannot be used to justify cybersecurity. Surprisingly, a panellist in **Cybersecurity, Human Rights and Internet Business Triangle** (WS 172) revealed that 80% of actionable intelligence comes from publically available resources.

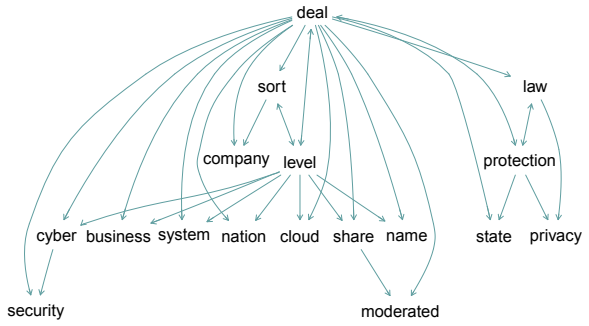
Also closely associated with cybersecurity is the issue of encryption. While greater protection for encryption and anonymity online is required, encryption needs to be viewed as more closely related to security, rather than a purely economic issue. During **Encryption and Anonymity: Rights and Risks** (WS 155), panellists discussed the pros and cons of legislation on encryption, and considered the implications of two jurisdictional cases on anonymity and encryption.

Encryption was compared to antibiotics, in **Law Enforcement in a World of Pervasive Encryption** (WS 141): we don't know if they will work but we need to trust that they will. Pervasive encryption could become a reality within the next decade; more so if there is continued pressure in favour of encryption from various angles, even though admittedly, encryption poses a challenge to criminal investigations.

In the same workshop, the UNESCO representative stressed that if we envisage ubiquitous encryption, all the countries and governments need a political will in order to agree to have the supporting regulatory framework on the encryption. She also provided an update on the progress that was made at UNESCO during its General Conference. The UNESCO research project on Balancing privacy and transparency in the context of promoting online freedom of expression, which is expected to look at privacy, transparency, encryption, and related issues, will be finalised by the end of the year.

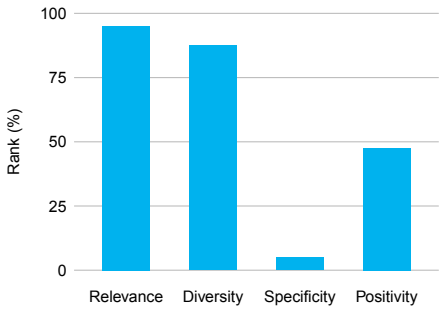
A similar discussion took place during **The Politics of Encryption** (WS 53). Here too, a law enforcement agent explained why governments needed access to encrypted data and how it can be used to prevent crime and increase public safety.

Read more and get the latest on cybersecurity, encryption, and other security-related issues, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

PRIVACY AND DATA PROTECTION



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

At this year's IGF, the discussion on privacy and data protection revisited a typical dilemma: How do we ensure both privacy and security or - at least - strike a right balance between two?

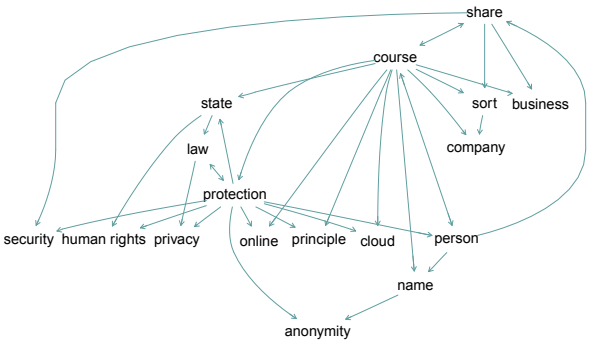
This 'balancing question' was echoed in many discussions. In the debate on encryption (WS 141 on **Law Enforcement in a World of Pervasive Encryption**, and WS 53 on **The Politics of Encryption**), human rights and security communities presented two different views. Human rights activists argued for pervasive encryption aimed at protecting privacy, while security officials believe that strong encryption hinders investigations and poses a problem to gathering data and preventing crime and terrorism.

In the debate between **Privacy and Transparency** (WS 124), it was argued that the treatment of personal data needs to be transparent, with transparency being also closely associated with accountability. Yet, a recently negotiated trade agreement, which will impact users' privacy, was not negotiated in such a transparent way.

In discussing these dichotomies, a few new proposals and ideas emerged. For example, in **Implementing Core Principles in the Digital Age** (WS 114), the two UN Special Rapporteurs on freedom of expression and on privacy argued that both rights could be protected in an integrated way, where encryption and transparency of policy should play an important role. The link between privacy, freedom of expression, and anonymity was discussed in depth in Special Rapporteur David Kaye's report on the promotion and protection of the right to freedom of opinion and expression (May 2015).

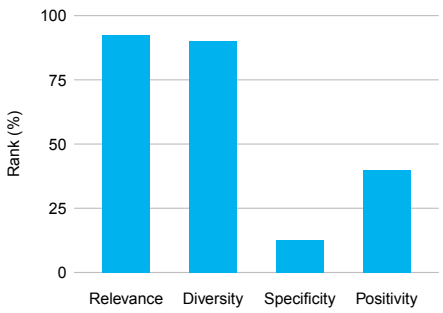
Another question was whether privacy should be protected on a national or international level. The prevailing view is that it needs to be afforded international protection. In the same workshop, Special Rapporteur Joseph Cannataci said that people needed 'safeguards without borders' and 'remedies across borders', neither of which he believe is possible at the moment. He also referred to the 'further development of international law' during the **Open Forum on the Right to Privacy in the Digital Age**, a view which was picked up by a Brazilian Foreign Ministry official: the right to privacy is already enshrined in international law through the **International Covenant on Civil and Political Rights**, which has been ratified by 168 countries. His comment: 'And we might ask ourselves what about the remaining countries? Well, all remaining countries recognise the universal Human Rights, which also [include] the right to privacy. So we have the norm. We have a foundation. A basis to work on.'

Read more and get the latest on privacy and data protection, and other human rights, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

Freedom of expression is a recurrent issue at IGFs, and this year's IGF also served to revisit well-known challenges. Yet, the discussion has evolved over the years: what was previously a debate in favour of declaring online freedom of speech a right, has become a discussion on how to ensure that the right is truly respected – both online and offline.

The UN resolution which proclaimed that the same rights which people have offline must also be protected online marked the turning point in the debate. It was preceded by another important instrument: former Special Rapporteur Frank La Rue's 2012 report and the three-part cumulative test, which has become a litmus test for the protection of freedom of speech.

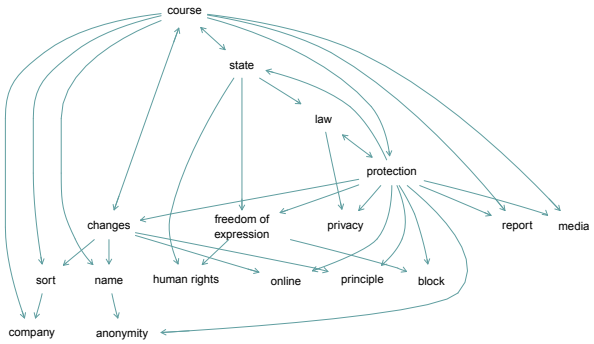
Several workshops made reference to La Rue's report, with discussions on various aspects related to implementing his recommendations. The workshop on **Freedom of Expression online: Gaps in policy and practice** (WS 153), for example, brought together groups to share their countries' experiences of the implementation (or otherwise) of the cumulative tests and indicators mentioned in La Rue's report.

Yet, various challenges still persist. While on one hand technology has increased the user's freedom of expression, on the other there are sev-

eral challenges ahead in adopting a framework for freedom of expression that can apply globally, which many are calling for. And in the **open microphone and taking stock session**, the need to prevent the Internet from becoming a tool of repression was once again emphasised.

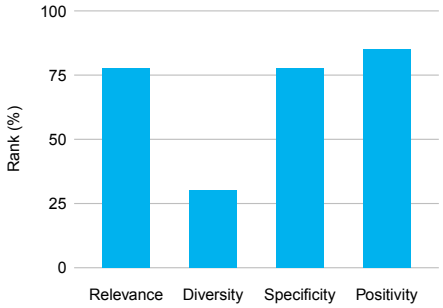
In the main session on **Internet Economy and Sustainable Development**, access to information was discussed in the context of the Sustainable Development Goals (SDGs). In referring to Goal 16.10, to 'ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements', it was agreed that in order to achieve a holistic approach to the importance of ICTs and the Internet in reaching the SDGs, the social, cultural, and educational components must also be addressed.

