



## **REPORT 2014**

**13 February 2014**

### **Report**

#### **Sponsor's Welcome, Lesley Cowley, CEO, Nominet**

Lesley Cowley outlined how Nominet had been active in the IGF since its creation following the World Summit on the Information Society in 2005. She thanked all of the stakeholders who had joined together to develop the programme and enable the meeting and pointed out that this is good evidence of the support in the UK for the IGF process. Lesley welcomed the engagement of new partners this year and called for this to continue to grow going forward.

Lesley explained how the IGF is important as it provides a much needed space for governments, industry and civil society to work together and to share understanding on Internet governance issues. She suggested that it helps us all to understand issues better and to make better decisions. She recounted how the UK has always taken the IGF very seriously and it was this that led to the creation of the UK-IG. Lesley explained how she believes that UK-IGF provides an opportunity to help us all to contribute more effectively to the IGF, and to help us learn from the IGF. She explained that this is why Nominet continues to support the UK-IGF by sponsoring annual events, being active in developing the programme and promoting engagement.

Lesley expressed gratitude to the successive Ministers who have supported the UK-IGF and stressed that this support does help to underline the importance that the Government gives to promoting multi-stakeholder dialogue on Internet governance issues.

#### **Plenary One: What is your vision for governance of the internet?**

Panel:

- Dr Vicki Nash, Oxford Internet Institute, University of Oxford (Moderator)
- Alex Blowers, Nominet
- Chris Disspain, AuDA (remote)
- Lea Kaspar, Global Partners Digital
- Jamie Saunders, FCO

This session focused on the global internet governance landscape, examining the driving forces for change and the meetings and milestones for 2014 and beyond. Key points from the discussion were: Political tension has caused the second committee of the UN General Assembly to set up a separate group to discuss the modalities necessary for the WSIS review. Therefore it is very unlikely that we will see a UN central body due to lack of consensus. Several speakers felt that the discussions around the globalisation of IANA are low hanging fruit so this may be achievable in 2015. Tensions are going to continue to grow on the discussion of the future of IGF and the Brazil meeting offers an opportunity to find some middle ground. Some of the panel hoped that we can begin to shift the debate back towards more practical themes rather than being dominated by politics. If we turn the IGF into a decision making process then the true value of it will be lost. Going forward we need to make sure the ethos serves the next billion users - who will come from emerging markets. We need to find a way to engage Internet users into these discussions.

Conclusion: It is important that we try and develop a proposal for concrete reforms, listen to the next billion users be realistic about what the issues and drivers for change are.

**Keynote: Hon Ed Vaizey MP, Minister for Culture, Communications and the Creative Industries: Discussion on the future of international internet governance.**



The Minister outlined how he had been participating in the UK IGF for many years and had attended several International IGF's including Kenya and in Azerbaijan. He praised the work that former Chair of the UK-IGF Rt Hon Alun Michael did on keeping these issues alive in Parliament, highlighting that it was very important that Parliamentarians, not just Government are very much involved and alive about the issues. The Minister welcomed the engagement of Alun Cairns MP who he said had done a fantastic job in picking up the baton and keeping IGF issues at the very much front and centre in the minds of Parliamentarians.

The Minister noted that Internet Governance remains as lively a topic as it has always been and that this year is going to continue to keep it front of mind. He set out key events, such as the meeting in Sao Paulo in April, the WSIS +10 review and the ITU's Plenipotentiary. He reassured the audience that the Government are preparing for all of these and want to make sure that they are as fully prepared as possible which means taking into account the views of UK Stakeholders as well. The Government's aim remains exactly the same as it's always been which is to protect and strengthen the multi-stakeholder model for Internet Governance. They want the internet to remain open, global and secure. He stressed that the Government do not want top down Government control of the internet, or a multi-lateral framework of governance which put Governments in the driving seat. They want to resist that pressure because they think it will lead to threats to freedom of expression, social development and to economic prosperity. The Minister acknowledged that the current model is not perfect, and that they have always said there is room for evolution.

The Minister highlighted the following questions: How do we globalise accountability for internet resources?

What should be the roles of international internet organisations? How do we ensure that critical technical functions are not compromised by political agendas? How do we continue to strengthen the IGF - what changes do we need to make in order for the IGF to be more accessible, more navigable, for it to develop more effective and practical output? How do we improve the role of GAC within ICANN? Do we need new ways of working to ensure that public policy interests are taken into account from the earliest stage? What role could a single set of high level principles play in guiding Internet Governance debates?

The Minister concluded by stressing that we need to develop our thinking and our arguments in ways which take into account the perspectives of other Stakeholders and also of course other parts of the world. He felt it is important that we are aware of how others see us and we take into account what can be legitimate concerns, reevaluating how we work in international forums, how we work with international organisations and what needs to be done so that all Stakeholders feel they are playing on an equal playing field. We need to reach out more and be more inclusive. He noted that the Government will play their part, but it must be a UK wide effort, it must involve industry, it must involve civil society, it must involve other Stakeholders and that's why the UK IGF plays such a valuable role.

