EuroDIG

European Dialogue on Internet Governance

Madrid

29-30 April 2010

Organised by

IGF SPAIN
FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA

DiPLO
www.diplomacy.edu

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

EBU·UER

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Kommunikation BAKOM
Office fédéral de la communication OFCOM
Ufficio federale delle comunicazioni UFCOM
Uffizi federal da communicaziun UFCOM

MEDIENSTADT LEIPZIG e.V.

Institutional partners

plan avanza2

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

¡MADRID!
fundación madrid tecnología

Hosted and supported by

Telefónica

European Dialogue on Internet Governance
EuroDIG 2010

Messages from Madrid

Madrid, 29-30 April 2010

Telefónica, Distrito C, Madrid

EuroDIG

EuroDIG secretariat
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

Printed at the Council of Europe

Information on EuroDIG

The Pan-European dialogue on Internet governance (EuroDIG), the European Internet Governance Forum, is an open platform for informal and inclusive discussion and exchange on public policy issues related to Internet Governance (IG) between stakeholders from all over Europe. It was created in 2008 by a number of key stakeholders representing various European stakeholder groups working in the field of IG.

EuroDIG is a network which is open to all European stakeholders that are interested in contributing to an open and interactive discussion on IG issues. The stakeholders participating in the EuroDIG programme network comprise a considerable number of representatives from civil society, the business sector, the technical and academic communities as well as European governments, institutions and organisations including the EU-presidency, the European Commission, the European Parliament, the Council of Europe and the European Broadcasting Union.[1]

The purpose of EuroDIG is twofold: first, to help European stakeholders to exchange their views and best practices on issues to be discussed at meetings of the Internet Governance Forum (IGF), including the identification of common ground shared by all European stakeholders and highlighting the diversity of experience of the different European stakeholders; second, to raise awareness in Europe and among European stakeholders about the relevance and value of multi-stakeholder dialogue.

The third edition of EuroDIG was held on 29-30 April 2010 at the headquarters of Telefónica, in Madrid. It was organised by the Spanish IGF, the Council of Europe and the Swiss Federal Office of Communication (OFCOM) together with a number of other stakeholders, with the support of Telefónica and Fundación Telefónica, the Ministry of Industry, Tourism and Commerce of Spain (through red.es) and the City of Madrid, coinciding with the Spanish Presidency of the European Union.

Following an opening session on the public and economic value of the Internet in Europe and a dialogue between representatives of 10 national IGF platforms, there were seven thematic workshops and five plenary sessions organised by open groups of interested European stakeholders. More information on these events and their organisers can be found on the EuroDIG website at: http://www.eurodig.org/.

EuroDIG 2010 was attended by around 290 participants from stakeholder groups and regions across Europe. There were approximately 220 remotely connected participants many of whom used EuroDIG remote hubs in 10 cities across Europe: Baku (Azerbaijan), Yerevan (Armenia), Sarajevo (Bosnia), Toulouse and Strasbourg (France), Tbilisi (Georgia), Chisinau (Moldova), Bucharest (Romania), Belgrade (Serbia) and Kiev (Ukraine). Remote participation was provided using a combination of live video-streaming, real-time captioning and tweets, social network and wiki reports. The remote hubs were meetings of local people who interacted with the Madrid meeting by sending comments and questions in real time. For every EuroDIG session, there was a remote participation moderator connecting hubs with the Madrid meeting.

The organisation of these remote hubs was an integral part of an Internet Governance Capacity Building Programme targeting stakeholders from Central and Southern European countries. This programme includes six months of teaching and research activities and the participation of the best students at EuroDIG.

1. For more information see: http://www.eurodig.org: programme network.

About the Messages from Madrid: This document contains a number of messages flowing from EuroDIG workshop and plenary events. The Messages are not a negotiated text. They have been put together by the rapporteurs in consultation with the organising teams of each plenary and workshop session and serve as key messages from Europe into the global debate.

Executive summary

What is the public and economic value of the Internet for Europe?

The Internet is a public value space bringing more than just economic wealth to users. Digital education is a precondition for employment and for generally empowering citizens. Avoiding over-regulation of the Internet is important.

National debates on Internet governance

National Internet governance platforms are important for sharing information and experiences, and offers spaces for interaction with policy makers. EuroDIG provides a common European focal point, in particular for their coordination and promotion.

Workshops

Cross-border cybercrime jurisdiction under cloud computing

The Budapest Convention and Convention 108 are the starting points in addressing cybercrime and data protection. The way forward should include reference to: development of policies and guidance for LEAs to carry out trans-border criminal investigations, multi-stakeholder cooperation and awareness raising efforts, and the setting up of a multi-stakeholder working group led by the Council of Europe in cooperation with the European Union.

Geographical and other names of public interest as new TLDs

The Domain Name Space is a global common resource, in which new gTLDs present various opportunities that must be developed in the global public interest perspective.

The "one size fits all" approach is one major reason for the delays in the new gTLD program because no single regime can be expected to reasonably cover TLDs as diverse as geographic TLDs, brand TLDs, linguistic community TLDs and keyword TLDs.

Short meaningful keyword TLDs also raise public interest issues. Different types of legal contracts are therefore necessary. It is preferable to respect local laws (rather than Californian law only) that TLDs purport to serve. Specific application procedures for terms of public interest as TLDs should be explored. To this end, ICANN should explore creating a public interest team of qualified experts.

Internet as a platform for innovation and development of new business models

The sharing of (cultural) content and its digitalization is important. Enabling access to digital content on the Internet from any and all countries/territories, 'mash-up', digital derivative works, and agreements between content creators, telco operators and content aggregators (in order to share revenue), were highlighted as different ways forward.

IPv6 transition – business impact and governance issues

There is an increasing IPv4 space exhaustion. Entering potential new markets dealing with IPv4 addresses is not recommended. EU member states are encouraged to move ahead to foster deployment by their communities. The industry sees no need to change model (RIR allocation, policies, etc.). Regulators must themselves learn about IPv6 so that they can then regulate as necessary from a position of knowledge.

Children and social media – opportunities and risks, rules and responsibilities

ICTs provide children with an unprecedented possibility of having their voice heard and in participating in the public discourse of society. Protectionist educational approaches to the use of Internet often produce negative results and do not allow young people to apply the principles of autonomy and critical reflection to negative messages nor do they let them develop self-defence communication against politically incorrect messages. Media literacy should be considered as one of the priority issues of Internet governance. New pedagogies of communication, minimum competencies in order to be Internet literate, and the implementation of media literacy programmes are important ways to move forward.

Sovereignty of states and the role and obligations of governments in the global multi-stakeholder Internet environment

International law provides a wealth of legal concepts which can be instructive for purposes of developing principles of international cooperation on cross-border Internet, such as the principle of equitable and reasonable access to critical resources, state responsibility for actions taking place within its jurisdiction which have negative impact in another as well as state responsibility for action taken by private actors, under a standard of due diligence.

Open hour on cloud computing: from fog to secure cloud – a regulatory perspective

The governance of cloud computing necessitates: clarifying the roles and responsibilities of actors; improving and facilitating international data transfers and improving certainty as to applicable law and jurisdiction; increasing transparency regarding privacy and security for customers of cloud computing services; improving consumers control over their privacy and the processing of their data (including deletion) and improved enforceability of consumers' data protection; increasing awareness of cloud services, privacy and contractual policies; increasing legal certainty through the adoption of global privacy standards.