Read more and get the latest on freedom of expression and other human rights, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

INTERNET ECONOMY AND DEVELOPMENT



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

Economic activities and business developments are among the Internet's main growth engines. Apart from its great influence on the ways in which the Internet evolves, the business sector is also greatly affected by the Internet in general, and by Internet governance policies in particular, such as those governing trade, copyright, and taxation.

During this year's IGF, economy-related topics were often linked to novel economic dynamics of the Internet industry. One of them was Internet Plus - described during **'Internet Plus' to Fuel Industry Evolution** (WS 110) - as a model that integrated mobile Internet, cloud computing, and the Internet of Things, with the aim of scaling for production and creating smart factories. The more ubiquitous platforms for mobile payments (WS 56) also boosted the Internet economy.

To keep the Internet engine running, innovation is key, especially when it comes to intellectual property. **Unlocking Internet Economy through Copyright Reform** (WS 167) addressed the consequences of copyright policies on Internet innovation, with the session organisers arguing that the current Internet innovation system, characterised by 'multinational corporations, fledging start-ups, telecommunications providers, content creators and consumers [forming] increasingly complex value chains', often contradicts the copyright regime.

Developments in the digital economy also have consequences on employment. **Digital Economy, Jobs and Multistakeholder Practices** (WS 29) discussed the short-term phenomenon of job losses due to automation, which is believed will be offset by the job-creating impact of innovation in the long term.

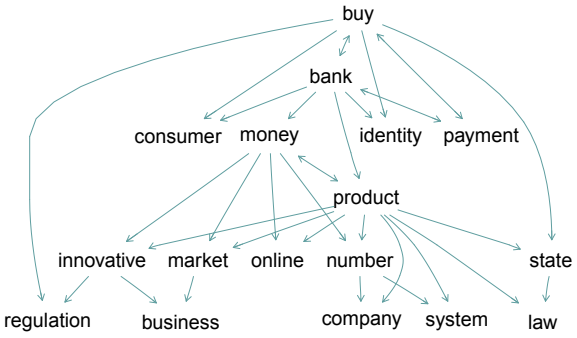
Apart from the role of copyright policies and the impact on employment, the consequences of trade agreements (WS 7) and tax strategies (WS 200) on the Internet economy and business sector were discussed. One particular view on taxation was that it was considered a hindrance to access. A typical example offered by a Facebook representative during **Revenue Streams that Grow & Sustain Internet Economies** (WS 241) was that of connectivity taxes: import duties, sales taxes of devices, and sales taxes on the purchase of data plans are being imposed at various points in the value chain between a user buying a device and actually being able to use it. 'Typically, you tax things you want less of. If you want more connectivity and you're imposing additional taxes, or you want more affordability and you're imposing additional taxes, that's a hindrance, not something that helps to facilitate what you're trying to achieve.'

The discussion on the Internet economy also looked at the development aspect, which was the topic of a number of workshops. With reference to taxation and developing countries, a panellist in **Economics of the Global Internet** (WS 112), said that despite the economic benefits of accessing ICTs, this did not mean that taxation was not required, but that a more balanced fiscal policy was needed.

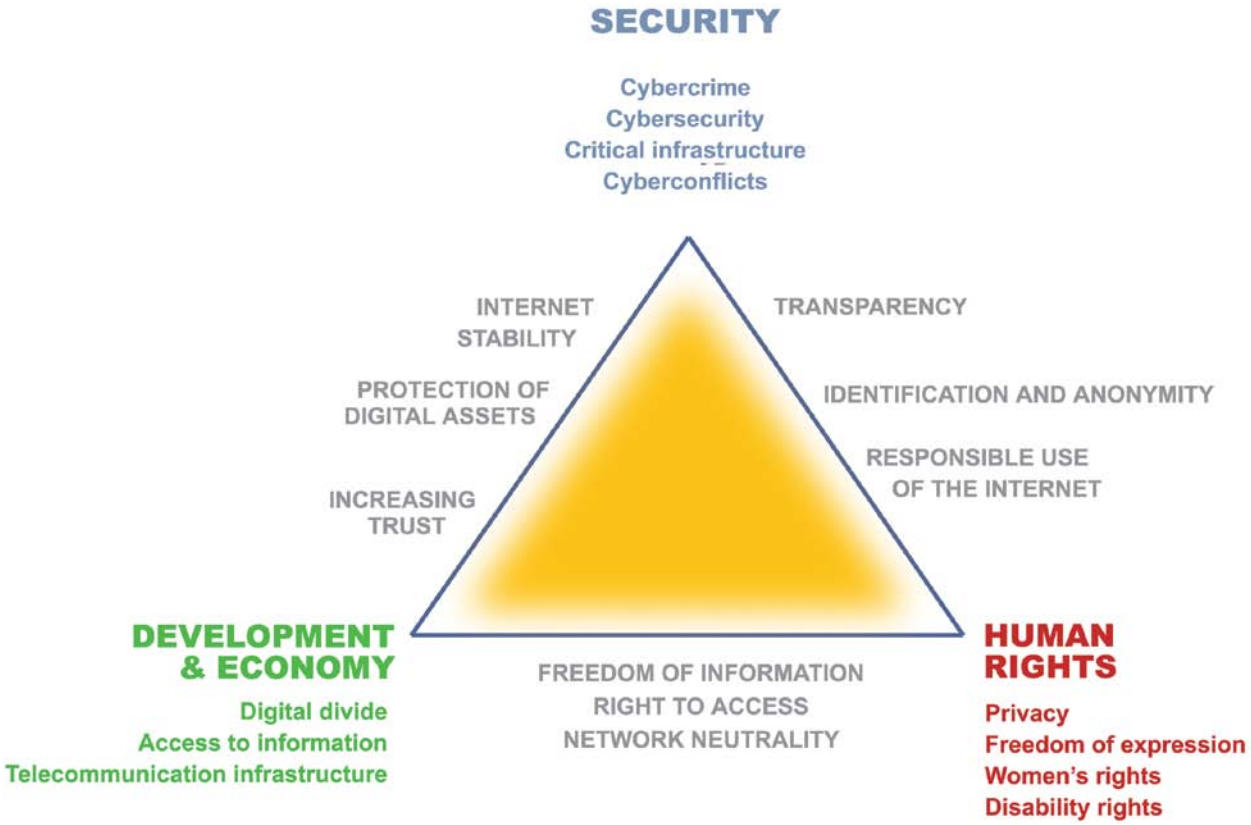
In **How to Bridge the Global Internet Economy Divide** (WS 97), a Google representative anchored the discussion to geographical realities: 'Both regions have challenges, but slightly different. In Europe it's about scaling and in Africa it is more about access.' The main challenge, therefore - as suggested in the main session on **Internet Economy and Sustainable Development** - was how to narrow the divide and empower developing countries. Additionally, we need to tap in to the potential of the Internet economy as a social and economic equaliser.

Notwithstanding, an important interplay between three areas of digital policy - cybersecurity, human rights, and Internet business - is unfolding. In the **workshop bearing the same name**, panellists discussed this interplay which has had a large impact on a wide range of social issues, citing as an example the current migration crisis to demonstrate the dynamics of the 'triangle'. As the diagram presented during the workshop illustrated, this interplay deeply permeates other aspects of digital policy.

Read more and get the latest on e-commerce, taxation, digital divide, labour law, and other economic-related issues, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.



AGENDA 2030 FOR SUSTAINABLE DEVELOPMENT AND ACCESS TO THE INTERNET

The 2030 Agenda for Sustainable Development provided the overall context for discussions at this year's IGF. In the **Opening Session**, most speakers emphasised the fact that an open, free, and neutral Internet would empower sustainable development. In particular, Goal 9 of the agenda sets an ambitious target to 'significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020'.

Access to the Internet is the main operational issue on sustainable development and the Internet. Technical infrastructure is necessary but is not a sufficient condition for full access to the Internet. As was indicated during **Freedom of Expression Online: Gaps in Policy and Practice** (WS 153), full affordability and accessibility requires a proper legal, economic, and social context. Users need skills in order to benefit fully from access to the Internet. On the economic aspect, the Broadband Commission's 2015 targets suggest that the Internet is affordable if the cost of the access is not more than 5% of average monthly income.