### **Three parallel workshops**

#### **a) Is the UK setting the standards for child online protection or going over the top?**

Panel:

- Simon Milner, Facebook (Moderator)
- Dan Butler, Virgin Media
- Will Gardner, Childnet International
- Jim Killock, Open Rights Group
- Jeremy Olivier, OfCOM

SM introduced the panel posing the questions:



- Why is that workshops on internet governance and child protection tend to be safety people talking to more safety people?
- Is the UK perceived as the country that thinks it controls the internet in relation to Child Online Protection (COP)?

Each panellist was asked to give a short presentation:

Will Gardner CEO of Childnet reported that at IGF Bali the Childnet Young Peoples' panel session was oversubscribed and that people clearly wanted to hear directly from young people. The theme was 'online anonymity' and the panel presented the findings of research that people from over 60 countries participated in. The young people were very clear about the benefits of anonymity as it helped to keep their personal information safe, but they also recognised that it can be used negatively too.

Will also presented the headline findings of 'Have your Say' in which 24,000 young people (12,000 from secondary schools and 12,000 from primary schools) took part making it the largest survey of its kind. The main concern for children aged 7-19 was "mean comments". Children aged 7-14 would go to a parent first for help, so it's important not to underestimate the parent in online safety. From 14+, they would go to friends first, though parents remained a close second. The key lesson from the young people was "inform us, don't scare us" - they wanted good education about how to use safety tools.

Jeremy Oliver from Ofcom presented the findings of detailed research into parents' confidence and young peoples' risk on the internet.

The research showed that 85% of parents undertake at least one of three methods of control:

- (i) Supervision;
- (ii) Regular engagement about online risks; and
- (iii) Technical tools/filtering controls.

The proportion of parents who are concerned about the internet has gone down.

The report also highlighted that 8% of children aged 12-15 reported that they had been bullied online in the past 12 months. However, a larger proportion of children had seen something that had concerned them on TV than on the internet

Jeremy felt that any intervention from the media to increase protection for children will have risks as well as benefits. For example, the 9pm watershed provides clarity about content on TV but this can be circumvented by catch up if there is no PIN control in place.

Daniel Butler of Virgin Media talked about the introduction of parental filtering which the four major ISPs have committed to introducing to create a safe online environment. This is not default filtering but 'Active Choice' which gives parents the choice about whether they want to introduce filtering. Virgin Media undertook research with their customers and 86% said that it was the responsibility of parents to decide what content is accessible in the home.

Virgin is committed to making their service as transparent as possible – pre-ticking is not the default setting, instead parents have to confirm their choice. The account holder will also be informed if any changes are made to controls. Virgin recognises that filters are fallible and never 100% accurate. Filters are a technological solution and are circumvent-able. They are concerned about over blocking and therefore they encourage customers to contact them if they believe they have been over blocked.



The four major ISPs have committed £25m to a national safety campaign. They also believe that this still leaves a gap which NGOs fill by providing good objective safety advice to parents. Jeremy reported that DCMS had asked Ofcom to look at the ISPs implementation of content filtering, not checking over/under blocking, but focusing on procedures for reporting, consistency of blocking decisions and transparency about complaints.

Daniel stated that the four ISPs have agreed a self-regulatory approach and are committed to the same policy objectives. They are moving faster than other international comparators. They have agreed consistency in terms of blocking and will block types of content not URLs. They have also agreed the categories that they decided to add to filtering by talking to key NGOs, Claire Perry, Helen Goodman etc. and they unilaterally agreed on the types of content to be blocked.

Peter Bradwell from the Open Rights Group (ORG) stated that child online protection is a serious issue and there is a huge amount of excellent work that has been undertaken by researchers and academics. The ORG's concern is the approach taken by policy makers and specifically by the Government which they believe has reduced the issue to a referendum about whether we care about children instead of being evidence based. They think the Government's position is unhelpful, superficial and divisive as it takes the focus away from the real concerns about filtering. They believe that internet policy cannot be driven by a Government which has grasped the issue as moral purpose.

Simon asked the panel if other countries can learn from the UK's approach. Daniel outlined how Virgin is now part of Liberty Global and is aware that other countries are looking to see what happens in the UK. He has some concerns that the conflation of issues in the UK, and perception of default filtering could have ramifications in other countries. Peter felt that other jurisdictions can learn from the UK both the good and bad, although this depends on the UK adopting a transparent approach to reporting mistakes. Jeremy suggested that the actions of the four ISPs should not be taken as an indicator of how the internet should or shouldn't be governed. The industry has been placed in a difficult position as the decision on what to block was devolved to them with the responsibility to implement any solutions, so they cannot be chided for then offering parents what they said they wanted.