Plenary sessions

Online content policies in Europe – where are we going: There is no clear common and holistic strategy regarding the issues of liability for and blocking of Internet content.

It is increasingly unclear what "actual knowledge of illegal activity or information" is with regard to the liability of service providers. The overly-cautious behaviour of these providers can be in conflict with user's freedom of expression. Users themselves are also increasingly being held liable for their online activities, particularly because of the criminalizing of copyright infringements. Concern was raised regarding the proportionality of the (legal) measures being introduced to deal with Internet content. The proportionality of any blocking measure *vis-à-vis* human rights was highlighted with reference to the need for a specific (legal) basis that makes it foreseeable (rule of law) while, on the other hand, procedural safeguards should be in place that allow users to question and challenge blocking measures.

Global privacy standards for the internet and working world

Important risks include data retention and how this may threaten freedom of association to form and join a trade union, the risks of centralising data held by governments and companies, the lack of legal certainty when defining jurisdictions in a global world, and the effect of the Internet on the so called "right to oblivion". Global privacy standards, privacy by design and by default for future technologies and applications, data protection education to be included in our education systems, and privacy enhancing infrastructure at work, were all highlighted as ways to move forward.

Principles of "network neutrality" and policies for an open Internet

The key principles underlying the "open Internet" or "network neutrality" evolve around: (i) no discrimination of traffic based on sender or receiver; (ii) unrestricted user choice and access and use of content, applications and services by consumers – businesses – citizens; (iii) appropriate, reasonable and non-discriminatory traffic management. More certainty is needed on rights and obligations, such as what discrimination entails (it should not be just about anti-competitive actions under strict competition criteria) and how to define 'reasonable' traffic management and prioritisation. User-centricity and real user choice and the transparency of business offers were also underlined. Key considerations for the European Commission to consider include: freedom of expression, i.e. no censorship; transparency; investments in open networks and infrastructure competition; fair competition across the value chain; preserving innovation and investment in both networks and services.

Policy and decision-making and multi-stakeholderism – international, national and regional experiences. Is there a European vision?

Multi-stakeholderism is a confrontation between different models of democracy: the representative democratic model versus the participatory democracy model which has developed as a way to counter the crisis of representative democracy. Multi-stakeholderism addresses the disconnection between the governors and the governed albeit noting that there are limitations as to what multi-stakeholderism can do: it cannot assure by itself legitimacy and representativeness. It cannot assure universality in points of view. It cannot be considered immune to being captured by special interests and manipulative practices. National IG debates support the idea of multi-stakeholderism on a global level. Where there is no tradition of consultation outside the spheres of government, countries have started adopting the multi-stakeholder approach for issues related to Internet governance.

The Internet in 2020

There is a need make sure that we keep the Internet user-centric, supporting the end-to-end principle so as for it to constitute no barriers to innovation. Europe's "systemic barrier" to the Internet's growth is baggage which has to be abandoned in favour of change. The protection of critical infrastructure and the issue of data distribution and their transfer are key issues that need to be addressed.

Contents

Opening sessions

The two leading lines of the session concerned the Internet as a market place which is driving development and the Internet as a public value space bringing more than just economic wealth to users. There were no doubts that the Internet is a platform for human development and that investments in it are adding significant financial value. Finding the right balance between the public interest and paying producers to produce even more (i.e. finding the balance between the social and economic value of the Internet) was highlighted.

Opening sessions

Messages prepared by Vladimir Radunovic, DiploFoundation Coordinator, Internet Governance Programme

Opening session panellists: Prof. José Mariano Gago, Minister of Science, Technology and Higher Education of Portugal; Elfa Ýr Gylfadottir, Ministry of Education, Science and Culture in Iceland; Visho Ajazi Lika, Deputy Minister for Innovation and the Technology of Information and Communication of Albania; Sebastian Muriel, General Director of Red.es (Chairman); Michael Niebel, European Commission; Frédéric Riehl, Vice-Director, OFCOM Switzerland; Jeroen Schokkenbroek, Head of Department on Human Rights Development, Council of Europe; Lieven Vermaele, Technical director of EBU

Digital education was considered to be a precondition for employment and for generally empowering citizens.

The attractiveness of the Internet as a market place was considered to be subject to several conditions:

- unlimited user access to content and services, including access to infrastructure and broadband. From the perspective of broadcasters, it was stated that wireless and optics-based broadband cannot be measured equally, and that the idea of giving out spectrum for broadband was considered to be not be a good option;
- uninterrupted access to the network by content and service providers with reference made to principles of 'network neutrality';
- open standards allowing competition on an equal footing;
- protection and respect for privacy and freedom of expression.

Balanced copyright protection was underlined with reference to the rights of authors while, at the same time, promoting the sharing of knowledge. Measures or sanctions in this respect should be proportionate and should not violate other rights and principles.

The Internet was clearly identified as a space of high public value with examples given of the power of the Internet to improve crisis management and to promote democratic processes. Protection of and respect for human rights on the Internet was also emphasised as a key factor.

Avoiding over-regulation of the Internet was emphasised, in particular with reference to the proportionality of (national) legal responses. Listening to the concerns and positions of stakeholders by way of an open dialogue was considered a better way forward to help build mutual trust. In this connection, policies and/or legislation should be technology neutral so that they can remain relevant as the Internet evolves.

Examples were provided of how states deal with key Internet governance issues. The Icelandic Modern Media Initiative was presented as an example to create a legal environment for new media that protects their freedom of expression and information (i.e. protection of whistle-blowers and sources of information). Albanian experiences were shared, in particular in linking schools and creating public access points, as well as enabling e-commerce and e-government services.

It was argued that there is not enough being done to digitally preserve, disseminate and promote pan-European values on the Internet, in particular with regard to cultural and language diversity.

National debates on Internet governance

National IGFs are multiplying in Europe with various operational models and origins (civil society, institutions, business sector etc) all of which are based on a multi-stakeholder approach to dialogue (i.e. not top-down approach) including strong interaction with policy makers (i.e. via a bottom-up approach and the involvement of parliamentarians in certain countries).

National debates on Internet governance

Messages prepared by Giacomo Mazzone, EBU

Panellists: Laurent Baup, Forum Internet, IGF France; Martin Boyle , NOMINET/IGF UK; Anders Johanson, Swedish Regulator PTS; Prof Luis Magalhães, Ministry of Science, Technology and Higher Education, Portugal; Siv Mørch Jacobsen, IGF Denmark; Wolfgang Kleinwächter, University of Aarhus, IGF D; Jorge Perez, IGF Spain; Vladimir Radunovic, DiploFoundation, Serbia; Leonid Todorov, CCTLD.RU; Stefano Trumpy, IGF Italy

In Western Europe, dialogue regarding the Internet is focused on the regulation of markets. In Eastern Europe, there is more attention to telecommunications, in particular market de-monopolisation and telecom market liberalisation (re: incumbent telecoms versus dominant providers) and to problems regarding rights and freedoms (e.g. privacy, freedom of expression, child protection etc).