The lack of data on the volume and cost of international traffic is a major problem for many policymakers in developing countries, as was indicated during **Economics of the Global Internet** (WS 112). Access has a high gender aspect as the World Wide Web Foundation's recent report shows that women in developing countries in Africa, Asia, and South America are 50% less likely than men - with the same education, income, and age - to have access to the Internet.

The **Roundtable on Small Island Developing States** (WS 21) discussed innovative solutions for access to typically geographically remote small island states. The cost of laying undersea cables to serve low populated communities makes access to the Internet not particularly attractive to the corporate sector. The Roundtable discussed the possible use of zero rating services and the impact on small markets.

Read more and get the latest on access, e-commerce, taxation, digital divide, labour law, and other economic-related issues, on *GIP Digital Watch* (dw.giplatform.org)

INFRASTRUCTURE: IXPS, IPV6, CRITICAL RESOURCES

In general, the workshops on infrastructure focused on specific areas, such as IXPs, spectrum, interconnection, and IPv6. The often technical discussions verged on other issues, such as sustainable development and security. In relation to other areas, few workshops on infrastructure were scheduled.

There must be a commercial rationale for IXPs to be more widely introduced and for actors to identify with. **IXPs: Driving Connectivity and Local Economies** (WS 171) served to showcase the success of some regions in establishing IXPs. Canada, for example, has 7 IXPs, whereas the Caribbean region has 11 IXPs. Accounting for this success,

especially in the Caribbean, is the fact that regulators are not running them but simply playing a mediatory role. The discussion provided further insights into the current usage of IXPs in developed and developing countries, and offered suggestions for successful uptake. Among these are the fact that they should be community-led rather than having a top-down structure, they should have a reasonable governance structure, and they should be not-for-profit organisations. More case studies were presented during **Ensuring Sustainability for IXPs in the Developing World** (WS 201), which concluded that, as in many areas of Internet governance, one size does not fit all when it comes to the governance of IXPs.

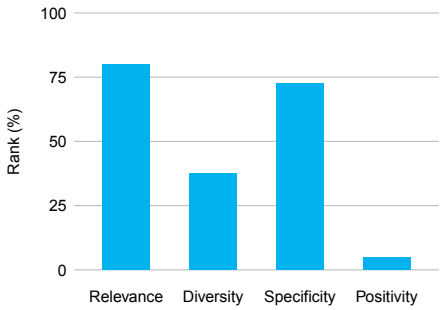
The topic of protection of key Internet resources resurfaces in digital policy discussions from time to time. In **The Global 'Public Interest' in Critical Internet Resources** (WS 52), it was concluded that an open process of running the infrastructure of the Internet was crucial. The discussion centred on how the Internet, as a global resource, could be managed in an open and inclusive manner that serves the public interest. It is interesting to note that the panellists could not agree on a definition of public interest in order to determine what this means with respect to critical Internet resources.

In **Spectrum Allocations: Challenges & Opportunities at the Edge** (WS 188), panellists discussed how new technology - including geo-satellites, orbits, high-altitude platform services, drones, and 'balloons' - was putting pressure on the use of spectrum. There are various opportunities, including the development of software for spectrum management. But just as software was introduced into the management of taxis, resulting in huge efficiencies but at the same time many social and economic downsides, we can either wait for the 'Uberisation' of spectrum management to happen, or regulate and manage the process in order to maximise the benefits of software.

In relation to the deployment of IPv6, further discussions on the persistent problem of the depletion of IPv4 numbers took place during the Best Practices Forum (BPF) on Creating an Enabling Environment for IPv6 Adoption. Although the pool of IPv4 is running out at an alarming rate, the panel agreed that the deployment of IPv6 is happening, albeit at its own pace. It was predicted that next year's BPF will most likely focus on the economic aspects of IPv6 deployment.

Read more and get the latest on telecommunications infrastructure, critical infrastructure, and IP numbers, on *GIP Digital Watch* (dw.giplatform.org)

NET NEUTRALITY AND ZERO RATING



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

As often happens at the IGF, an issue emerged as the hot topic of the week. A couple of years ago, in Bali, it was online surveillance. This year, it was zero rating.

Zero rating is the practice of not charging customers for specific applications or services they use. The most famous example is Facebook's internet.org, now rebranded 'Free Basics'. The Free Basics service provides free access to content and applications to populations in a number of developing countries, with the aim of providing some level of Internet service to people who otherwise would have no service at all.

However, for critics of zero rating, this 'walled garden' approach conflicts with any rational policy of social development through innovation, as panellists from **Can Internet Rights and Access Goals be Reconciled?** (WS 126) said.

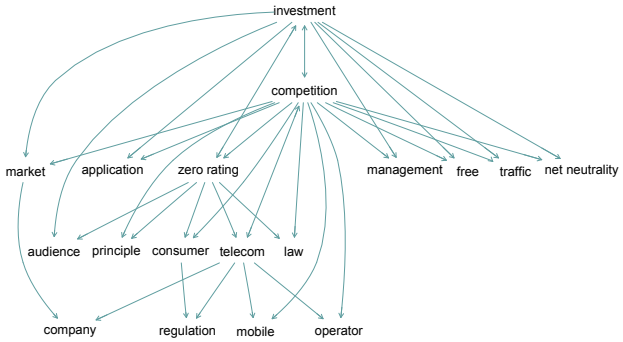
While zero rating in developed markets may have stronger implications for competition and unfettered access to information, in an undeveloped market, where there is otherwise very limited or no access to the Internet, does the provision of some services through zero rating actually empower, rather than disempower, users?

One idea discussed during the **Dynamic Coalition for Net Neutrality's meeting** is the existence of alternatives to zero rating that may be more sustainable in fostering Internet access and interconnectivity, among which are community networks that provide a decentralised alternative.

Some have asked whether we are witnessing a new 'cyber' imperialism, where the well-resourced tell the non-resourced that it is better for them to remain non-resourced until they have full resources rather than enjoy partial resources. On one hand, as speakers in **Zero-rating and Neutrality Policies in Developing Countries** (WS 156) said, users in least developed countries might prefer some access over no access. But as another speaker said (in WS 126), 'If you want to give us access, don't give us these tricks, give us real access. Don't give us condescending statements like you're too poor. Just deal with it. Give us real access.'

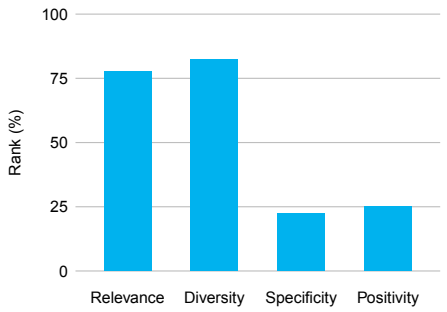
As with the two previous IGF hot topics, it may be that this IGF is the initial brainstorming phase of the zero rating discussion, with all parties passionately telling each other what they think without listening quite as intensely to each other's viewpoints. As with online surveillance and human rights, perhaps IGF2016 will see a more focused and mature discussion on zero rating – possibly as part of the wider discussion on how to bring access to all.

Read more and get the latest on net neutrality and zero rating and development, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

CONTENT POLICY, DIGITAL LEGACIES, AND THE RIGHT TO BE FORGOTTEN



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

Content policy is one of the main sociocultural areas in the Internet governance debate. Although not always mentioned explicitly, it is often embedded in discussions on human rights, liability of intermediaries, intellectual property, child safety, jurisdiction, and more. Last week's discussions were once again a vivid example of the intersecting nature of content policy.

Several sessions addressed the need for content control in different cases: from fighting violence against women online, to protecting children and adolescents, and safeguarding LGBT rights. At the same time, the discussions recognised the need to safeguard freedom of expression and other rights.

Although there was general consensus on the need to protect vulnerable communities, the extent of content control was not always agreed on. For example, during the **Best Practice Forum on Practices to Countering Abuse and Gender-Based Violence against Women Online**, several panellists spoke of the difficulty of establishing strong legal mechanisms that do not cause over-censorship. The workshop on **Tech-related Gender Violence x Freedom of Expression** (WS 196) explicitly dealt with the tension between gender protection and the right to free speech.

At the other end of the spectrum, several sessions addressed cases in which Internet content is censored by governments to establish digital control over their citizens. For example, **Information Controls in the Global South** (WS 224) addressed the challenges faced by civil society to have a meaningful impact when faced with information censorship.