There was a discussion about whether there were lessons to be learnt on internet governance good practice from the field of child online protection in which all the key players worked together on a voluntary basis and were very effective. Surely, this is a model of multi stakeholder practice that could be replicated in other areas of cyber security?

## **b) Will Internet governance principles enable a better Internet?**

Panel

- Matthew McDermott, Access Partnership (Moderator)
- Paul Blaker, DCMS
- Marianne Franklin, Goldsmiths (University of London)
- Nigel Hickson, ICANN
- Jean-Jacques Sahel, Microsoft
- Matthew Shears, Center for Democracy and Technology

Throughout the session, speakers reaffirmed the importance of ensuring all sets of Internet governance principles have multi-stakeholder support. Only by guaranteeing a multi-stakeholder process for the development of Internet governance principles can they have legitimacy across all stakeholder groups. While it was agreed that a single stakeholder group cannot be allowed to decide on the rules of the road for the Internet, there was also agreement that principles for specific topics may need to be developed by subject experts, requiring some flexibility in how we approach the development of Internet governance principles. The Netmundial conference in Brazil was seen as an opportunity for the global community to agree on some core values, but there was also scepticism as



to whether the Brazil conference will produce any concrete solutions to the concerns the global community has about the existing model of Internet governance.

### **WHAT IS THE POINT OF INTERNET GOVERNANCE PRINCIPLES?**

A primary reason given to support the development of principles was the importance of putting principles down on paper. Seeing them written down immediately gives principles legitimacy, and allows a wider audience to compare them against their own principles and experiences. This transparent sharing of principles enables the creation of an effective “market for principles” – only those that have relevance for a wide range of Internet users in different stakeholder groups will survive.

Principles also play an important role in helping to develop common ground between parties. This is especially important where there is widespread disagreement on an issue or range of issues. By starting with principles, rather than binding legislation or international law, we can begin the process of building bridges between parties. Developing a set of principles that all parties can agree on is the first step towards a more democratic and multi-stakeholder approach to Internet governance issues.

However, criticisms were raised relating to the implementation of existing sets of principles. More is required on a practical level. Further, there is still a lack of guidance on who is responsible for specific policy issues, even where agreed principles already exist. It was noted that the treaty text agreed as part of the World Summit on the Information Society (WSIS) is the only text which has agreement from all global stakeholders, yet there has been insufficient effort to implement the actions it proposes. It was suggested that the global community should do more to rectify this problem.

The group debated whether there are a common set of themes that can be used to identify good principles. Ideas that came up included:

- future proof,
- high-level,
- agreed (by all stakeholders across all geographies), and
- Respect for human rights.

In addition, there was agreement that a good set of principles should work well and efficiently, and be straightforward to implement in practice. A possible derogation from the common themes could be technical principles, which may be required to abide by different guidance, depending on the context within which they are developed.

There was a lot of discussion about what can be expected to come out of the Brazil conference. It was agreed that it will be difficult to agree on the more difficult and contentious issues in Brazil, such as net neutrality. A more positive approach would be to focus on the core issues where agreement can be achieved between all stakeholders in the two days available for the conference. A suggestion that received support from many of the attendees was for the Brazil conference to develop principles on process, with the aim of filling in some of the gaps in existing mechanisms. This would help in the development of ‘rules of the road’ - providing guidance for the development of future sets of principles on specific issues.

The discussion also agreed that all actors in the Internet governance space must be aware that we cannot take the status quo for granted. Following the Snowden revelations we have entered a new era of Internet governance, and we may need to use the Brazil event to focus on rebuilding trust before all stakeholders are able to work together to create agreed sets of Internet governance principles.

No one at the session expected the Netmundial event to solve any problems, and the general perception is that it is the start, rather than the end, of a process. There was clear agreement that we need to identify the next steps to build on the outputs from Brazil, and ensure that we do not lose momentum. It was also noted that over the last six months there has been a growing realisation that



Internet governance and surveillance issues should be treated in different fora, and many attendees hoped that the Brazil conference will be able to separate these issues out, rather than producing outputs where the two are conflated.

### **c) Surveillance and Law Enforcement**

Panel:

- Ian Fish, BCS (Moderator)
- John Doody, BCS
- David Williams, BCS

Ian Fish led the panel on behalf of the BCS with John Doody and David Williams all are members of the BCS Security Community of Expertise. This Workshop focussed on Surveillance and Law Enforcement on the Internet. It was a response to the international reaction to Edward Snowden's revelations which started last year about NSA surveillance operations. In the view of BCS, the Chartered Institute for IT, these leaks have severely damaged trust in the Internet and a rational debate is needed to restore that trust and ensure that the free open global Internet is not compromised by individual Government's responses to intelligence surveillance operations.

Ian began by outlining the key issues, particularly those of trust post Snowden and sought views on how we restore trust in the internet. John considered the issues from the UK government perspective, in particular the legal framework for government surveillance and the need to understand the risks from criminals, hackers, terrorists and hostile intelligence services. David explained that NGOs and commercial organisations are also involved in surveillance for business reasons and explained the impact of Big Data collection and analysis.