There was discussion on the perception of Internet governance: what the IGF is and what it could be in countries. The need to convince citizens that this dialogue concerns them more that this is relevant and important for them was highlighted.

Sharing experiences and information between national Internet governance platforms was considered important. The transmission of national messages to a common European focal point and better coordination of these platforms via EuroDIG was considered to be a next step in promoting national dialogue, especially in more fragile countries.

It was suggested that the capacity of the Internet to self-regulate could be coming to an end which, if so, would require a EuroDIG network of national Internet governance platforms to unite.

Workshops

Workshop one: Cross-border cybercrime jurisdiction under cloud computing

Transnational investigations

Law enforcement authorities (LEA) act within national borders, while cybercrime is international and while data stored in the clouds are often difficult to localise. This situation generates several concerns: How to define when an investigation crosses a national border? In which cases can an investigator access data stored abroad without referring to the local LEA? How to go beyond the obstacles that could disrupt legitimate investigations, such as when there are no legal frameworks to enable data to be requested from another country?

Traditional legal mechanisms often prove unsuited to the online environment. Mechanisms such as mutual legal assistance treaties (MLATs) and letters rogatory, which often have their origins in the nineteenth century, are too slow and cumbersome for collecting evidence in the digital age.

The Budapest Convention on Cybercrime provides for the possibility of efficient international cooperation, including expedited preservation of data and mutual legal assistance on an expedited basis. Many countries have yet to ratify this Convention or are not fully exploiting its opportunities.

While the 24/7 contact points can be helpful, they must be better resourced in order to operate effectively. Nearly four dozen countries have ratified and/

Workshop one: Cross-border cybercrime jurisdiction under cloud computing

Messages prepared by Estelle de Marco, Inthemis – CRESIC (Centre de recherche et d'études sur la sécurité de l'information et la cybercriminalité)

Workshop panellists/key participants: Ioana Bogdana Albani, Chief Prosecutor, Terrorism and Organized Crime Directorate at the Prosecutor's General Office of Romania; Prof. Henrik Kaspersen, Law Professor, Vrije Universiteit Amsterdam; Cornelia Kutterer, Senior Policy Manager, Microsoft; Francisco Monserrat, Representative of RED IRIS-CERT, Spain; Michael Rotert, EuroISPA, European ISP Association (eco); Alexander Seger, Council of Europe, Head of Economic Crime Division; Cristos Velasco, Director General, Ciberdelincuencia.Org and Member of the IGF Spain Advisory Group

or signed the Council of Europe's Budapest Convention on Cybercrime, which requires signatories to establish points of contact who are available 24/7 in order to process requests from law enforcement authorities. There is a fairly widespread sense, however, that the system should be improved further and many stakeholders expressed concerns regarding the resourcing and reliability of the current system.

In its recently adopted Stockholm programme (December 2009), the European Union proposes to establish a comprehensive system for obtaining evidence in cross-borders cases, including a real Euro-

pean evidence warrant. It will be important to ensure that any new EU instruments remain connected to existing international legal instruments and provide real added value for practitioners.

Law enforcement efforts dealing with cyber-security need to be better funded, staffed and trained. The private sector has a role to play here, including through public-private partnerships to support enhanced training for police and to undertake expert forensic analysis.

- There is a need for international guidelines for LEAs to access cross-border data, ensuring respect for mutual assistance procedures, and in reducing the time needed to carry out cybercrime investigations;
- There is a need for further discussion about the criteria used to determine the laws applicable to information hosted in the clouds;
- There is a need to improve the global harmonization of national laws in line with the Budapest Convention in order to more effectively tackle cybercrime, as well as to secure financial resources to assist countries in the implementation of domestic measures against cybercrime;
- There is still a problem of harmonization of cybercrime legislation, in particular with regard to investigations and access to personal data. It was suggested that there should be specific rules to access data across national borders perhaps in the form of an additional protocol to the Budapest Convention;
- There is the urgent need to provide training and build the capacity of LEAs, for example under the auspices of existing training initiatives;
- There is the need for a multi-stakeholder approach to promote understanding and awareness of cybercrime jurisdiction and cloud computing and the establishment of clear obligations and responsibilities for each of stakeholder;
- There is a need to explore the possibility of creating platforms to improve regional and international cooperation among judicial networks and the industry;
- The creation of future European policies and initiatives in the field of cloud computing and cybercrime should also be well coordinated.

Due process and the protection of human rights in law enforcement

The movement of data across borders is a common feature of cloud computing services. Individuals and business customers of cloud computing services may not be clear about who may have access to their information for the purposes of law enforcement.

In this context, the question arises as to who retains data, for how long, and who has jurisdiction over it. Although the Data Retention Directive applies only to electronic communications services, there is disagreement across and even within Member States as to which services constitute ECSs. These issues are made more complex because there is no harmonised period for the retention of data nor clear rules governing access to or jurisdiction data in Europe. There is a similar lack of clarity regarding jurisdiction and rules on retention and access at the international level.

The questions concerning the constitutionality of European data retention laws emphasises the difficult relationship between data retention and data protection regimes. The Internet services industry has evoked for several years that data retained for their own needs, such as for commercial purposes , is generally sufficient to respond to the requests of LEAs.

The *Bundesverfassungsgericht* decision highlights the often challenging regulatory environment. Over and above the fundamental questions about the constitutionality of data retention laws, the baseline requirements set out in the Data Retention Directive for electronic communication services providers to retain certain data have been interpreted and applied differently across Member States, leading to significant confusion and difficulties.

Already in October 2009, the Romanian Constitutional Court ruled that the Romanian data retention law is incompatible with the Romanian constitution and in breach of the European Convention on Human Rights. Similar constitutional challenges have been made or suggested in other Member States.

- There is a need for international guidelines for LEAs to access cross-border data, ensuring respect for mutual assistance procedures, and in reducing the time needed to carry out cybercrime investigations;
- There is a need for further discussion about the criteria used to determine the laws applicable to information hosted in the clouds;
- There is a need to strengthen legal certainty on the application of data protection and international best practice for Internet service providers within the framework of cybercrime investigations;
- There was general consensus on the need to establish fair data retention policies that strike balance between investigation needs and the implementation of adequate safeguards in the field of privacy and data protection;
- There is the need for a multi-stakeholder approach to promote understanding and awareness of cybercrime jurisdiction and cloud computing and the establishment of clear obligations and responsibilities for each of stakeholder;
- There is a need for full implementation of the Budapest Convention, including the procedural safeguards and conditions pursuant to Article 15 thereof;
- There is a need to update the rules of judicial competence and jurisdiction in the field of data protection with regard to cloud-computing,

ensuring a better efficiency and transparency of criminal investigations while respecting the existing international standards on privacy and data protection. These concerns should be considered in the recently launched process to revise Convention 108;
- The creation of future European policies and initiatives in the field of cloud computing and cybercrime should also be well coordinated.

Legal quagmire for cloud service providers and ISPs

There is a lack of consistency and harmonization of data access, retention, and privacy regulatory frameworks, in particular as to applicable law and jurisdiction, which creates legal uncertainty. Cloud users and providers find it increasingly difficult to determine which jurisdiction rules to apply, and how, even within the EU. Lawful demands for user data in one Member State to which an ISP or cloud provider may need to respond may place a provider at risk of violating data protection rules in another.