New areas in content policy are being explored. For example, the emerging issue of content quality control was discussed during **Open Education Resources** (WS 58). What happens with our digital assets after we pass away? **Death and the Internet** (WS 70) looked at the issue of digital legacies... with a touch of humour. In a hypothetical set-up, panellists played the role of an online user who died testate without a valid power of attorney; his family were suing for the right to access his data, while legal experts applied different laws to the scenario. Although future planning is a topic many avoid, the amount of personal data we leave behind merits an in-depth discussion about privacy, personal data, conflicting policies and regulations, jurisdiction, and the role of policymakers. It is expected that more discussions on digital legacies will take place, especially among the legal community and the industry.

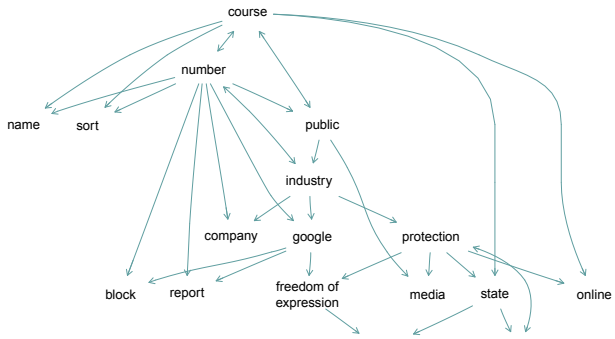
With regard to the right to be forgotten (RTBF), last year's Court of Justice of the European Union (CJEU) ruling (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González) had far-reaching implications, and created a ripple effect across different jurisdictions.

One of the main issues is with regard to the terminology, as the RTBF can generate false reassurances that an individual's past can be forgotten. Panellists in The **'Right to be Forgotten' Rulings and their Implications** (WS 31) suggested that the right be renamed to 'the right to be de-indexed'. The main issues were reiterated in **Cases on the Right to be Forgotten, What Have we Learned?** (WS 142): the term is problematic, and policymakers and the judiciary need a better understanding of technology. The process of de-listing imposes an unnecessary burden on online media houses to continually update their published stories. The process is also likely to be abused in jurisdictions where the take-down notice system is implemented.

Both workshops discussed the risk that the RTBF is affecting other human rights including the right to memory and the flow of ideas, the right to know the truth, and freedom of the press. These essential rights to democracy could be threatened by the RTBF. In fact, the representative from the United Nations Commission for Human Rights commented that the RTBF contrasts with the right to know the truth, which is a distinct right. The erasure of information could impact the right to truth, and thus create a need for due process.

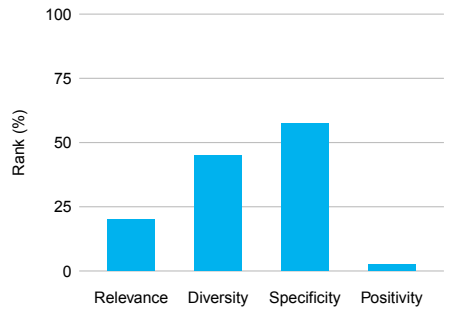
Among the practical implications is the fact that different jurisdictions have ruled or legislated on the RTBF. These include a judgement by the Constitutional Court of Colombia; new legislation in Chile, Nicaragua, and Russia; and data authorities' rulings on search engines. The CJEU ruling has therefore created a ripple effect, extending the European cyberlaw footprint to a global level.

Read more and get the latest on content policy, jurisdiction, intermediaries, human rights, and other legal aspects, on *GIP Digital Watch* **(dw.giplatform.org)**



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

CHILD ONLINE SAFETY



IG Barometer scores. The rank (%) of each score is computed relative to 40 IG issues that were considered in the analysis of IGF 2015 session transcripts. To learn more about the GIP IG Barometer scores, visit **http://www.giplatform.org/barometer#scores**.

Children face numerous online risks from being exposed to indecent content and inappropriate contact, to over-sharing information and falling victims of identity theft and privacy invasion. The risks are increasing: more children are accessing the Internet at a younger age. At the same time, awareness of child safety is also on the increase, as are the number of initiatives on child online safety.

Child online safety was discussed in a number of sessions, where several key themes emerged. In the workshop on **Child Online Protection through Multistakeholder Engagement** (WS 6), panellists emphasised the role of stakeholders in combating the threats. Best practices discussed during the workshop showed that in Indonesia, this is being tackled through legal frameworks, cultural and educational initiatives, and technical approaches including parental guidance apps and software. In the UK, an equally alarming number of people have been involved in offences related to child sexual abuse material; this growing phenomenon requires a multistakeholder approach to deal with such cases.

When it comes to online child sexual abuse, the Internet has amplified this growing phenomenon, as perpetrators hide behind a veil of anonymity and false identities to evade law enforcement. It is here that issues related to online child sexual abuse intersect with other issues related to security, encryption, and anonymity.

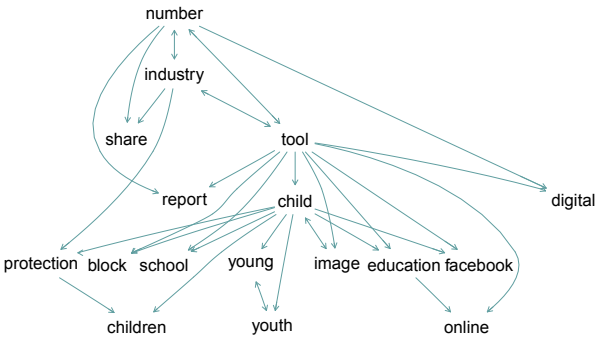
One of the issues related to child sexual abuse material (CSAM) – that of grey area content which sits on the verge between legal and illegal – was discussed in **No Grey Area – Against Sexual Exploitation of Children** (WS 49). Such images may not be illegal in every country but are harmful both to children posing – such as in highly sexualised images – and to children who are shown these images as part of a perpetrator's grooming process.

Developments in technology used to identify CSAM are being made. For example, speakers described programmes which are being used to identify CSAM through key terms used by perpetrators to search for content.

The **Dynamic Coalition on Child Online Safety** also described the use of hash technology (digital fingerprints of photos) and databases to identify CSAM. Many of the images are copies of originals, and in some cases, thousands of copies of the same image exist. Hash lists could identify duplicates with the aim of stopping the revictimisation of children every time the images are seen, and find new images with the aim of identifying and rescuing the victims, and identifying and prosecuting the perpetrators.

From the discussions at IG F2015, it is clear that significant developments are expected in the technology used to identify new CSAM. More advanced technology – and cooperation among stakeholders – will enable authorities, especially law enforcement, to better combat CSAM.

Read more and get the latest on child safety online and cybersecurity, on *GIP Digital Watch* (dw.giplatform.org)



Associative paths. Each keyword on the graph receives exactly two inputs, from the two keywords that are found in the semantic context most similar to it.

ACCESS AND DISABILITIES, AND ONLINE (E-) PARTICIPATION

The issues of access for persons with disabilities, and e- or online (remote) participation are in a state of constant change, making them particularly interesting to follow. They are addressed together here because of their inherent alliance (for example captioning and better tools) in support of strategies and tools that foster greater and more equitable inclusion.

Difficulties for access for persons with disabilities have been brought to the forefront by the work of the **Dynamic Coalition on Access and Disability (DCAD)** and have the full support of the IGF Secretariat and the Multistakeholder Advisory Group (MAG). Improvement is slow, but constant. DCAD is raising awareness, and assisting organisers, including the IGF Secretariat, to understand and improve strategies, such as expedited access to links for the DCAD and others needing them, and to assist with registration at workshops.

Awareness raising is critical, as shown in the comment made at the **NETmundial main session** noting that the NETmundial principles make no reference at all to addressing the needs of persons with disabilities. **Empowering the Next Billion by Improving Accessibility** (WS 253) provided an excellent presentation and discussion of tools that are invaluable for everyone (Skype translator, F123 Initiative) highlighting the unrecognised cross-cutting nature of these issues.

Online participation received little attention as an issue, although the debate in **Viable Application & Debate: Online Participation Principles** (WS 27) was dynamic and brought out basic issues in black and white. The principles for online participation, developed in successive IGF workshops with global online collaboration, should be widely disseminated for use and comment, and in support of funding for further innovative improvement for inclusive online access.

Online participation for IGF 2015 was supported and closely followed by the IGF support team, and congratulations are in order. One step backwards was the placement of remote moderators at the back (to facilitate technical coordination) making communication with panel moderators difficult, if not impossible. It is noteworthy that most moderators worked to overcome this challenge.