Ian then threw the session open to the floor and a lively discussion ensued. Recurring themes focused on Snowden's revelation and their impact with little discussion on commercial surveillance. Three main themes emerged:

1. Data owners needed to take ownership of data about themselves and to risk manage where they allow it to go on the internet and how it can/cannot be accessed. This requires more education for internet users and examples of some schemes were cited. Who is liable for what and to what extent needs to be taken into account.
2. The need for anonymity was acknowledged but not really addressed in any detail.
3. Trust and the value of trust was discussed in some detail:
  - a. UK is in a good position in that lots of the world trust the UK more than many other countries and we tend to be a relatively law-abiding nation.
  - b. However, the outside world's perception of trust in the UK has been reduced as a result of Snowden's revelations but is still good.

There were fewer ideas on what to carry forward. In the main people were content with the current approach to governance of the internet and thought that "Balkanisation" was not a good idea. In the UK we need to be more positive publically on the good aspects of our system and encourage other nations to follow our example – e.g our oversight regime, accountability and application of the law. We need to ensure that the UK government uses our own laws properly e.g. Official Secrets Act, Data Protection Act, Anti-terrorist laws, e-Commerce law, RIPA etc (it was felt, however, that the wrong law was used to destroy the disc that David Miranda was couriering from Snowden to the Guardian). Above all, it was felt that what we need to improve was the perception of trust and to do that we need senior politicians and journalists to put a positive spin on the UK approach. At the same time we need



to improve policy in the background and as the internet is a global asset to push for an international legal framework such as encouraging other nations to support the draft UN resolution to provide a starting point for international law. It was recognised that data on digital networks is significantly different from previous systems such as telecommunications and this needs to be recognised in law.

## **Plenary Two: Cyber Security**

Panel:

- Amy Jordan, BIS (Moderator)
- Carla Baker, Symantec
- Dr Martin Koyabe, Commonwealth Telecommunications Organisation
- Simon McCalla, Nominet
- David Pollington, Microsoft

The session opened with the panellists discussing how we can encourage a responsible cyber-culture, both at a global and local level. The discussion noted that ICT is used differently in each country so technology providers have to find a way to help people to help themselves. Any solution would have to be collaborative so how do Government and industry come together to do this? It was felt that Governments need to create the right legislative environment that is consistent across borders. The “right” frameworks are the ones that mesh together and allow flexibility. Cyber security affects all countries but the approach is different between them.

The London Cyberspace Conference series (London, Budapest and Seoul) were highlighted as a good example of nation states coming together to examine shared challenges and attempting to develop common solutions. At the Seoul cyber conference a new theme of capacity building emerged which shows there is a growing understanding of the interconnectedness of issues and that one size does not fit all. It was generally felt that, although there are improvements to be made, the UK had a successful approach with Ministerial responsibility for cyber security, clear policy direction and drive from the Cabinet Office as well as interest from the Prime Minister and Foreign Secretary. There needs to be a strong leadership focus in order to try and build a successful solution.

The discussion moved on to consider what the role of Governments should be in this space. It was felt that governments have an essential role to work out how this can be done systematically, but one-off events are not enough. Governments have to lead by example - critical national infrastructure so they need to have their house in order. Only governments have the power to initiate, drive and lead overarching policies and they need to set a clear road map for industry and provide a suitable environment for collaboration.

The discussion then turned to education and skills. In terms of addressing the skills gap, the panel members thought that to a certain extent this is about finding less conventional ways of giving people opportunities and education. Technology is developing rapidly and education needs to keep pace with this. In the past companies just had an IT department, but now companies increasingly need their entire workforce to have cyber skills in order to maintain good cyber hygiene. Apprentice training is a successful model for skills building as it allows keen people to be trained in key skills as required.

The panel rounded off discussing the balance between innovation and security. It was suggested that we can't have one at the expense of the other. To counter this view, it was argued that true innovation is never at the expense of security because if something is inherently insecure, this means that it is actually not innovative as it creates more problems.



## **UK-IGF summer messaging session - 1 July 2014**

### **Report**

#### **Sponsor's welcome – Baroness Rennie Fritchie, Nominet**

Rennie welcomed delegates to the event which forms part of the UK's preparations for the global IGF in Istanbul. She thanked all of the UKIGF committee, the session organisers moderators and speakers who have coordinated the event and gave a special thanks to ISOC England for facilitating the remote participation.

The IGF is more important than ever before. It provides a much needed space for Governments, industry and civil society, to share understanding on Internet Issues and discuss issues with a range of stakeholders that they might not otherwise engage with. IGF helps us all to learn from each other and understand other's points of view in order to inform better decisions.

Support from successive Ministers demonstrates the Government's support for promoting multi-stakeholder dialogue on IG issues. Rennie thanked him for his continued personal support for the IGF and the UK-IGF.

