IGF DAILY No. 3

REPORTING DAILY FROM THE 2015
INTERNET GOVERNANCE FORUM
dw.giplatform.org/igf

Photo by Samantha Dickinson

IGF OUTPUTS & IGF RENEWAL

On day 2, many discussions focused on draft outcome documents from intersessional IGF work. IGF outcomes have been an 'elephant in the room' since the first IGF in 2006. Since then, the 'elephant' has continued to grow and yet the IGF community has been slow to decide how to get this large obstacle out of the way. The Tunis Agenda that gave IGF its mandate states, in paragraph 72(g), that the IGF can 'Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, **where appropriate**, make recommendations.'

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 keep 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 got a new turn with the NETmundial meeting in 2014, when an outcome document was negotiated and agreed on in a multistakeholder setting.

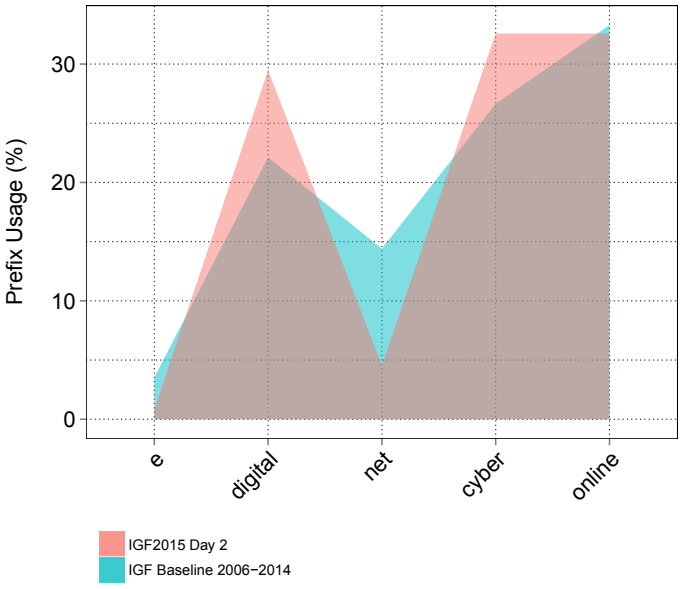
With the decision to hold a UN WSIS+10 High Level Meeting in December 2015, and its potential power to require changes to the IGF's scope and processes, late last year the IGF community finally decided to experiment with more tangible outputs at IGF 2015. Yesterday, the IGF community discussed the outputs created as part of the experimental intersessional work stream in the lead up to Joao Pessoa: a synthesis document of over 80 contributions on the theme 'Policy Options for Connecting the Next Billion' and six documents developed by the Best Practice Forums. All of these documents are substantial pieces of work.

What was interesting about the community response to these documents was the desire to keep them as 'living' documents rather than releasing them as more static outputs of IGF 2015. Perhaps, this approach could lead to a workable compromise between the need to achieve more tangible outcomes and the fact that outcome documents can have limited shelf-life due to a rapidly changing Internet environment.

PREFIX MONITOR

The Prefix Monitor for Day 2 of IGF 2015 (11 November) shows increasing relevance of the prefix *cyber*, from 18% on Day 1 to 33% on Day 2. The main reason was the high focus on cybersecurity issues (see page 2). *Digital* kept almost the same level of presence in the IGF discussions. *Net* declined sharply from 32% on Day 1 to 9% Day 2. A possible reason could be the diminished presence of net neutrality in the discussions. *Online* increased from 19% (Day 1) to 33% (Day 2) due to the higher prominence give to human rights issues (women's rights, the right to be forgotten, privacy, etc).

This analysis is based on 16 available transcripts from Day 2 of IGF 2015. Prefix Monitor follows the use of prefixes and identifies trends in discourse shaping, session by session, at the end of each day. Percents represent the relative presence of a particular prefix among all characteristically prefixed IG terms used. Diplo's CreativeLab text-mining DTAF platform powers the Prefix Monitor.