- There is a need for international guidelines for LEAs to access cross-border data, ensuring respect for mutual assistance procedures, and in reducing the time needed to carry out cybercrime investigations;
- There is a need for further discussions about the criteria used to determine the laws applicable to information hosted in the clouds;
- There is the need for a multi-stakeholder approach to promote understanding and awareness of cybercrime jurisdiction and cloud computing and the establishment of clear obligations and responsibilities for each of stakeholder;
- There is a need to strengthen legal certainty on the application of data protection and international best practice for Internet service providers within the framework of cybercrime investigations;
- There was general consensus on the need to establish fair data retention policies that strike balance between investigation needs and the implementation of adequate safeguards in the field of privacy and data protection;
- There is a need to explore the possibility of creating platforms to improve regional and international cooperation among judicial networks and the industry;
- The creation of future European policies and initiatives in the field of cloud computing and cybercrime should also be well coordinated.

Ensuring confidence and transparency in cloud computing services

The issue of transnational investigations becomes further complicated as the movement of data across borders develops as a common feature of cloud computing services. While increased due process notably implies efforts from the industry towards more transparency regarding the place where data are stored, it also reinforces the need for global standards in the regulatory frameworks around data retention, access and privacy in law enforcement.

- There is the need for a multi stakeholder approach to provide a better understanding and awareness for cybercrime jurisdiction and cloud computing and establishment of clear obligations and responsibilities for each of the stakeholders;
- There is a need to update the rules of judicial competence and jurisdiction in the field of data protection in the cloud environment, ensuring a better efficiency and transparency of criminal investigations, while respecting the existing international standards on privacy and data protection; these concerns should be considered in the recently launched process to revise Convention 108;
- The creation of future European policies and initiatives in the field of cloud computing should be well coordinated.

Conclusions

The needs highlighted above can be summarized by way of the following;

Conclusions:

- Full implementation of existing tools and instruments addressing cybercrime and data protection, notably the Budapest Convention and the Convention 108 respectively, are the starting point that will help address a number of the challenges related to cloud computing;
- Cooperation should be improved among industry, government, law enforcement authorities, academia and civil society, in order to promote understanding and raise awareness of cybercrime jurisdiction and cloud computing;

Recommendations:

- For the Council of Europe – in cooperation with the European Union and other international organizations – to establish a multi-stakeholder working group (composed of experts from the private sector, civil society, academics and government representatives) to provide guidance on issues raised by cloud-computing, covering cybercrime aspects as well as data protection, jurisdiction and conflict of law aspects;
- For the Council of Europe to draft specific policies and guidance for LEAs to carry out trans-border criminal investigations;
- For the fifth edition of the Internet Governance Forum (Vilnius, 14-17 September 2010) to consider the issue of cybercrime jurisdiction.

Workshop two: Geographical and other names of public interest as new TLDs?

Workshop two: Geographical and other names of public interest as new TLDs?

Messages prepared by Wolfgang Kleinwächter, University of Aarhus, Chair of the Council of Europe Internet Expert Group

Workshop panellists/key participants: Amadeu Abri i Abril, CORE Internet Council of Registrars; Iratxe Esnaola Arribillaga, dotEUS Association; Jordi Iparraguirre, Director /CEO at Fundació puntCAT; Dirk Krischenowski, dotBerlin, Germany; Susan Reynolds, Asociación Punto-Gal; Hubert Schöttner, Federal Ministry of Economics and Technology, Germany; Thomas Schneider, Swiss Federal Office of Communication (OFCOM) International Information Society; Nick Wood, Com Laude

There was general agreement on the following:

- New TLDs present various opportunities and should be introduced as soon as possible once a viable process has been developed.
- The Domain Name Space is a global common resource: the final regime(s) for new gTLDs must therefore be developed in a Global Public Interest perspective in accordance with ICANN's Articles of Incorporation and the Affirmation of Commitment (AoC).
- Serving the Public Interest does not mean that TLDs have to be run as non-profit. Commercially run TLDs can also contribute to the public interest.
- The "one size fits all" approach is one of the major reasons for the delay regarding the new gTLD program. This is because no single regime can be expected to reasonably cover TLDs as diverse as geographic TLDs, grand TLDs, linguistic community TLDs and keyword TLDs.
- Different types of legal contracts are therefore necessary, but these potential regimes need to be kept simple and of a limited number to reduce incentives for gaming.
- Possible elements of regime differentiation could be, inter alia, the special conditions under which registries could use non ICANN-accredited registrars, especially local ones, and be bound by contracts under the local law related to the community they purport to serve rather than by California law only.
- There is not only a public interest dimension to Geo-, City- and cultural-linguistic TLDs. Short meaningful keyword TLDs also raise public interest issues , in particular as regards sectors where there is potential consumer harm or fraud such as TLDs linked to health, food, banking, financial aid/NGOs, etc.

There were several proposals made:

- Regimes for new TLDs should build on the experience with already existing TLDs that could serve as a model for similar TLDs (e.g. .Cat could serve as a model for further cultural-linguistic TLDs).
- Specific application procedures for terms of public interest should be explored.
- ICANN should explore creating a Public Interest Team of qualified experts from all over the world that would assist ICANN in taking into account the global public interest.
- ICANN could explore establishing a supporting organisation for Public Interest Registries and Registrars.
- Registry-operators contracts should reflect the local laws of the community concerned.
- A EuroDIG working group will be set up to follow-up this workshop in order to prepare input into the ICANN meeting to be held in Brussels in June 2010.

Workshop three: Internet as a platform for innovation and development of new business models

Workshop three: Internet as a platform for innovation and development of new business models

Messages prepared by Lourdes Muñoz Santamaría, Member of the Spanish Parliament from the province of Barcelona, and Alberto Abella

Workshop panellists/key participants: Martin Perez, ASIMELEC; Elfa Ýr Gylfadottir, Ministry of Education, Science and Culture in Iceland; Sergio Mejías Sánchez, Bubok S.L.; Miguel Perez Subias, Internet Users Association; Rafael Sánchez, EGEDA; Oleguer Sarsanedas,TV3 Catalunya; Juan Zafra, ASIMELEC, Digital Content Commission

Internet has brought social and economic change which also affects the digital content sector. This is a stage of transition. We should support content digitalization and specifically cultural content and cultural heritage. The challenge ahead is how to provide for an environment that allows the development of a sustainable model which allows and facilitates business models for digital content to flourish and make a return on investment. A new business model must enable creators to be remunerated.

Different options and views that came up during the debate:

- Users/civil society support sharing. It is necessary to tackle a restructuring of the digital content industry.
- The need for harmonized European legislation, suppressing territorial boundaries/obstacles. An example of these obstacles is the licensed rights depending on the territory which thereby obstruct the development of the sector due to the elevated costs (in terms of time, money and uncertainty) of making content available on the Internet.

- Allow for negotiation. Stop the "old" Europe from being "old" – if we want to create opportunities for European companies it must be possible to promote projects that are worldwide.
- There is a demand to enable access to digital content on the Internet from any and all countries/territories, thereby suppressing national IP-based access restrictions.

