Report of the

5th Internet Governance Forum

Vilnius, Lithuania,
September 14-17, 2010

Prepared by Monika Ermert
For the CENTR secretariat

Table of Contents

Highlights

IGF at the end of it's first five-year mandate: In search for tangible outcomes

Despite a lot of enthusiasm by private sector, non-governmental organizations and many governments about the multi-stakeholder dialogue established by the Internet Governance Forum (IGF) the forum is at a cross-road. The five year mandate the forum was bestowed with by the Tunis World Summit of the Information society in 2005 will run out by the end of 2010. The UN Secretary General, Ban Ki Moon, following open consultations at IGF 4 in Sharm El Sheik (2009), has recommended a second five-year mandate, but the final decision will only be taken by the General Assembly in New York later this year.

Participants reflect on IGF results

So the time had come for many attendees to reflect on the results so far and if coming is worthwhile. IGF secretary Markus Kummer has an easy answer to this: people from all stakeholder groups show up in numbers every year (2010, 1400 active participants from 107 countries, delegations from 79 countries and more than 600 remote participants, including people from more than 30 hubs worldwide). Many were glad, Kummer said at a press conference, about the non-negotiating format.

A government representative from South Africa on the other had said, the IGF should be able to come out with some results in the future. „Recommendations“ or at least „messages“ from the IGF were covered by the existing Tunis Agenda. An expert from the Council of Europe said there seemed to be a need for a „new impulse“ for the IGF to get it going. A representative from the RIR community on the other site described the meeting as „fruitful“ and applauded the quality of many workshops. From the perspective of the technical community the much toned down criticism towards the Internet Governance self-regulatory bodies must be viewed a clear success.

While the US dependence of ICANN/IANA and the perceived unevenness of IP address allocation led to heated debates in earlier years, now the respective sessions were much about information about the status quo of IPv6 deployment, roll-out of IDNs and the start of the work of the international ICANN review team (http://www.icann.org/en/reviews/affirmation/composition-1-en.htm). Kummer said during a press conference while management of critical Internet resources couldn't even be put on the agenda during the first IGF, the critical Internet resources session had become nearly „boring“. It’s an interesting question if discussion of some of the still controversial issues, for example the future of IANA (see below) have moved on to other fora.

Dispute about who will decide about IGF reform

While one can safely assume that the IGF will be continued, there is considerable discussion about necessary changes with regard to the IGF-format and output. And not only is there a lot of discussion about how substantive the change has to be, but there is also a barely hidden dispute about who should decide and develop reforms and which United Nations body the IGF should be attached to.

Both the New York based Economic and Social Committee (ECOSOC) and the UN Committee for Science and Technology for Development (CSTD) claimed responsibility for overseeing the process. During a special session of newly established working group of the CSTD, led by Swiss Ofcom official Frédéric Riehl, alongside the IGF in Vilnius the question about who was in charge became visible.

Riehl announced his intention to start consultations on the IGF's format, output, working methods and outreach early because of the limited time. But the Chinese delegation said the CSTD group should not duplicate work and wait for the UN General Assembly to decide on continuation and necessary reforms. The Chinese contrary to the majority were clearly against allowing the CSTD working group to be built along the old Working Group on Internet Governance (WGIG) model, so as to allow all stakeholder groups to participate on an equal footing.

In a conversation Wolfganggg Kleinwächter, long-time IGF expert and special advisor to Nitin Desai said to this reporter, he was concerned that there were governments who did think „now we've had enough of the multi-stakeholder model". The considerable independence of the IGF and its secretariat could be crushed, Kleinwächter is afraid, when governments during the General Assembly would decide to move the IGF secretariat to the UN headquarter in New York, attach it closer to the UN's bodies responsible for development (namely the Millennium Development Goals) and possibly even decide in favor of a classical intergovernmental bureau to decide on the IGF program.

The International Telecommunication Union that was very quiet during the Vilnius IGF was already there as it has moved the so called WSIS forum that is much more government oriented to New York.

Secretary Kummer confirmed in a very open statement during the press conference that some member countries did not feel at ease with the IGF setting where there were no flags and reserved seats for governments and where „everybody who runs the Internet has a front-row seat".