Technology and strategies have made significant advances, but work must continue to optimise the use of available tools and strategies. It is noteworthy that while the IGF is known for pioneering remote hubs and wide online (remote) participation for IG meetings, the ITU and ICANN have increased the pace of online inclusion at a greater and more constant pace. An indefinite extension of the IGF mandate should create an opportunity for funding to build on the existing foundation to ensure inclusion for those who are so close, but yet so far.

Read more and get the latest on access and rights of people with disabilities, and other socio-cultural and development issues, on *GIP Digital Watch* (dw.giplatform.org)

IANA TRANSITION AND ICANN'S ACCOUNTABILITY

The discussions on the IANA transition during the IGF need to be looked at from the broader process which has been ongoing for the past few months. Specifically, the IANA Stewardship Transition Coordination Group (ICG) recently completed its work (with only one outstanding item related to accountability), while the Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) agreed on the development of the Triple E approach (engagement, escalation, and enforcement) and on the Sole Designator model.

At the IGF, two main discussions took place. The first was in relation to jurisdiction and the fact that ICANN is subject to the laws of California. Although the question was floated as to whether ICANN would serve the global public interest if it remained subject to California's jurisdiction, the conclusions of the workshop on **National and Transnational Internet Governance: Jurisdiction** (WS 135) were quite clear. It was concluded that the stability of the existing operation of ICANN in California should not be disturbed, and that the few motivations for change are political and not realistic. In addition, the new arrangements which would see ICANN remain in the USA are sound. They allow for future change, but no change is foreseen. The discussion on jurisdiction continued during a parallel session on **IANA Functions Transition: A New Era in Internet Governance?** (WS 72).

In another discussion - **Multistakeholder Internet Governance - IANA Stewardship** (WS 163) - ICANN was urged to put more effort into ensuring greater diversity in its engagement process. Contributors to the ongoing process are not representative of the whole community, as statistics show that most contributors are from North America and Europe, whereas Africa and Latin America are hardly represented in the exercise. In addition, ICANN's participation model is a challenge to some contributors; extended conference calls and time zone differences were among the examples used to urge ICANN to enhance its outreach programme.

The next step is for CCWG-Accountability to publish a high-level overview of recommendations and a summary of changes from the second draft proposal.

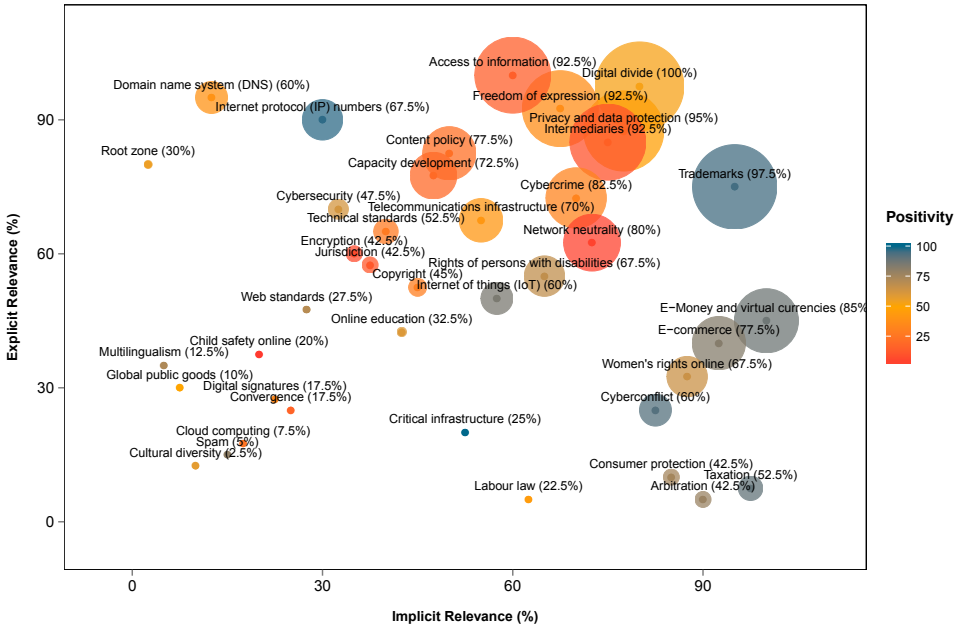
Read more and get the latest on the IANA Transition and ICANN Accountability, on *GIP Digital Watch* (dw.giplatform.org)

Our IGF reporting was supported by data-mining and text analysis. It provided evidence-based input into coverage of the IGF. Text analysis was embedded in the overall approach to IGF reporting. For example, the findings from our text analysis were used in the preparation of the illustrations (including the IGF selfies). In addition, data analysis supported daily summaries published in the four issues of the *IGF Daily*.

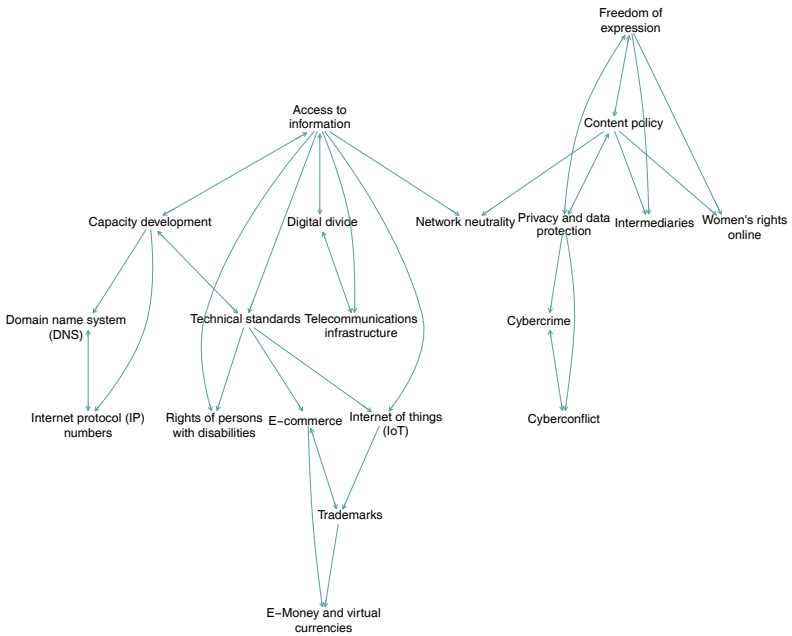
IGF reporting used two major sources: transcripts from the session, and social media input (Twitter feeds). They were analysed by Diplo's IG Terminological Model.

RELEVANCE AND SENTIMENT OF IG ISSUES

Implicit relevance is computed from the session's semantic similarity with all previously held IGF sessions between the 2006 and 2014 meetings. Explicit relevance is computed in comparison to the absolute count of issue-specific keywords. Percent and marker size are on the plot scale with Total IG issue relevance (average of Implicit and Explicit relevance). Sentiment analysis (color-coded in the plot) is computed with regards to the usage of emotionally charged terms (positively/negatively) characteristic of each issue.



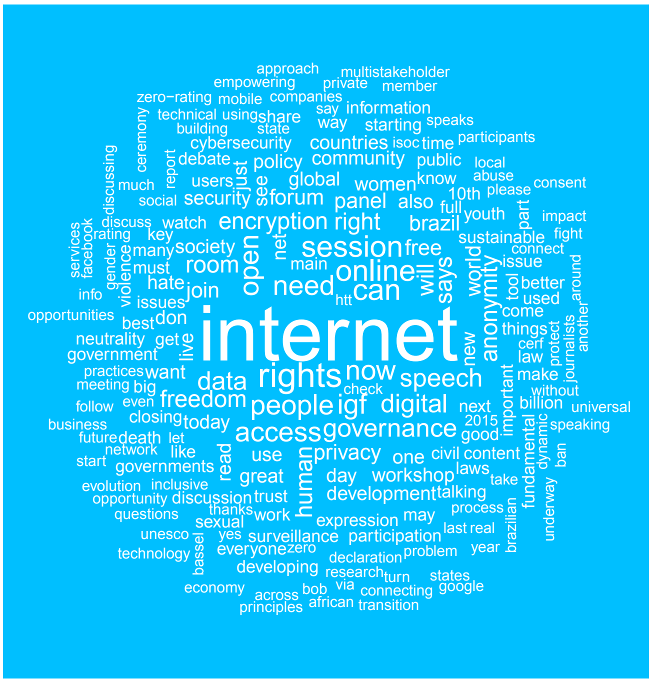
ASSOCIATIVE PATHS BETWEEN IG ISSUES



The semantic similarity between the IG issues was computed from the topic-model of the 2006-14 IGF session transcripts and projected onto the IGF 2015 sessions. Each IG issue in the plot receives exactly two inputs, both originating from two other issues that are found in the most similar semantic context to it.