In contrast, there are two different perspectives on digital content, cultural content, and copyright:

- Copyright collecting societies have shown that there is fear (in Spain) to include content on the Internet because they consider there is not enough legal security.
- Different stakeholders demand to include content on the Internet, stating that there is not enough supply (e.g. books in non-majority languages – a few months delay will be too late for such products).

In this connection, there is a demand from all stakeholders (i.e. including users, Internet Services Providers, copyright holders) for efforts to be made by governments, regulators and institutions to increase certainty in this field. Equally, there should be a space/platform created to promote dialogue between these different stakeholders in order to reach some critical agreements.

New promising business models could:

- explore and develop mash-up, digital derivative works (contrary to a direct translation of the off-line contents to the digital world),
- launch agreements between content creators, telco operators and content aggregators in order to share revenue.

As regards 'network neutrality' this is a debate brought out by the exponential increase in digital content available. Operators increase their costs to deploy networks capable to deal with increasing traffic. However, it was suggested that there is a need for a sustainable model which is able to act as an incentive for such deployment by providing a suitable return of investment. Otherwise, services to citizens and society could suffer in quality and availability.

Workshop four: IPv6 transition – business impact and governance issues

The future availability of IPv4 resources and the scenarios that follow the exhaustion of the free resource pool were discussed. An explicit call for planning and action to start immediately was made. It was asked whether this will be a new occasion for the industry to perform a better business cost and opportunity analysis.

Workshop four: IPv6 transition – business impact and governance issues

Messages prepared by Joao Damas, Bondis and Carlos Ralli Ucendo, Universidad Politécnica de Madrid

Workshop panellists/key participants: Jacques Babot, European Commission; Marcelo Bagnulo, IAB member; Fred Harrison, Head of Telefónica Standards; Patrik Fältström, Cisco; Geoff Huston, Asia Pacific Network Information Centre (APNIC); Martin Levy, Hurricane Electric; Roland Perry, RIPE NCC; Pedro Veiga, Foundation for National Scientific Computing

Business impact

The key messages in the business discussion have been:

- The driver today for IPv6 is theIPv4 addressing space exhaustion. Entering potential new markets dealing with IPv4 addresses is not recommended at all.
- The time for IPv6 uptake is "right now", because allocations left will provide less time than what is actually needed to adapt complex infrastructures with back-office applications and coordinate efforts among all involved players.
- IPv6 is considered a strategic cost and therefore not in the revenues increase or costs decrease but as a necessary step in order to continue operations.

The next steps regarding business impact identified during the session were:

- Start planning of your network as soon as possible. Small networks and core infrastructure appear easy to migrate while large access infrastructures may demand further analysis, consideration of various complex scenarios and strategies.
- Opportunities ahead such as M2M ("Internet of the things") need to be early identified and worked out.

Further discussion needed on

how to market IPv6 towards the end-users when most of the routers at home premises are not yet enabled and most probably will require a hardware upgrade.

Governance issues

- National initiatives started by governments involve requirements in public procurement processes as well as ensuring that citizens will continue to be able to reach public services without impediment.
- The RIR system in the face of IPv6 deployment: RIR system has been ready for a long time. Probably one of the most compliant systems involved.
- No need seen in industry for a change in model (RIR allocation, policies, etc).

- Facilitating deployment by making resources available: http://www.ipv6actnow.org/

The role of the European Union

- Today the role of fostering deployment rests with the community. Historically for 15 years, the EU has devoted resources to foster IPv6 evolution. Since 2005 research is considered mostly complete. Since then the EU encourages member states to move ahead.
- The European Commission has invested more than 100 M€ to share the risk with industrial, academia and SMEs partners to drive IPv6 adoption in Europe. Additionally internal infrastructures are being adapted and since last week there's even a WiFi v6-enabled network at one of the EC building.
- The most recent communication included a plan for action. Training is a key issue and so is monitoring work.
- Continued economic growth requires ease of Internet growth.
- The European Commission is concerned with market distortions related to eventual IPV4 secondary markets.
- The Internal move to IPv6. Study at DIGIT going to provision all infrastructure

The role of regulators concerning IPv6

- Inspect whether there is any regulation impeding use of IPv6.
- Depending on each country's structure the approach to regulation, find the way to have public services enabled.
- Regulators must themselves learn about ipv6 so that they can then regulate as necessary from a position of knowledge.
- The alternative scenarios for continued Internet growth, involving complex multi-layer address translation introduces the risk of regression as the new devices will let operators to control which applications manage to work through the network, creating captive markets and monopolies that are later very hard to devolve, as past experience has shown.

Workshop five: Children and social media – opportunities and risks, rules and responsibilities

Opportunities and risks

Opportunities

- ICTs provide children with an unprecedented possibility of having their voice heard and in participating in the public discourse of society.
- Technologically savvy children and young people can use the Internet to advance positive changes in society.

Risks

- Children are not always aware of all the positive opportunities of the Internet or of the threats to their rights and security online.
- Children are excluded from discussions on Internet governance.
- Digital generation gap: parents and teachers are often not fully informed about technological developments in order to teach children about using the Internet.
- Many parents are not always available to teach their children about using the Internet.
- Young people who are most at risk from online harm are those who are most at risk from offline harm.
- Protectionist educational approaches to the use of Internet often produce negative results. They do not allow young people to apply the principles of autonomy and critical reflection to negative messages nor do they let them develop self-defence communication against politically incor-

Workshop five: Children and social media – opportunities and risks, rules and responsibilities

Messages prepared by Franziska Klopfer, Council of Europe

Workshop panellists/key participants: Roberto Aparici, Universidad Nacional de Educación a Distancia, Spain; María José Cantarino, Telefonica, Teachtoday.eu; Jutta Croll, Digital Opportunities Foundation, Managing Director; Javier Garcia, Madrid Office of the Ombudsman for Children; Silva Järvinen, The Finnish Children's Parliament; Anders Johanson, Swedish Regulator PTS; Nadine Karbach, European Youth Forum; Narine Khatchatryan, Media Education Center; Georgios Kipouros, European Youth Forum; Yuliya Morenets, TaC – Together against Cybercrime; Rauna Nerelli, The Finnish Children's Parliament; Sara Reid, The Finnish Children's Parliament; Graham Ritchie, CEOP – Child Exploitation and Online Protection Centre; Ana Luiza Rotta, eNASCO; Yolanda Rueda, Fundación Cibervoluntarios; Matthias Traimer, Information Society, Austrian Federal Chancellery

Rules (what needs to be taught and how?)

What?

- Media literacy should be considered as one of the priority issues of Internet Governance.
- Measures to increase child participation through the use of ICTs should be increased – this includes child participation in discussions on Internet governance.
- New pedagogies of communication should help children to develop social and technological skills

that allow them in their online as well as offline lives.
- Digital literacy programmes should also be provided for parents and teachers.

How?

- Media literacy means to develop the skills needed to read and produce thoughtful, creative and critical "online prosumers" (producers and consumers) in different media and languages.
- Media literacy needs to be improved, for example through educommunication, i.e. teaching children a thoughtful and critical use of the Internet making them not passive consumers but also active producers of media content.
- Minimum competencies to be Internet literate includes knowing and understanding the convergence of media and languages, to analyse levels and patterns of interactivity and navigation, understanding and applying the criteria of usability and accessibility in a context of collaborative and participative learning.