Rennie emphasised the importance of dialogue and encouraged active participation from delegates during the day.

#### **Plenary One: Net governance: NETmundial, the London High Level Government Meeting, now what?**

Panel:

- Caroline Baylon, Chatham House (moderator)
- Dr Olivier Crépin-Leblond, Internet Society UK England
- Gabrielle Guillemin, Article 19
- Desiree Miloshevic, Afilias / Internet Society
- Sarah Taylor, DCMS

The panel opened by outlining the key Internet Governance development developments since the UK-IGF last met in February. The main headlines being the US Government's announcement that it intends to transition the IANA Stewardship and the Netmundial conference. The panel remarked that the debate which used to be about multi-stakeholder vs multi-lateral, has now shifted to discussing what a definition of what multi-stakeholderism means. The panellists felt this is an overwhelmingly positive step but cautioned that we shouldn't be complacent about this shift. They stressed that we need to think about how we work with those that disagree with multi-stakeholderism as well as those that agree.

The discussion of Netmundial focussed on the refreshing difference that the defined stakeholder queues made by ensuring that everyone was engaging in an interactive way but also on an equal footing. It was also felt that the Netmundial principles were a significant step forward as they managed to garner support across the different stakeholder groups. Overall there was a lot of praise for the Netmundial event and how open and transparent it was. It was suggested that the IGF should learn lessons from the success of the Netmundial event and how it was able to bring together a multi-stakeholder and multi-lateral approach into something collaborative and constructive .



The panel members also warned that Netmundial posed a risk as some governments have not endorsed it which risks fragmentation. However, there was a feeling that it was good for the Internet Governance society to see the dynamics of the process of making rough consensus, understanding complaints of others and making their own judgement on the issues.

The discussion moved on to the topic of inclusion. It was suggested that one of the downsides of the IGF was that it excluded those who are not “believers” in the IGF model. The panel felt that going forward the IGF needs to reach out to encourage those with more disparate voices to participate. The G77 countries need to feel that the forum is open to them discussing the issues of importance to them. In order to attract nations such as China and India, those involved in the IGF need to be pragmatic and demonstrate that good policy decisions can be made when all the experts are in the room rather than focussing on ideals and democratic processes.

An audience-member asked the panel to explain the value of the IGF and why people should participate in Istanbul this year. The Panel highlighted:

- The best practice forums will be launched at the Istanbul IGF and this will add a new dynamic to the discussions.
- Remote participation options are available for those not able to attend in person and the IGF was praised for its efforts to try and make participation as easy as possible.
- Historically Turkey does not have a good reputation for freedom of expression so this year’s IGF provides an opportunity to shine a light on these issues.
- For a number of stakeholders the IGF is their only chance to meet other stakeholders. The value of the “corridor” meetings was emphasised. The IGF offers a forum to provide answers and ideas to help with local problems. It was felt that this should be more pronounced if the Forum moves towards more output oriented focus.
- Multi-stakeholder discussion forums like the IGF take work and participation to be successful. If people do not go and make the model work then an alternative mechanism will be found.

The discussion also covered implementing outcomes from IGF’s and the question of the impact of previous meetings. The main point in the discussion was that the UK Government adjust and develop their policy positions based in discussions at the IGF and other fora.

Moving on to discuss drivers for change, it was felt that Netmundial is a big driver for change but it is not without risk. We should resist efforts to define MS roles. There needs to be flexibility in the system and participation should be encouraged in all areas. The IGF needs to be more focussed with more tangible outcomes and identify the big issues that people want to talk about. The discussion is not moving forward. It needs to bring in new people and look to find solutions. A shift is needed at the workshop level in order to produce the outcome based focus that people are calling for.

The Government position on net neutrality was clarified. There was concern that the kind of regulation being discussed in Europe is overly-prescriptive and isn’t going to allow businesses to meet their legitimate needs. At the moment there is no clear view on what is the right way to protect and enforce it. The government is keen to deliver on net neutrality but at the moment the correct way to do this is not clear. No definition of net neutrality – need to define the concept first. This has been included in the European Parliament text.

Thinking of the threats and opportunities in 2015, the panel felt that we are currently in a good place. Snowden has probably had a good effect as it has brought human rights to the centre of the debate and also has drawn senior government attention to the IG debate. Without Snowden the NetMundial would not have happened nor would the IANA transition. There is now a maturity to the debate.



**Hon Ed Vaizey MP, Minister for Culture,  
Communications and the Creative Industries**

Good morning. I'm honoured to be opening the summer meeting of the UK IGF. So a big welcome to you all. There is a lot happening this year.

The UK was privileged last week to be the host for the 50<sup>th</sup> ICANN meeting. We not only welcomed a record number of 3300 Internet stakeholders from across the world to London – but we also underlined the UK's key role in Internet governance.