Tangible outcomes

The ones from the front seats on the other site are clearly aware that dialog at the IGF and politics back home are worlds apart. Lynn St. Amour, president of the Internet Society, warned during the opening session: „It seems extremely unlikely that closed processes will lead to policies that support a truly Open Internet". St. Amour pointed to the ACTA negotiations, the net neutrality debate in the US and the locking down of the Internet under the disguise of cybersecurity as negative examples that were ongoing alongside all the nice talk at IGF.

Jeremy Malcolm from Consumer International said, decision makers had „either been oblivious to or perhaps even deliberately disregarded the best practices shared at the IGF so far." Discussions at the IGF on issues such as human rights in the Internet, network neutrality and the development intervention of Internet governance were insightful, relevant and did not occur anywhere else in such a multi-stakeholder fashion, but „the next step for us is to focus those discussions, reduce them to a form that policy makers can use, and make sure that they don't end here at the IGF."

How big the appetite is for „tangible results of the IGF" becomes obvious when looking at the many „principles" proposed in the various workshops at Vilnius:

- principles for civil rights on the net (with a 10 principle document from Brazil taking center stage in Vilnius, there is also a dynamic coalition working on this)
- guidelines for intermediary liabilities (on set proposed by the OECD, another by EFF and others)
- duties for states regarding the integrity of core network infrastructures (Council of Europe and others)
- code for transparency in Internet Governance (Council of Europe)

Even Markus Kummer, always cautions with regard to IGF recommendations, said when asked what he thought of the Brazilian Internet Governance and Use principles: "I for myself would happily endorse them, put them on our website as IGF core principles, but I know that may be jumping it a bit as we've always shied away from doing that sort of thing."

On a somewhat more practical note, CENTR presented its contribution to the „tangible result" during several workshops: the organization is building up a database about fields of expertise of its members, also coordinating with its sister organizations AFTLD, APTLD and LACTLD. „Instead of informally exchanging information between the all four regional organizations we're effectively going to build a knowledge platform that will group basically all ccTLDs across the world, and this again would focus on operational issues", said Peter van Roste, representing CENTR during the plenary on critical infrastructures.

Internet Governance I: IANA discussion cut short

The IANA contract between ICANN and the US Department of Commerce (DoC) comes to a close in September 2011. A separate contract between the US DoC and VeriSign over the management of the master server – for distributing the root zone file – runs out 2012. This issue, according to Milton Mueller, one of the real governance issues was somewhat kept off the table during the plenary on managing critical Internet resources.

Bertrand de la Chapelle, French Foreign Ministry official who will soon leave government service to become a member of the ICANN Board of Directors, pointed to both issues saying that change might become difficult (especially for the US site) if there was no guarantee for the same level of stability and security as under the current regime. Syracuse professor and Internet Governance Project co-founder Milton Mueller reminded the audience to earlier proposals to split IANA into several functions, namely the DNS and root function, the IP address allocation function and the registration of protocol parameters.

The split had first been proposed by RIRs back at the Shanghai meeting of ICANN 2002 before ICANN and the RIR community came to terms about their respective competencies and the RIRs fought against ICANN in what they saw as intervening in their work.

But moderator Chris Dispain was quick to say that as a lawyer he was aware that no answers to the IANA questions could be expected as legal issues were involved. Mueller posted a highly critical note on the debate on the Internet Governance blog about a „a lack of substance (that) has been institutionalized in the IGF". The IANA debate had been deliberately ignored.

Andrew McLaughlin, ex-ICANN, ex-Google and now Deputy CTO of the White House said to this reporter after the welcome session, that „we currently are checking how much flexibility we have". He did understand that „some parties were interested in not doing this as a procurement". McLaughlin did not touch this issue during his opening ceremony speech, that mainly circled around what can be described as the US IGF 2010 logo: „innovation without permission".

Contrary to their US counterparts two European representatives spoke about their expectations to reconsider the current IANA regime. EU Commissioner Neelie Kroes Public said: „Public authorities across the world must now be able, on an equal footing, to effectively carry out their roles and responsibility when international public policy issues are at stake. There are already some signs of progress and I see that ICANN is reviewing its working methods. And I'm hopeful that similar steps can be made when it comes to IANA functions. We need reform; but we don't

need a revolution.“ Kroes also welcomed that the Secretary General has started an official consultation on „enhanced cooperation“.