Responsibilities (who needs to act?)

- The implementation of media literacy programmes has been delayed for too long: much more effort needs to be made now to make children truly media literate.
- Parents and teachers must not be left alone with this task - the industry, as well as the education system and governments and NGOs, have to contribute.
- The key responsibility may lie with the industry and law enforcement bodies.

Workshop six: Sovereignty of states and the role and obligations of governments in the global multi-stakeholder Internet environment

Different aspects of cross-border Internet were discussed from a legal and human rights protection perspective. There was a common understanding that the challenges to the effective exercise and enjoyment of freedom of expression, privacy and other fundamental rights pertaining to the Internet should be addressed at an international level.

Workshop six: Sovereignty of states and the role and obligations of governments in the global multi-stakeholder Internet environment

Messages prepared by Elvana Thaci, Council of Europe

Workshop panellists/key participants: Marco Gercke, Cybercrime Research Institute; Elfa Ýr Gylfadottir, Ministry of Education, Science and Culture in Iceland; Wolfgang Kleinwächter, University of Aarhus, Chair of the Council of Europe Internet Expert Group; Michael Rotert, EuroISPA, European ISP Association (eco); Rolf Weber, Zürich University, GIGA Net; Michael Yakushew, Russian Internet Coordination Center

Solutions are currently being explored in different settings. It was reported that the Icelandic Modern Media Initiative (http://www.immi.is/?l=en) aims at finding ways to strengthen freedom of expression and information globally by, inter alia, providing a modern legal environment for the protection of information sources, whistleblowers and communications.

The Internet is transboundary but it was felt that somehow state territorial borders remain valid as content is stored locally.

One of the main messages that came out of the discussions was that international law provides a wealth of legal concepts which can be instructive for purposes of developing principles of international cooperation on cross-border Internet, such as the principle of equitable and reasonable access to critical resources, state responsibility for actions taking place within its jurisdiction which have negative impact in another as well as state responsibility for action taken by private actors, under a standard of due diligence. Some interesting perspectives on the concept of sovereignty were also discussed. It was suggested that the understanding of sovereignty in Internet governance should be informed by concepts such as aggregated sovereignty of citizens or co-operative sovereignty.

Workshop seven: Open hour on cloud computing: from fog to secure cloud – a regulatory perspective

How can we go from fog to secure cloud?

- Clarifying the roles and responsibilities of actors (including services provided to individuals acting in their personal capacity) through interpretation, guidance and possible revision of regulatory frameworks.
- Improving and facilitating international data transfers and improving certainty as to applicable law and jurisdiction.
- Increasing transparency regarding privacy and security for customers of cloud computing services.
- Improving consumers control over their privacy and the processing of their data (including deletion) and improved enforceability of consumers' data protection;
- Increasing awareness of cloud services, privacy and contractual policies.

- Increasing legal certainty through the adoption of global privacy standards.

Workshop seven: Open hour on cloud computing: from fog to secure cloud – a regulatory perspective

Messages prepared by Kevin Fraser and Sophie Kwasny, Council of Europe

Workshop panellists/key participants: Kevin Fraser, Council of Europe Consultative Committee of Convention 108; Paolo Balboni, Baker & McKenzie (Milan); Rosa Barcelo, Legal adviser to the European Data Protection Supervisor; Cornelia Kutterer, Senior Policy Manager, Microsoft; Jean-Philippe Moiny, research fellow at the FNRS; Katitza Rodriguez, International Rights Director, Electronic Frontier Foundation (EFF); Sophie Kwasny, Council of Europe, Directorate General of Human Rights and Legal Affairs; Barbara Leiner, AEGEE; Cristos Velasco, Director General, Ciberdelincuencia.Org and Member of the IGF Spain Advisory Group

Plenary sessions

Plenary one: Online content policies in Europe – where are we going?

The plenary was divided into two major parts: The first part dealt with the question of **liability**, namely who is responsible for what on the Internet. The second part covered the issue of blocking internet content by the internet industry (without informing the user), comprising both self regulatory regimes and mandatory regulation.

The following questions were asked: What direction is European content policy heading in? Is there a common direction? Is it the right direction, and if not, what should be changed and how?

Plenary one: Online content policies in Europe – where are we going?

Messages prepared by Michael Truppe, Federal Chancellery Austria, Council of Europe

Workshop panellists/key participants: Franziska Klopfer, Council of Europe; Nicholas Lansman , EuroISPA, European ISP Association; Giacomo Mazzone , European Broadcasting Union (EBU) Head of strategic audit; Meryem Marzouki, European Digital Rights (EDRI) & CNRS; Ženet Mujic (OSCE); Vladimir Radunovic , Diplo-Foundation Coordinator, Internet Governance Programme; Maja Rakovic, Ministry of Culture of Serbia, Adviser; Jeroen Schokkenbroek, Head of the Human Rights Development Department, Directorate General of Human Rights and Legal Affairs, Council of Europe; Chris Sherwood, Director, Public Policy, Yahoo; Andrei Soldatov, Agentura.Ru, Journalist ; Avniye Tansug, Lawyer, Senior Member of Cyber-Rights.Org.TR

What direction is European content policy heading in?

The discussion showed that with regard to **liability** of (not solely but in particular) internet service providers, the legal framework itself appears to be relatively stable. As a general tendency it can be noted that the role of the service providers becomes to some extent more complicated with regard to determining whether or not "qualified" actual knowledge of illegal content could result in a liability of the service provider exists in a given case. Some interventions also pointed out that users themselves are increasingly being held liable for their online activities, particularly through criminalizing copyright infringements. Even new sanctioning mechanisms are being introduced, such as the possibility to be cut off from internet access for a certain period of time.

With regard to **blocking,** reference was made to current legislative initiatives to block child pornography websites, while at the same time alternatives do exist and significant effort is being put in combating the problem at the source, namely by taking down websites. Standard-setting is also being conducted with regard to procedural safeguards and minimum requirements when applying blocking mechanisms.

Is there a common direction?

The discussion showed that to some extent a common policy direction exists at European level. With regard to the **liability** issue, the EU since 2000 has in place its Directive 2000/31/EC on electronic commerce, setting out detailed rules for the liability of providers of information society services. This legal framework seems to be quite stable and forms a broadly acknowledged basis for a balance of responsibilities still valid, in principle, today. With regard to the increasing tendency to hold users themselves liable for their online activity at the national level, no common strategy is obvious yet. In fact the measures being introduced at national level vary greatly from country to country, particularly with regard to the idea of using the cutting of internet access as a sanction for illegal online behaviour.

The same is valid also for the question of **blocking**: Some contributors referred to recent plans announced by the EU Commission to block online

child pornography which suggests that the issue will probably remain on the European political agenda for quite some time. Representatives from Eastern European countries gave similar and even further reaching examples of blocking practices in their countries. Standard setting in this field has been conducted by the Council of Europe which presented its Recommendation (2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, that sets out minimum rules for the exercise of blocking measures either being conducted by state or private actors. On the national level however, the practices appear pretty inhomogeneous, ranging from a "no blocking at all" policy to quite extensive models.

Is it the right direction, and if not, what should be changed and how?