It was also a very timely meeting: ICANN's primary role and accountability as the global coordinator for the Internet's domain name system is rightly under focus and scrutiny - as the US government now undertakes the long-awaited, final stage of the transition of the stewardship of the IANA function relating to the management of the root zone of the system away from government oversight, to the global community.

Governments need to contribute to the discussions leading to the process of transition and implementation of the new global IANA model - and this was one of the critical issues which were discussed at a high level governmental meeting which I chaired on the opening day of the ICANN meeting.

We also did a first take on the report of the ICANN Panel on Global Internet Cooperation and Governance Mechanisms chaired by the Estonian President, Toomas Ilves, and Vint Cerf. This is looking at how we can make decentralised Internet governance eco-system more collaborative and responsive to individual problems – for example in developing country economies which lack the necessary capacity and expertise. We in government have a key role, therefore, working with the ICANN community of stakeholders, to help that process.

Our high level meeting was of course also a first opportunity for ministers and senior officials to take stock of the NETmundial meeting in Sao Paulo in April and in particular how to implement the roadmap and action on specific issues identified in the principal outcome - the NETmundial Multi-stakeholder Statement which I'm sure many of you here today have seen.

That roadmap may have started in Sao Paulo but it led to London. Especially as I believe it is directly relevant to our meeting today. While we may have not achieved everything that we wanted in Sao Paulo – one key conclusion we strongly support and must do our bit to deliver on: improving the existing Internet governance framework and strengthening and evolving the multi-stakeholder model of Internet governance.

That model includes not only the global IGF but also the regional and national fora such as this one. The UK IGF was the first national IGF and has been the lynchpin and is the most visible manifestation of the multi-stakeholder model in practice in the UK. Here I must pay tribute to Nominet for all its hard work in supporting and organising UK IGF events like today.

This is a fast-moving space and NETmundial rightly said that there is a need to develop multi-stakeholder mechanisms at the national level because many issues should be tackled at the national level. Moreover, the Internet governance processes, mechanisms, and institutions should form stronger linkages. I support this outlook for the successful evolution of the multi-stakeholder model.

In particular I see great potential for the more tangible outcomes from the upcoming global IGF in Istanbul, feeding out for action or further development, to the regional and national IGFs, or depending on the issue, to the IETF (Internet Engineering Task Force), the Internet Society, ICANN or whichever institution is the most appropriate for the issue or problem in question.



We can also envisage issues or problems coming back to the agenda of the following IGF in Brazil next year – but not simply for a revisit or update – but crucially, the issue will have advanced – perhaps in identifying options for solutions - through some kind of distributed inter-sessional activity with the IGF providing the coordination.

So I offer this as food for thought today: as the UK IGF continues to build on its long history of success and effective practice in preparation for the next global IGF, should we develop a stronger linkage to the IGF on specific issues and outcomes - and in that way contribute to the inter-sessional activity that will ultimately produce concrete results.

I hope you have a successful meeting today – and I look forward to hearing your thoughts on how the UK IGF can contribute to implementing the NETmundial outcomes. And I hope to see many of you at the IGF in Istanbul in September.

### **Three parallel workshop sessions**

#### **a) IANA function**

Panel:

- Chris Marsden, Sussex University (moderator)
- Jean Jacques Sahel, ICANN
- Alex Blowers, Nominet
- Dominique Lazanski, GSMA

Jean Jacques began the workshop proper by setting the discussion in context. He notes that on 14<sup>th</sup> March the US Government announced its intention to transition its stewardship of the IANA function by the end of its current contract with ICANN (September 2015). He continues to outline how a transition might occur, highlighting the imminent creation of a 27 person multi-stakeholder ‘coordination working group’, tasked with creating a blueprint for the new model of stewardship, and a second ‘accountability working group’, intended to evaluate if ICANN would remain fit for purpose.

Chris Marsden, referencing Milton Mueller, then offered four ideas as a basis for starting discussion: (a) that ICANN and IANA are not inextricably linked (b) the role and influence of GAC (and its supposed veto) in the coordinating committee (c) the power of the ICANN board in the transition process (d) the French communiqué after ICANN 50 suggesting that ‘ICANN is no longer that appropriate forum to discuss Internet governance’. A summary of the main responses around these points are recorded below:

It was frequently suggested that more practical debates, such as how to maintain the technical and operational management of the root, not be lost to more intriguing discussions. There was general agreement that a Treaty based solution or other forms of international law would not be an appropriate model for transition, not least because the US government would reject anything intergovernmental or multilateral.

There were mixed opinions about the absoluteness of the September 2015 deadline – there was concern expressed about the enormous scope of the challenge, but also the potential influence of the US Presidential election and electioneering on the outcome if the deadline was not met. It was clarified that it is not IANA being transitioned, but the NTIAs stewardship role.