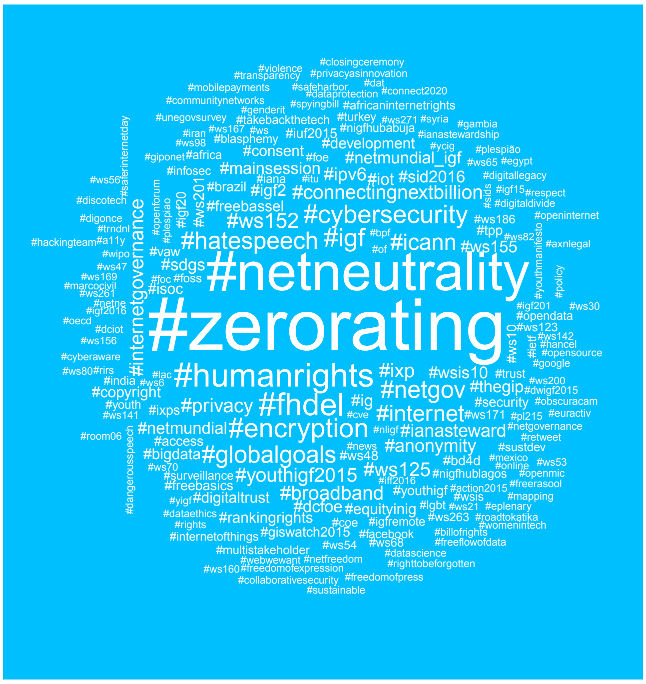
TWITTER WORDCLOUD

The size of the word scales with the frequency of its occurrence in a sample of 17,100 most relevant tweets with a #IGF2015 hashtag as returned by Twitter Search API.



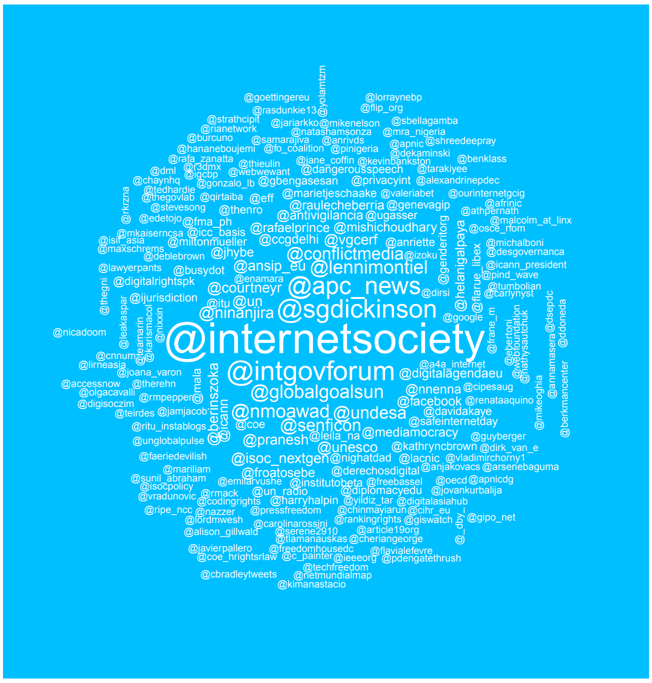
TWITTER HASHCLOUD

The size of the hashtag scales with the number of its uses in a sample of 17,100 most relevant tweets with a #IGF2015 hashtag as returned by Twitter Search API.



TWITTER USERCLOUD

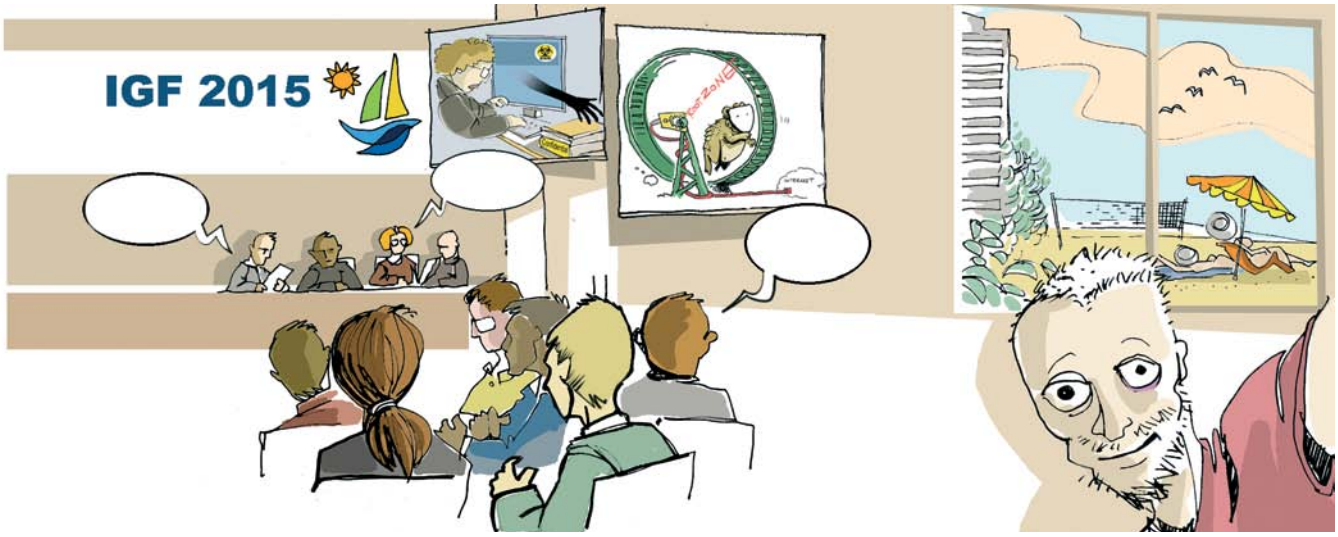
The size of the user name scales with the number of mentions it received in a sample of 17,100 most relevant tweets with a #IGF2015 hashtag as returned by Twitter Search API.



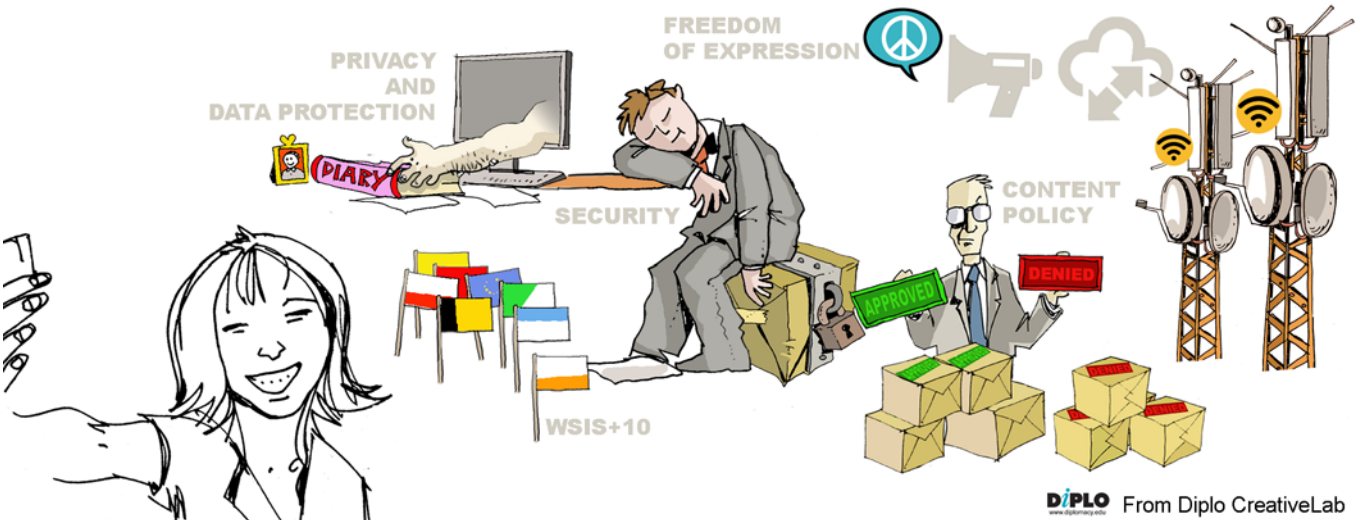
Diplo's CreativeLab illustrated the main IG issues. Concepts for illustration were developed in close cooperation with IG experts who were following the issues.