Kroes was backed up by French State Secretary for Forward Planning and the Development of the Digital Economy, Nathalie Kosciusko-Morizet, who said: „What France seeks to do and what Europe will do under the impetus of Neelie Kroes the commissioner will not be enough if we do not have international level reflection, and discussion on Internet Governance including the subjects that come under ICANN“.

One long-standing critic of US oversight did not show up at the IGF at all, Arab countries were represented much less this time at the IGF. Have they given up on the IGF or were conflicting UN conferences the reason for this? Perhaps the Arab countries just calculated that not much might happen before the start of the new IGF mandate.

Internet Governance II: Routing Security RPKI

The effort to secure routing using a Resource Public Key Infrastructure was discussed in a panel co-organized by Milton Mueller, co-founder of the Internet Governance Project and the RIRs. It was one of the more geeky, but also more controversial topics with regard to critical infrastructure management.

The five RIR have committed to officially starting certification for IP addresses Jan. 1. The certificates and the Resource Public Key Infrastructure (RPKI) would make it impossible to hijack traffic as was done in the diversion of YouTube traffic to Pakistan Telecom, the RIRs said. But a European Union representative and academics from the Internet Governance Project said they fear a power shift from Internet service providers to the RIRs.

John Curran of the North American IP registry ARIN said it's good that RPKI would allow networks to "look up the public certificate and check 'did I get this from the service provider, that you said you've authorized to connect you to the Internet?'" He rejected worries about political implications. "You could as well talk about the political implications of a screw driver." There would be no big change in the routing system, Curran said.

But service providers could lose their autonomy, because the RIRs could revoke IP address resources, warned Syracuse University Professor Milton Mueller, an IGP co-founder, and Brenden Kuerbis of IGP. Use of a fully deployed RPKI would mean that many IP addresses without valid certificates would be dropped and become unavailable.

"This is a big change," said Malcolm Hutty, president of EuroISPA. He said there's a need for policies defining the rules for revocation. "For example, if a policemen shows up at the RIR's door and says, 'On this address block over there, there is bad stuff happening which is against the law, and we would like you to revoke the certificate of that address block so that it's no longer generally routable,' what is the RIR's policy on that going to be?" Now, Hutty said, the RIRs could just say "sorry," because routing decisions are made independently by each provider.

Steven Kent of Bolt, Beranek and Newman, who's one of the RPKI developers, pointed to a document introduced at the Internet Engineering Task Force that would allow every provider to produce its own routing table and literally overwrite untrusted routing recommendations by its RIR. Kent and the RIRs also said the use of the certificates is voluntary.

Once large providers implement RPKI there would be at least "a strong encouragement" for smaller providers to do it, too, said Andrea Glorioso, policy officer of the EC DG Information Society and Media. Glorioso also compared RPKI to Domain Name Security Extensions (DNSSEC), which similarly sought to secure the domain name system through digital signatures. For now, the five RIRs have decided to pass on a central trust anchor, but for the technical experts a central trust anchor at the Internet Assigned Numbers Authority (IANA) was the natural choice.

IANA, which oversees the DNS root and holds free IP address blocks is managed by the ICANN under contract with the U.S. Department of Commerce. Because of U.S. oversight over IANA, Glorioso said RPKI could run into the problem DNSSEC did, because it would be giving "more power to one single government than to others, and for governments and public authorities this is quite an important point.“ A way to solve the central authority question would be to split IANA and hand over the IP address function to the Numbers Resource Organisation, the RIR body, some experts said. The IANA contract is up for renewal next year.

Kuerbis said there's a potential for RPKI "to centralize authority" and provide "a target for regulatory action,"The history of RPKI showed the Internet-specific role that governments like the U.S. play in nongovernmental Internet governance institutions. With RPKI, Kuerbis said, "we've seen the U.S. government has succeeded in participating and shaping the bottom-up standards and policy development process at the IETF and the RIRs, by contracting with science and researchers to do research on the relevant standards and then interact more or less as peers with other participants in the development process.“

Main other topics

Governments' hot topic: Security and Cyberwar

The growing arsenal for cyberwarfare in the hands of countries and their citizens and statements by some military officials, including those of the U.S., that attacks on the critical network infrastructure would justify armed responses has raised concerns among diplomats. When the Council of Europe presented a draft on "Duties of States" on protecting Internet resources and cross border infrastructure at the Internet Governance Forum (IGF), international law experts warned about possible consequences.