With regard to **liability** it was criticised that it is becoming increasingly unclear, what "actual knowledge of illegal activity or information" (which would lead to a liability of the service provider) means, in particular with regard to interactive user generated content (Web 2.0). Some participants claimed that it should not be the responsibility of the service provider to decide upon the legality of the content, but that independent courts need to be further involved. Some are afraid that increasing the liability of service providers could lead to "over cautious" behaviour conflicting with user's freedom of expression. Several interventions also questioned the proportionality of sanctions versus users for illegal online activities, particularly with regard to criminalizing copyright infringements or cutting internet access of perpetrators.

As **blocking** is concerned, a number of participants questioned the approach in general, referring to other methods of combating illegal activities at the source of the problem, namely the host provider level. Some argued that in the vast majority of the cases a takedown of the content could be achieved within hours even in cross-border cases. In addition, very practical problems (such as the efficiency of blocking and the probability of "over-blocking") need to be taken into consideration. Some in favour of blocking mechanisms referred to it as a "second best solution": While taking down the content itself and hunting down the criminals should be the priority, blocking has proven to have a very measurable effect. There was general agreement that the key question to be solved is in any case how to ensure **proportionality** of any blocking measure in relation to related human rights, namely the freedom to receive and impart information. Reference was made to formal requirements that need to be observed: On the one hand, blocking does require a specific (legal) basis that makes it foreseeable (rule of law) while, on the other hand, procedural safeguards should be in place that allow users to question and challenge blocking measures, typically by way of a court decision. Several interventions also stressed the need to further work on the removal of administrative and practical barriers when confronted with cross-border cases both inside and outside Europe.

So where is Europe going with its online content policy? In these two specific fields of liability and blocking, one could conclude from the plenary that while a number of developments take place at the moment there is no clear common and holistic strategy that could be identified. It was emphasized that in order to combat criminal activities at source, there is a significant demand for improvements in international cooperation, particularly by creating efficient procedures and thus speeding up content takedown processes.

Plenary two: Global privacy standards for the internet and working world

Plenary two: Global privacy standards for the internet and working world

Messages prepared by Katitza Rodriguez International Rights Director, Electronic Frontier Foundation (EFF)

Workshop panellists/key participants: Kevin Fraser, Council of Europe Consultative Committee of Convention 108; Andreas Krisch, President of European Digital Rights (EDRi); Sophie Kwasny, Council of Europe, Directorate General of Human Rights and Legal Affairs; Annette Mühlberg, United Services Union (ver.di)/ EURALO Head of E-Government; Jesus Rubi Navarrete, Assistant to the Director of the Data Protection Agency (Spain); Jose Leandro Nunez Garcia, Spanish Data Protection Agency; Eduardo Ustarán, Field Fisher Waterhouse LLP

Privacy and data protection are taking an increasingly important place on both national and international agendas (whether social networking, search engines, Internet of Things, the protection of children online, collection of biometric data as way of asserting identity, cloud-computing and the international exchanges of personal data through billions of online transactions).

Several risks were highlighted: data retention and how this may threaten freedom of association to form and join a trade union; the risks of centralising data held by governments and companies; the lack of legal certainty when defining jurisdictions in a global world, and the effect of the Internet on the so called "right to oblivion".

Some proposals were provided: the need global privacy standards to enable the development of human rights friendly future technologies. Privacy by design and by default need to be the fundamental design principle for future technologies and applications. Data Protection education needs to be included in our education systems to enable every-

body to participate in the information society without putting her/his privacy at risk. Strengthening data protection authorities in order to ensure proper protection.

Civil Society made recommendations in its Madrid Civil Society Declaration: Convention 108 (and its 2001 protocol) and Joint Proposal for Data Protection.

Convention 108 is a legally binding instrument with a flexible follow-up mechanism already in place. Adoption of this binding instrument not only enhances the rights of the data subject, but also strengthens international co-operation between data protection authorities and enhances the ability of organizations to do business around the world. It was said that the Council of Europe has every interest to promote its standards in an increasingly globalize world.

The supervisory authorities from more than 50 countries from all over the world adopted the "Resolution of Madrid", a Joint Proposal of International Standards on the Protection of Privacy aimed to harmonize the various regimes of protection existing in different geographical areas, providing a regulatory model that guarantees a high level of protection and that, simultaneously, can be adopted by any country, with the minimum adaptation necessary to its particular legal, social and economic culture. Standards like this could help to avoid jurisdiction issues in the Internet, and even, if their principles (especially the so called "Privacy by Design") are implemented in the infrastructure of the Net, they could contribute to a better protection to individuals and to an easier and more efficient observance by industry.

There is a need of privacy enhancing infrastructure at work. There is a need to take co-decision making between work councils and employers regarding the introduction of technology that can be used for surveillance.

Law cannot be as fast as technology frameworks. However, international privacy standards like those of the Council of Europe and the Madrid Resolution are based in general principles that can apply to today's environment. Those principles have passed the test of time.

Data Portability: A user should be able to take his data in bulk away from a service and move it to a different service.

Plenary three: Principles of "network neutrality" and policies for an open Internet

The key principles underlying the "open Internet" or network neutrality concept evolve around

- No discrimination of traffic based on sender or receiver
- Unrestricted user choice and access and use of content, applications and services by consumers – businesses – citizens
- Appropriate, reasonable and non-discriminatory traffic management.

Plenary three: Principles of "network neutrality" and policies for an open Internet

Messages prepared by Vladimir Radunovic, DiploFoundation Coordinator, Internet Governance Programmes

Workshop panellists/key participants: Ivan Brincat, Directorate General for Information Society and the Media, DG INFSO – B.1: Electronic Communications Policy Development (video message); Bart Cammaerts, Senior Lecturer, Media & Communication Department, LSE; Angela Daly, Department of Law, European University Institute Frédéric Donck, ISOC European Regional Bureau ; Anders Johanson, Director Network Security Department, Swedish Regulator PTS; Steve Jordan, Telefonica; Franziska Klopfer, Council of Europe; Ana Olmos, Spanish IGF; Michael Rotert, EuroISPA/President of ECO, the German ISPA; Jean-Jacques Sahel, Skype Director of Government and Regulatory Affairs, EMEA; Andrei Soldatov, Agentura.Ru, Journalist; Christoph Steck, Telefonica; Michael Truppe, Federal Chancellery Austria Department for media affairs/information society; Alejandro Vidal, International Office Telefónica, S. A. Public Policy; Christopher Wilkinson, ISOC Wallonia

Under these principles, more detail would likely be needed to provide all stakeholders with more certainty on their rights and obligations, such as what 'discrimination' entails (it should not be just about anti-competitive actions under strict competition criteria); how to define 'reasonable' traffic management and prioritisation (also having in mind eventual disaster management), etc.

Although it was felt that user-centricity/real user choice was key in the debate, it was also emphasised as important to ensure that the perspectives of all stakeholders are considered – end-users, B2B, carrier, operators, applications and service providers.

The importance of transparency of business offers was also strongly underlined by several speakers. It would be important to further discuss: what information of interest for stakeholders should be provided, and which are the best ways to truly inform consumers so that they can make informed choices about which access provider and which subscriptions/plans they pay for.