DiPLO | CreativeLab

9 November 2015 – Day 0'

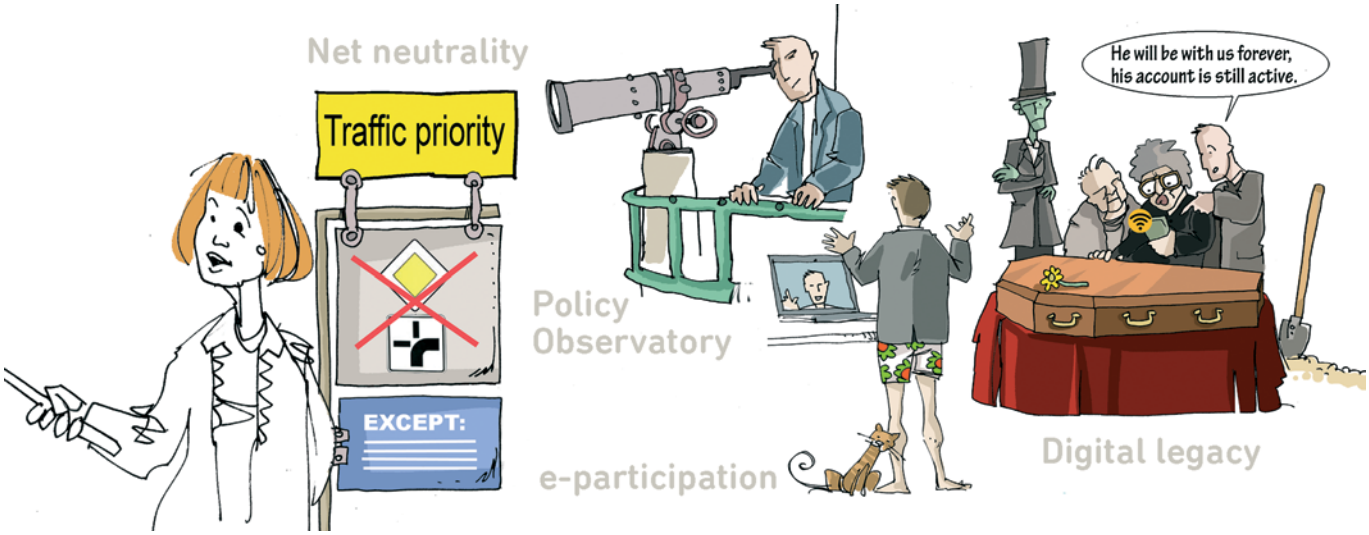


10 November 2015 – Day 1

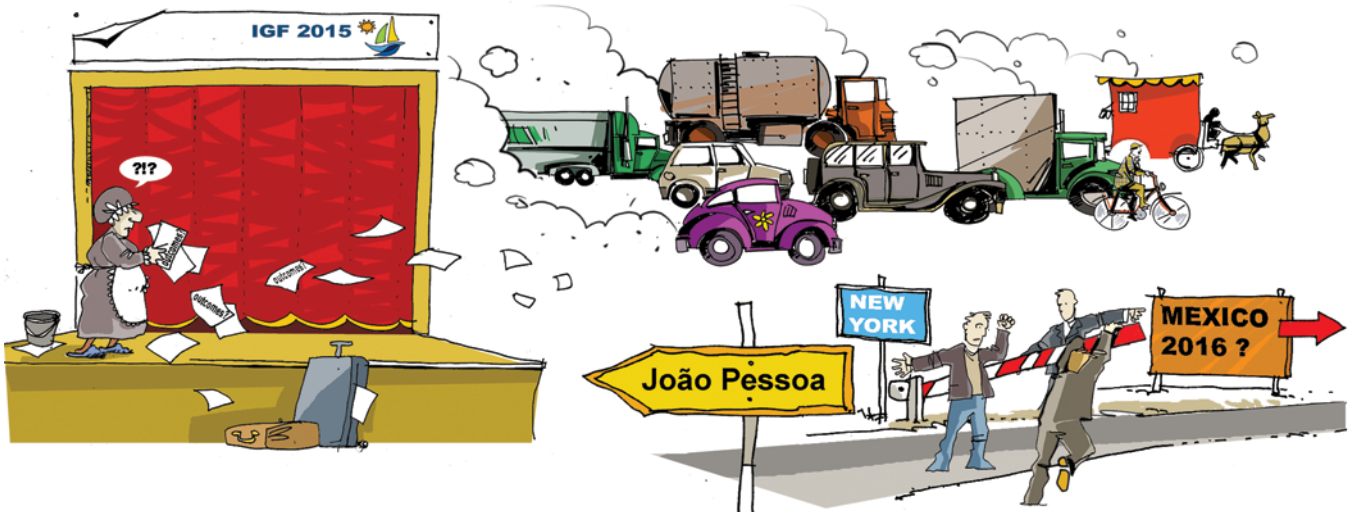


11 November 2015 – Day 2

12 November 2015 – Day 3



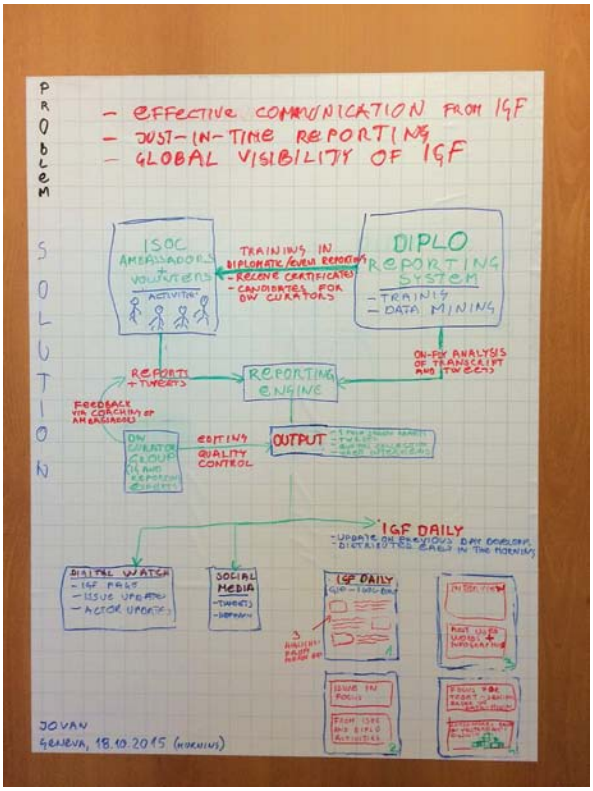
13 November 2015 – Day 4



ABOUT IGF REPORTING

The concept for IGF Reporting was outlined on Jovan's door on 18 October. It combines traditional reporting from sessions and data-mining of transcripts. Reports were prepared by 20 rapporteurs (ISOC Ambassadors), edited by editors in Europe and integrated with results of data-mining analysis of text transcripts from the sessions. It served as the basis for illustrators to prepare artistic views of the sessions.

All materials were available just-in-time on the website while every morning *IGF Daily* was distributed as a summary of the previous day's activities. The global team worked around the clock.



THANKING THE IGF DAILY TEAM!