The CoE draft proposal covers government duties to take "measures to prevent and respond to" interference with the Internet. It would hold governments liable for acts by their citizens. The draft said Internet users must be prevented from "involvement in cyber attacks and other forms of malicious use of the Internet." This would bring international courts a heck of a lot new cases immediately, said Jovan Kurbilja, director of the Diplo Foundation.

The draft would "lead to a reaction from governments to step up surveillance of their citizens in order to avoid incidents and being held liable for it," said William Drake, senior associate at the Center for International Governance of the Geneva Graduate Institute for International and Development Studies. Drake said deep packet inspection might be a natural result. A member of a Western government told this reporter that parts of his government could be well interested in such an option. In fact more network monitoring was already on the rise. Europe might be interested, according to the government

representative, to do some advance planning as there were discussions about possible „duties“ and „responsibilities“ the US government wanted to push forward with.

Academics confirmed that there were internal discussions in the US about this topic. There is also a proposal co-sponsored by Senators Hatch and Gillibrand that wants to introduce a benchmarking of Cybercrime prevention measures of countries worldwide: „Countries of cyber concern that do not reach their benchmarks may have one of the following benefits suspended, restricted or prohibited: new OPIC or ExIm financing, new multilateral financing, new TDA assistance, preferential trade programs, or new foreign assistance, as long as such do not limit projects to combat cybercrime.“

Members of the CoE working group on the document said they were open to proposals for the document and discussion had only started. The working group also proposed citizens' rights on the Internet, and enshrining values such as openness and net neutrality and limitation of liability. The main goal, a CoE expert said to this reporter, was to protect the international infrastructure.

Google evangelist Vinton Cerf tried to tone down the Cyberwar rhetoric during one of the Cybercrime panels. Cyber attacks were more about guerrilla than about war. He recommended a Cyber fire departmentto help to put out cyber fires first before starting investigation – not to talk of cyber counterattacks.

Liability y for Intermediaries

Not only countries hold liable for their citizens, but also Internet intermediaries hold liable for their customers' possible offenses might become over regulating, over reacting and turn to more surveillance.

The long-sought system of immunity from liability for Internet intermediaries such as ISPs is under attack, not only in Third World countries, but also in nations that opted to protect intermediaries before, experts told the Internet Governance Forum. Several coalitions and organizations, including the Organization for Economic Co-operation and Development (OECD), are trying to come up with guidelines or principles against over-regulation.

The big push resulted from "the concerns of the copyright industry, the content industry," said Lilian Edwards, professor of Internet law at the University of Sheffield and contributor to a OECD study on the situation. "They want a three strikes regime, pre-emptive filtering, website blocking and even deep-packet filtering." Content owners contend notice and take down isn't adequate and they want to "move on" to some sort of "notice and disconnection or graduated response," she said.

Unwanted material, from extreme pornography to hate speech or predator material, and "the idea that we are facing a cybersecurity crisis, and" and that ISPs might "perform a role in trying to identify and isolate zombie machines," also are behind the effort, Edwards said. Major questions include if providers could do this, could identify the traffic and what the implications for privacy and autonomy for the subscriber were, she said. "How do you identify the good and bad traffic?"

"The system is under pressure," said Marc Berejka, senior policy advisor of the U.S. Commerce Secretary's office. "When content owners signed up to the Digital Millennium Copyright Act, they expected they would send a notice to the ISP, the ISP would receive that and then take the content down." Experience has shown pirates are moving very fast, he said. "Notice and take down has proven of very limited value.“

Rather than giving up existing immunities that had proven economically valuable, the Obama administration would like to see what could be done by cooperating with big providers, Berejka said. Technologies like Google's content ID were an example for this effort. The Commerce Department is also aware of pressure on U.S.-based companies from other countries to exert ex-ante or "before the event" censoring of content. Because of the global pressure, the Commerce Department established an Internet Policy Task Force to address the question.