There was universal agreement that maintaining ICANNs and IANAs public interest objectives (similar to the NTIAs commitment to security, stability, resilience and openness) was important, both during the transition but also ensuring those objectives endure beyond the transition and into the new model. However, there was also a general consensus that people must discriminate between ICANN and IANA, and particular care needed to be taken to not misallocate problems associated with ICANN as problems also associated with IANA. IANA was reviewed very positively from a technical perspective.

Further comments from the floor:

- It was suggested that the rejection of multilateral agreements, because the topic becomes mired with problems of politics, is misleading – power and interests are embedded in ICANN, in the working groups etc.
- An individual called for the GAC model to be reconsidered, although further discussion led to this being widened to reconsidering all channels for multi-stakeholder input on the grounds that this would improve the quality and diversity of the environment.

The workshop ended with generic conclusions about continuing discussion and increasing participation.

## **b) Governance of cybersecurity**

Panel:

- Dr Louise Bennett, BCS, The Chartered Institute for IT (moderator)
- Christian de Larrinaga, Internet Society UK England
- Professor Ian Brown, Oxford Internet Institute
- Andy Smith, BCS, The Chartered Institute for IT

Louise introduced the session by stating how vital security is for internet commerce, and praised the UK for taking a leading role – for example by acting as a consensus building agent to remove sites related to child exploitation (IWF). She challenged those present to consider how cybersecurity can evolve, putting aside the Snowden revelations by quoting the US ITIFs estimate that the level of mistrust as a result of US intelligence activities will cost US businesses \$22-35bn over three years. Instead, she suggested the discussion should be taken forward by focusing on improved international cooperation to make progress on, for example, suppressing illegal content, enhancing the ability to enforce legislation and pursue criminals or increasing knowledge about cybersecurity.

Ian then followed by discussing the International Covenant on Civil and Political Rights, suggesting that it demonstrates broad international agreement by directly addressing issues of the state protecting citizens from terrorism and serious or organised crime. He continued to suggest that this legal framework initiates safeguards that prevent arbitrary decisions or excessive discretion by the state, and that the equivalent UN business advice should be taken up under the corporate social responsibility framework by business, particularly those operating in potentially less regulated environments abroad. Ian then responded to a question about the inefficiency of the MLAT procedure, trying to remain positive by positive by highlighting the Obama administration's desire to increase funding to respond to US requests; in response to a second question he cautioned people



about comparing the role of MLAT with the sometimes difficult expectations placed upon global intermediaries in aiding law enforcement.

Christian then spoke about security practices and problems. Amongst other things he spoke about the necessity to reconsider the security of cloud servers (clarifying that the \$22-35bn was just the loss to the cloud computing industry), about the importance of metadata – especially building metadata privacy into protocols – and the need for a societal as well as a technical response. On this last point, he suggested the debate be widened from a privacy-security binary to perhaps less-often considered questions like the ability of the market to self-regulate or the necessity and type of government action.

Andy, hopefully playing devil’s advocate, offered a rather grave warning that the privacy-security debate was leaning much too far towards privacy. He controversially suggested that wanting anonymity online could only be intended for bad things, and strongly defended the intelligence services with a warning that the post-Snowden backlash is making it harder to protect individuals.

Further comments, in a more interactive style, included the ideas that:

- Snowden has helped the average internet user understand the importance of protecting their data and that simple, preferably free methods of achieving this are important.
- GHCQ might be more transparent than corporations (such as Google) in taking and using personal data – but how could you know at all?
- Perhaps the discussion would be helped by having examples of ‘good’ surveillance.
- Anonymity can be both good and bad.

### **c) IPV6**

Panel:

- Dr Olivier Crépin-Leblond, Internet Society UK England
- Alain Fiocco, CISCO
- Tim Chown, University of Southampton
- Adrian Kennard, Andrews & Arnold Ltd (AAISP)

Tim opened the session outlining a project that students from the University of Southampton have been working on with ISOC England, measuring IPV6 deployment: <http://www.ipv6matrix.org/>. The project looks at IPV6 enabled website, DNS servers and mail exchanges. He showed some stats about IPV6 usage 3.5-4% of traffic to Google is via IPV6. Data from the project is open and can be exported.

A demonstration of the site was given with some headline stats from the UK over time. Tim welcomed everyone to use the site and send feedback.

Alain explained that it was hard for Cisco to define the business case for IPV6 as it was hard to understand how much was deployed and what the demand for it was. They started a project to measure global IPV6 usage, looking at readiness of transit systems, availability of content and user statistics. IPV6 enabled sites are ranked in terms of their number of users/ impact.

Some anomalies in some countries such as in Greece where Cloudflare have enabled IPV6 for all their users. For ISPs if they enable IPV6 for their users then there is quite a lot of content out



there. Also tracking users and by the end of the year it is expected to have 8% of global users on IPV6. Most of the big employers of IPV6 are in the US and Europe rather than in Asia.