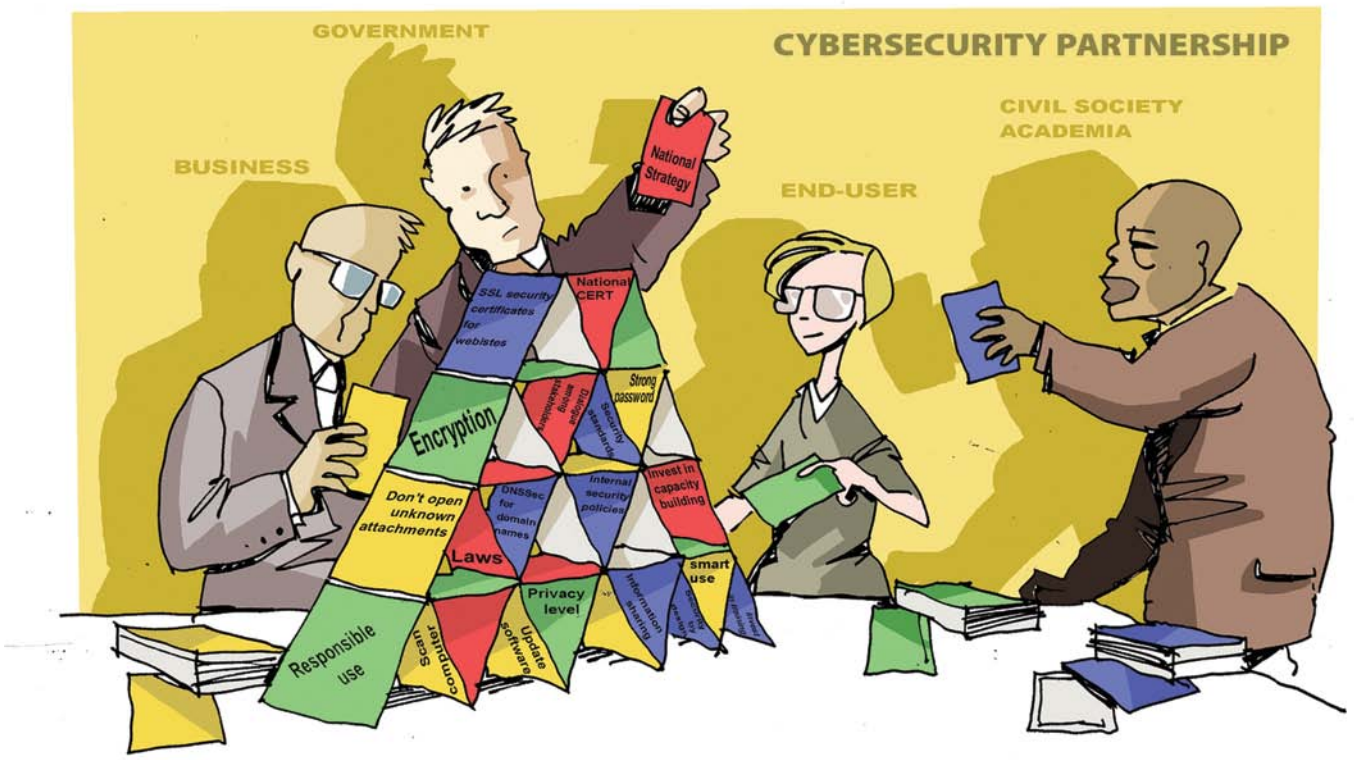


IGF Daily is prepared by *GIP Digital Watch* with support of the Internet Society and DiploFoundation

Geneva Internet Platform DigitalWatch

Internet Society

DiPLO www.diplomacy.edu



CYBERSECURITY, ENCRYPTION, AND SUSTAINABLE DEVELOPMENT

Cybersecurity was among the most frequently discussed policy issues during Day 2 of IGF 2015. With the current increase in cybercrime and a sharper focus on cybersecurity, it is no surprise that the issue was discussed at great length. The following themes emerged from the sessions we followed on Day 2:

- Cyber-attacks are on the rise, and are evolving with the growth of cable infrastructure, mobile money transfer, and social media. Cybersecurity, which should be tackled by governments in partnership with the private sector, regulators, and other governments, requires legal frameworks, the use of technology, harmonisation of regional laws, and cooperation among states to tackle cross-border cybercrimes. Existing cybersecurity strategies are too focused on technology and miss the human element (**Commonwealth Approach on National Cybersecurity Strategies**).

- Cybercrime affects the economic growth and sustainable development of many countries; the real economic cost of cyber-attacks is considerable. The OECD's recommendation on **Digital Security Risk Management for Economic and Social Prosperity** seeks to ensure that risk management is given high priority when decisions are made on digital issues. However, it is hard to identify and calculate the cost of each cyber-attack due to multiple tangible and intangible effects. One of the consequences is the limited availability of global statistics on cyber-attacks (**Managing Security Risks for Sustainable Development**).

- Pervasive encryption could become a reality within the next decade, especially if there is continued pressure in favour of encryption from various sources, despite the fact that encryption poses a challenge to criminal investigations. An international regulatory framework on encryption is needed (**Law Enforcement in a World of Pervasive Encryption**).