As a possible answer to the problem, the OECD has developed a set of "good practices." The OECD ministerial committee will decide Oct. 1 if the guidelines will become a legal instrument, which would include 2-year implementation reports about the member states, OECD expert Karine Perset told us. The principles include the provision of "appropriate protection and liability and remedy limitations to Internet intermediaries for actions of third party users," inclusion of stakeholders in respective policy-making processes, caution not to jeopardize investment, considering social cost and externalities, and undertaking cost-benefit analysis that assess costs and benefits to intermediaries and other affected parties.

The proposed principles request that governments "encourage and support private sector initiatives to self and co-regulation and international cooperation." One meeting participant warned against putting social costs and externalities — including loss of freedom of protection but also negative effects for innovation — behind the sheer issues of cost. At a separate panel organized by the Electronic Frontier Foundation, Association for Progressive Communication, Google, Council of Europe, the Swiss Telecom regulator, Austrian Federal Chancellery and others,

Eddan Katz, EFF international affairs director, said EFF was considering its own set of principles focusing on human rights and freedom of expression. The panel heard reports from a variety of countries about chilling effects for intermediaries.

Using the IGF, for example Brazil, Google, CoE

It is interesting to see how some stakeholders make use of the IGF, and here are some examples of companies highly visible at the IGF and there declared or obvious strategies for IGF engagement.

Government example: Brazil

The Brazilian government showed up with one of the larger delegations (like 2011 host Kenya and the US) and presented their Internet Governance and Internet Use Principles in various plenary sessions and workshops. While the delegation strongly supported IGF continuation, it made clear that it favored a more active role of the IGF in setting Internet Governance recommendations in the future. Brazil's New York Ambassador Everton Lucero also reiterated the old Brazil request for a regime change in Internet critical resource management, presenting a paper on „Global Governance of Critical Internet Resources: A perspective from the South.“ during the academic GIGAnet pre-event. Lucero while speaking in an individual capacity according to his statement said the current regime (of root zone oversight) still was only open to changes within the regime (and not real change).

Company example: Google

Max Senges from Google's policy team in Germany explained one of the motives for tech companies for coming to the IGF with relatively large groups during a session with members from the German Parliament (who participated remotely in a German IGF regional session, one of many national and regional IGF sessions during the week). Senges pointed out that Google wanted to use the IGF to present „integrate“ new services developed by Google into the discussion at large. Referring to the street view debacle in Germany where citizens in large numbers currently file objections to having their houses displayed on the web tech companies had to engage in discussion about their services all the time. Google together with Microsoft promoted the Global Network Imitative (GNI), a self-regulatory exercise in balancing investment and human rights policy.

International Organization: Council of Europe

According to this reporter's observations the CoE is the winner when it comes to promotion for its legal instruments during the IGF, in part this may result from the pretty aggressive public relation work of the CoE during the IGF. In fact the CoE promoted not only the Cybercrime Convention, a „standard that has be developed regionally, but can be implemented internationally“, as CoE never cease to underline. The CoE also promoted a Code of good practice on information, participation and transparency in internet governance together with the Association for Progressive Communication, it presented ideas for the update of the Convention 108 on privacy and tested the waters for two new legislative efforts underway: a possible document for the protection of critical resources (see above) and another possible recommendation for a system of „graduated responsibility“ for content on the Internet to freshly tackle the much debated question of liability on the net. Especially with regard to the latter two projects one should note that the CoE obviously decided to bring these early to the community in order to look for responses and objections possibly. Contrary to the ITU that seems to have given up on the IGF for now (ITU was much less visible during the Vilnius IGF than during earlier IGF's, see above), the CoE was running a lot of panels and participating in more.

Dynamic Coalitions

Several Dynamic Coalitions met during the IGF in Vilnius, but progress in the Coalitions has been slow with a few exceptions, notably the Internet Rights Coalition. Some of the Dynamic Coalitions even are dormant – or perhaps even dead, like the access2knowledge DC. The considerable cut in the IGF activities of the ITU also resulted in less activity of several of the ITU initiated Dcs, like the one on climate change, but also the one on the Internet of things. Dcs quite obviously tend to go dormant when a core group or figure moves on to other work with or without taking the topic there.

Jeremy Malcolm from Consumer International put it best in his closing speech, saying that the Dcs did not as much become the producers for recommendations as first envisaged. There might be, he said, a need for DC 2.0.

The next IGF will take place in Nairobi, Kenya, next year.