DiploFoundation in collaboration with the Internet Society has added another layer to *GIP Digital Watch* : integrated reporting from the Internet Governance Forum (IGF). The experiment addressed the challenge of navigating through parallel sessions and numerous activities at the IGF. Our appreciation goes to *IGF Daily's* rapporteurs for their dedication:

Internet Society IGF ambassadors: Amanda Soares Kemmer (Brazil), Argyro Karanasiou (Greece), Arsene Tungali (Democratic Republic of Congo), Ashell Forde (Barbados), Evelyn Namara (Uganda), Grace Mutung'u (Kenya), Krishna Kumar Rajamannar (India), Lianna Galstyan (Armenia), Maureen Hernandez (Venezuela), Mwendwa Kivuva (Kenya), Suprita Lnu (India), Michael Oghia (United States), Maria Paola Pérez (Venezuela), Mohit Saraswat (United Arab Emirates)

Diplo colleagues and friends present at the IGF: Patrick Curry (UK), Radek Bejdak (Czech Republic), Samantha Dickinson (Australia), Virginia Paque (USA), Vladimir Radunovic (Serbia)

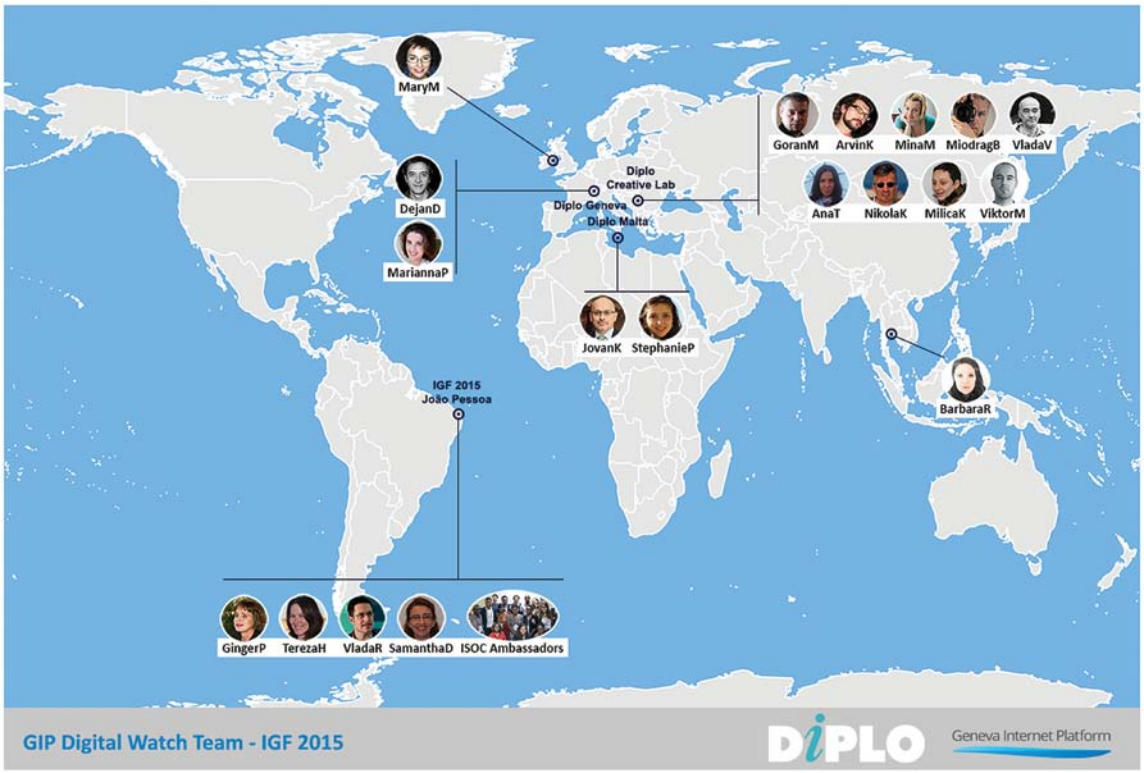
Diplo rapporteurs online: Arvin Kamberi (Serbia), Barbara Rosen Jacobson (Netherlands), Stephanie Borg Psaila (Malta)

Diplo editors: Hannah Slavik (Romania), Marianna Drake (UK), Mary Murphy (Hungary), Stephanie Borg Psaila (Malta)

Special thanks also to Diplo's CreativeLab team (in Malta, Switzerland and Serbia): Aleksandar Nedeljkov, Ana Trifunovic, Dejan Dincic, Goran Milovanovic, Jelena Jakovljevic, Milica Virijevic Konstantinovic, Mina Mudric, Nikola Krstic, Tanja Nikolic, Viktor Mijatovic, Vladimir Veljasevic

Concept: Jovan Kurbalija, director of DiploFoundation, head of the Geneva Internet Platform

Coordination: Tereza Horejsova, director project development of DiploFoundation, coordinator of the Geneva Internet Platform



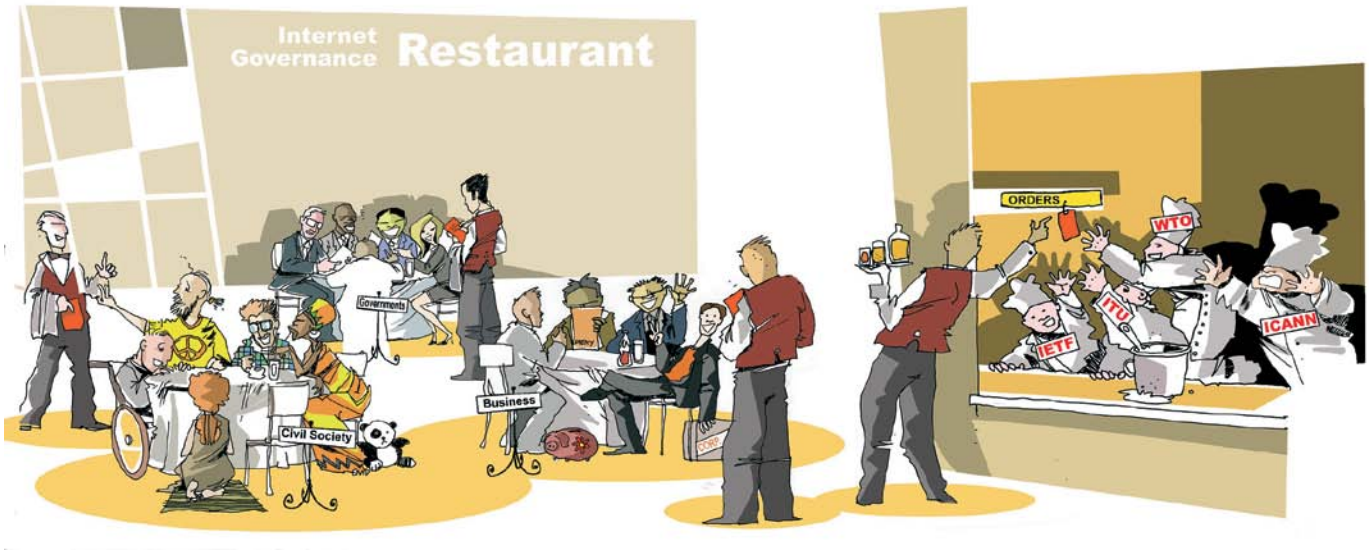
HOW TO DRAFT A DIGITAL POLICY SPEECH

Cooking recipe

Recent negotiations during the WSIS+10 process, and discussions at last week's 10th IGF, have inspired us to share the following recipe for writing a successful digital speech, guaranteed to satisfy all appetites and keep your audience coming back for more. The recipe was originally published in Issue no. 2 of *Geneva Digital Watch*.

- Mix a handful of Internet opportunities with a handful of challenges, taking care to balance them carefully.
- Select from the almost limitless larder of risks and threats, taking care to add one sweet ingredient for every savoury one - for example, security and privacy, or privacy and transparency.
- To fully engage with the audience, liberally sprinkle with the terms 'multistakeholder' or 'multistakeholderism' - it's a popular ingredient that many would love to have more of.
- If you're out of multistakeholderism, you can substitute with inclusiveness.
- For a touch of spice that might be too hot for some to handle, add measures of gender and youth.
- To neutralise the spice, consider a cup of net neutrality or zero rating.
- Throw in a few first names of people everyone should know but no one is sure that they do, and don't add last names - this will pique people's interest.
- No digital speech would be complete without a healthy topping of paternal references to Vint Cerf or another father of the Internet.
- Gain credibility by adding a teaspoon of techie slang - particularly if you've never cooked before.
- Additional credibility can be gained by the smart mixing of three ingredients in the form of Venn diagrams. Choose any. If in doubt, cybersecurity, human rights and Internet business would work.
- If you run out of ideas, add 'building trust' or look for 'mitigating the risks' if you want to add a cybersecurity taste.
- And don't forget those acronyms. Here you walk a delicate line between creating a mysterious taste or losing your audience entirely.

Mix well. Smile constantly. Add the occasional rueful shrug. Deliver with confidence.



GIP Digital Watch is service provided by
Geneva Internet Platform
in partnership with
Internet Society
and members of the GIP Steering Committee
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
UNIVERSITÉ DE GENÈVE
DCAF a centre for security, development and the rule of law
ETH BOARD
GIP Digital Watch is operated by
DiPLO
www.diplomacy.edu