COUNTERING VIOLENCE AGAINST WOMEN ONLINE

Countering abuse against women online was the subject of a **Best Practice Forum**, in which the panellists expressed the need for more research and data on violence against women online. The debate is still controversial, and while an existing legal framework is often available, effective law enforcement mechanisms are lacking.

The recommendations included addressing the underlying causes of violence against women online in the light of local social contexts, and looking at the wider spectrum of human rights. Not only is the issue of violation of women's rights online a part of human rights, but the same approaches used to counter online hate speech and violent extremism could lend themselves to combatting abuse. At the same time, care is needed to ensure that legal mechanisms are not too stringent, as these could lead to over-censorship.

CHILD ONLINE PROTECTION

Children face numerous online risks, from being exposed to indecent content and inappropriate contact, to over-sharing of information and being victims of identity theft and privacy invasion. The workshop on **Child Online Protection through Multistakeholder Engagement** referred to such risks, and ways of combatting the threats.

Research and statistics show that an alarming number of children are accessing online pornography. In Indonesia, this is being tackled through legal frameworks, cultural and educational initiatives, and technical approaches including parental guidance apps and software. The number of people involved in offences related to child sexual abuse material in the UK is also alarming; a multistakeholder approach is needed to deal with this growing phenomenon.

The session on **No grey area – against sexual exploitation of children** highlighted gray area surrounding child sexual abuse material, such as content which pot rays children in highly sexualised setting.

IMPLICATIONS OF THE RIGHT TO BE FORGOTTEN

The Mario Costeja judgment on the right to be forgotten (RTBF) took users – and intermediaries, especially search engines – by surprise when the Court declared that intermediaries were obliged to consider such requests. The workshop on **The "Right to be Forgotten" Rulings and their Implications** saw an interesting suggestion in favour of changing the name to 'the right to be de-indexed'. The RTBF ruling had a major impact on the balance between this right, on the one hand, and public interest and the right to truth, on the other.

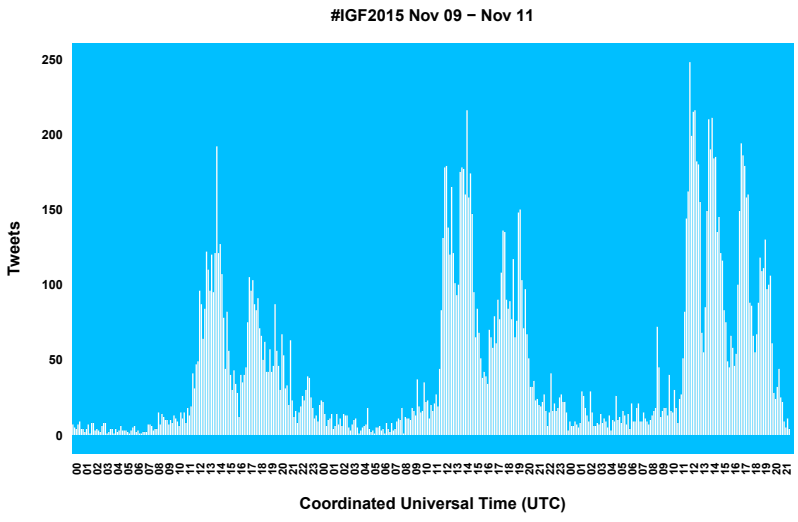
Panellists in a second workshop (**Cases on the Right to be Forgotten, What Have We Learned?**) reiterated the main issues: the term, itself, is problematic, and policy-makers and the judiciary need a better understanding of technology; the process is likely to be abused in jurisdictions where the take-down notice system is implemented; and the process of de-listing imposes an unnecessary burden on online media houses to continually update their published stories.

Both workshops discussed the risk that the RTBF threatens 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 rights are essential to a democracy.

> The impact of the Court of Justice of the European Union ruling is extending beyond European borders, as the RTBF is being considered in Korea, Mexico, and Brazil, among other countries. The European cyberlaw footprint is extending beyond its shores, with rulings in Colombia, and legislation in Russia.