The technology is difficult to justify as a business case. Cisco came up with two statements:

“If we don’t overcome the challenges of IPV4, we will slow down the growth of the Internet and lose momentum as an industry. IPV6 is important to all of us, to everyone around the world. It is crucial to our ability to tie together everyone and every device. “

The Cisco commitment is:

“At Cisco we are committed architecturally to IPv6 across the board: All of our devices, all of our applications and all of our services.”

The result of this was a high-impact project that implemented IPV6 into a number of products and software. The engineering process had to be changed to mandate the integration of V6.

Adrian – Supplied of IPV6 to their customers for 12 years. Many of the issues they experienced over this time are no longer an issue. The first was the lack of content 12 years ago but now there is a lot of content including Facebook and Google which is what the vast majority of domestic customers will want to access.

Connecting to content was an issue but now an increasing number of Transit providers offer IPV6 connections over the past few years. They had to ensure that all their network was compatible. Generally these are agnostic and did not cause a problem. A bug in the system was an issue but were able to update their routers to work round it.

Router at the end of the line was the biggest challenge. Initially these were very expensive. Needed to be able to source cheap consumer routers that supported IPV6 that they could give away with their broadband packages. Certainly most of the technical challenges have been overcome now. Feels there is no reason why an ISP shouldn’t implement. Cost of change is the only barrier that remains.

Lessons learned in other countries. In Belgium ISPs, police, regulator and dept Justice signed an MoU which fixed the number of ports per users and simplified crime investigations. The side effect of this was that it put an end date to CGN which has led to all ISP’s in Belgium enabling IPV6 and approx 20% of uptake. The right business incentive is needed.

UKIPV6 Council (<http://www.ipv6.org.uk/>) has been established to try and encourage uptake and also to try and replicate what has been successful in other countries.

Impact of IoT on IPV6 takeup. Depends on definition on IoT but smart meters for example are only operating on IPV6 as they cannot determine which stack to use.

The panel concluded that we should be optimistic about IPV6 as growth is increasing, albeit slowly. Stressed importance of IPV6 and that it is the future. There is a cost for IPV6 transition but don’t underestimate the increasing cost of staying with IPV4.

#### **14.15 Network filtering plenary**

Panel:



- Simon Milner, Facebook (moderator)
- David Miles, Family Online Safety Institute (FOSI)
- David Austin, The British Board of Film Classification
- Jim Killock, Open Rights Group

Simon introduces the panellists and set the session in context. He explained that this session follows on from the February UK-IGF where the ISP's updated us on what they were currently doing to help safety measures.

David Austin explained that the BBFC is the regulator of film and video in the UK. In cinema and DVD their work is governed by statute but they also have developed a suite of voluntary self-regulatory services for companies who are active online which includes a system of trusted ratings and content advice. They are working with the major mobile network operators on a voluntary self regulated best practise for content served over their network. Standards of age rating which are set through public research and surveys. These are transparent standards of age rating which are set through public research and surveys and are published on their website. They have also worked with filtering companies to match their standards to those the BBFC have developed. Some tailoring was necessary – such as slap stick violence. They also operate an appeals process in cases of over blocking. Now the system has been established, the mobile operators are able to deal with the clear cut cases of appeal. Appeals received so far have included abortions sites - both pro and anti, racism, sex chat lines, strippers, assisted dying, sex education, body piercing and rape. So far the system has been in operation for 9 months and seems to be working well. Volume of complaints have been approx 20 over the 9 months and the majority of reports are dealt with the mobile operators. It is a binary system – the restrictions are either over 18 or not. This does not mean that all permitted content is child safe. Working with ORG they do now publish the results of each appeals case on a quarterly basis.

#### **15.45 Wrap-up**

Q&A session,

- Kate Russell, Freelance journalist and BBC Click
- Eleanor Bradley, Nominet

Kate opened the session and praised the level of participation and engagement from a wide range of stakeholders. New ground has been covered in the old conversations as well as new topics such as IANA.

Eleanor outlined her main messages. The opening session highlighted that post Snowden and netmundial, the IG debate is now centre stage in the political global scene. She recognised the demand for outcomes but asked how we keep the open nature of the discussions as well as creating something tangible? Moving forward we need to work on joining the dots between the global discussion and the regional and national.

We also need to improve and increase youth participation. This needs to be wider than just tokenism.

Other countries have specific multi-stakeholder mechanisms such as CGI brazil that meet regularly and work on issue specific topics. The UK-IGF works in isolation perhaps a more systematic approach is needed?



The fact that the netmundial outputs were endorsed was a positive outcome. The message of impetus for change came out strongly from that meeting.

Cyber security conversations are evolving and are now considering the broader implications. We need legislation that change as quickly as the criminals are able to. There was a strong feeling in the room that education is key, rather than legislation. This was illustrated with a streetlight analogy. We need to work on lighting dark areas of the internet.

Discussions on IPV6 have moved on from problems of implementation to those of opportunity. We now need tools for measuring adoption and take--up to visualise the scale of the issue.

Netfiltering is currently a contentious topic. We have to talk about the issues in order to move forward from this.