The IGF via 19,218 tweets

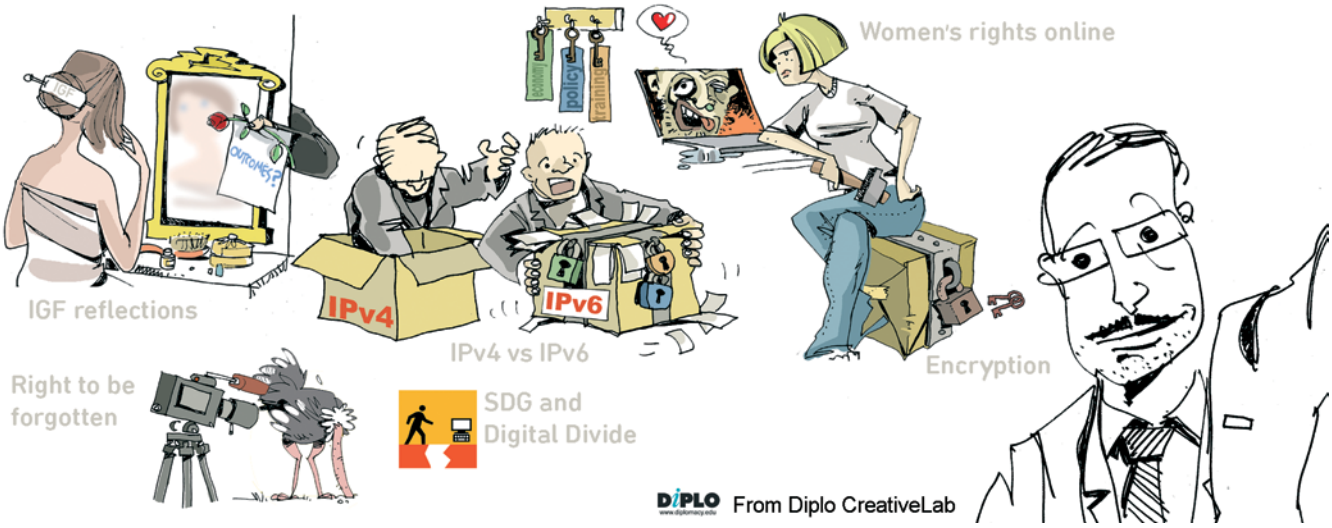
The two illustrations below are based on analysis of 19,218 tweets for #IGF2015, gathered between 9 and 11 November 2015.



Tweeting histogram
(for UTC time | Joao Pessoa is UCT – 3).

#hashtag cloud

IGF Selfie



DO NOT MISS TODAY

Death and the Internet – Managing Digital Legacies – 11:00-12:30 (Workshop Room 7)
This workshop was one of the most popular workshops at the auIGF in Melbourne, Australia last year. What happens to the online presence of those who have died? Do their loved ones have the right to access and control the digital impressions of those who have departed the real world? Have you considered leaving your digital presence to someone in your will?

A Dialogue on "Zero Rating" and Network Neutrality – 14:00-16:00 (Main Meeting Hall)
Net neutrality and zero rating have been hot topics at IGF 2015. Some see zero rating as better than nothing; others see zero rating as worse than nothing. This main session will hear reports from workshops on these topics and continue the discussion with the aim of providing participants with a more well-rounded understanding of the issues at stake.

Building Internet Observatories: approaches and challenges – 14:00-15:30 (Workshop Room 9)
In response to a need for an easy and functional access to digital policy information, many observatories and mapping projects have been created. The roundtable organiser posed the following leading question: How can different projects create synergies, avoid duplication of efforts in their activities and foster cooperation among different projects to leverage capacity-building and education as well as policy-making vis-a-vis Internet governance?

Viable application & debate: online participation principles – 16:00-17:30 (Workshop Room 8)
The process of developing e-participation principles as a substantial part of the IGF meetings, which started a few years ago, has seen a rapid integration of e-participation into many IG meetings. This year, the workshop will present the **principles** as a formal and tangible output of the IGF.

Session on Dynamic Coalitions – 16:30-18:00 (Main Meeting Hall)
Dynamic Coalitions weren't part of the original IGF mandate. Instead, they started to emerge organically during the first IGF in 2006 as people with similar interests decided to work on very specific topics. Joao Pessoa will be the first time that these Dynamic Coalitions have the opportunity to present their work to the larger IGF community for their consideration and feedback.

ANNOUNCEMENT

Get-together for Diplo & GIP alumni: Thursday at 17:45 at the booth

Diplo & GIP alumni are invited to the traditional IGF get-together for alumni, on Thursday at 17:45, at the Diplo/GIP Booth. As always at the IGF, we would like to meet you to touch base, and learn about the activities you are involved in. Join us at the booth – we look forward to seeing you!

IGF Daily is prepared by *GIP Digital Watch* with support of the Internet Society and DiploFoundation
Geneva Internet Platform DigitalWatch
Internet Society
DiPLO www.diplomacy.edu