The European Commission calls for public discussion and will issue a consultation on net neutrality by the summer, with a view to report to the European Parliament and European governments by the end of 2010.

They key considerations for the Commission will be

- Freedom of expression, ie no censorship.

- Transparency.
- Investments in open networks and infrastructure competition.
- Fair competition across the value chain.
- Preserving innovation and investment in both networks and services.

As to whether regulation was needed, many mentioned that the EU already has some provisions in the new telecoms laws around net neutrality – non-discrimination and transparency – and was therefore in a slightly better position than the US. A debate remained opened on the most convenient regulatory approach and legal instruments – if any – in such a dynamic environment. Swedish and Norwegian approaches were mentioned as examples.

Observing the debate from a technical perspective – the need for management – there was a question on whether the bandwidth worries by operators might be short-term predicaments and therefore the discussion should focus on longer term principles for what the Internet should be or remain. The complex economic perspective – creating new business models – was not opened at this time.

The importance of building mutual trust among stakeholders through an open dialogue was emphasised. Generally, it was felt that more work could be done to look at some of the detailed issues, and a multi-stakeholder approach to looking at key issues such as defining reasonable network management (as had been suggested at the 2009 EuroDIG) would be a useful action going forwards, which could be done within the EuroDIG or IGF context perhaps.

The Council of Europe is also finalising a Declaration on Human Rights and Net Neutrality, which has two focal points: (i) proportionality and the necessarily temporary nature of traffic management, and (ii) the enforceability of users' rights, allowing users to challenge ISPs and obtain redress.

Beside possible multi-stakeholder work on issues of detail, and the forthcoming CoE declaration on NN and Freedom of Expression, and beyond possible regulation, many speakers referred to the need for a common EU/European policy for an open Internet.

Plenary four: Policy and decision-making and multistakeholderism – international, national and regional experiences. Is there an European vision?

Multi-stakeholderism is in a way a confrontation between different models of democracy: the representative democratic model versus the participatory democracy model which developed as a way to counter the crisis of representative democracy. Multi-stakeholderism addresses the disconnection between the governors and the governed.

Plenary four: Policy and decision-making and multi-stakeholderism – international, national and regional experiences. Is there an European vision?

Messages prepared by Georgios Kipouros

Workshop panellists/key participants: Ana Cristina Neves, Knowledge Society Agency, Ministry of Science, Technology and Higher Education Head; Bart Cammaerts, London School of Economics and Political Science (LSE) ; Frédéric Donck, ISOC European Regional Bureau ; Markus Kummer, IGF Secretariat; Prof Luis Magalhães, President of the Knowledge Society Agency (UMIC), Ministry of Science, Technology and Higher Education; Giacomo Mazzone, EBU; David Souter, ICT Development Associates/University of Strathclyde; Leonid Todorov, CCTLD.RU

Multi-stakeholderism is indeed related to government accountability to citizens and responsiveness to citizen demands yet it has to function in a dialogue with traditional representative schemes in democracy.

However there are limitations as to what multi-stakeholderism can do. It cannot assure by itself legitimacy and representatively. It cannot assure universality in points of view. It cannot be considered immune to being captured by special interests and manipulative practices.

Multi-stakeholderism is important in today's world but the nature of international politics, rather confliction instead of consensual, should also be considered when examining its potential impact. In fact, multi-stakeholderism has proven to work in practice only when the stakes are not too high.

When expectations from multi-stakeholderism are great but not materialized in actual, real life practices, then this can be a source of frustration for all sides involved.

The definition of participation is also important: there are different kinds of participation varying from full to partial to fake and manipulative participation and each kind can define the success or failure of a multi-stakeholder approach.

Who participates, who are the stakeholders to be involved in multi-stakeholder processes? Who is part of the civil society? What are the right means for inclusion?

Internet governance (IG) and multi-stakeholderism

The IGF is sometimes expected to produce more than its mission, which is to provide a platform for a dialogue. It does not entail a direct decision-making result; it is a policy-shaping rather than a policy-making setting. The IGF gathers all the stakeholders together; there is a substantial, open, transparent

dialogue between governments, private sector, civil society and technical community.

The governments and institutions that run the internet cannot be substituted by the IGF, in the end it's the governments who take the decisions.

Broadly speaking, the value of a forum like the IGF and EuroDIG is established by its participants and such efforts are worthwhile because of the ability of its stakeholders to freely ensure the coherence between local and international models.

The IGF is in many ways a good practice of multi-stakeholderism. There is a substantial impact from the IGF in IG-related legislation. The forum supports the notion that multi-stakeholderism could effectively spread in other areas too.

National IG debates further support the idea of multi-stakeholderism on a global level. For example, authorities in Africa, where there is no tradition of consultation outside the spheres of government, have started adopting the multi-stakeholder approach for issues related to Internet governance.

The genius of the Internet lies in its decentralized architecture. As such, the structure of the Internet governance mechanism mirrors its technical architecture: the Internet is all about inclusiveness, shared responsibility and a multi-stakeholder approach.

There exists a draft code of practice on information participation and transparency for Internet Governance.[1] It sets principles and guidelines in four main areas. The mission of the code is for Internet Governance entities to use it to review their own experience, compare it with other Internet Governance bodies and provide a framework for developing practices as the field grows.

Finally, we should be asking the question: which stakeholders are missing from the dialogue on Internet governance? It is not just for Internet insiders but must engage with those primarily concerned that are spread in different policy areas.

1. The Council of Europe, the UN Economic Commission for Europe and the Association for Progressive Communications (APC) have jointly prepared a draft code of practice on information, participation and transparency in Internet Governance. It sets principles and guidelines in four main areas. The mission of the code is for Internet Governance entities to use it to review their own experience, compare it with other Internet Governance bodies and provide a framework for developing practices as the field grows.

Plenary five: The Internet in 2020?

Important projects have been developed for future Internet devices that take the form of a cognitive assistant (US Military Data Glove, DARPA's PAL – Personal Assistant that Learns, CALO – Cognitive Assistant that Learns and Organises).

Plenary five: The Internet in 2020?

Messages prepared by Yuliya Morenets

Workshop panellists/key participants: João Barros, Director of Carnegie Mellon-Portugal Program, Portugal; Ilias Chantoz, Symantec Government Relations – EMEA and APJ; Oliver M.J. Crepin Leblond, ISOC England/EURALO/GIH Ltd; Wolfgang Kleinwächter, University of Aarhus, Chair of the Council of Europe Internet Expert Group; Yuliya Morenets, TaC –Together against Cybercrime Representative; Ana Cristina Neves, Knowledge Society Agency, Ministry of Science, Technology and Higher Education Head International Relations

We know that the Internet of the future will support a lot more devices. What we don't know is exactly what future Internet services will be in place in 2020.

As a result, we need make sure that we keep the Internet user-centric, supporting the end-to-end principle so as for it to constitute no barriers to innovation. Europe's "systemic barrier" to the Internet's growth is baggage which has to be abandoned in favour of change.

In the future, there will probably be a proliferation of information. The Internet network will be a tool of concentration of information. The question of the protection of critical infrastructure therefore appears. It also engenders military interest in this infrastructure. It will be a question of cyber commands and cyber defence.

It would be interesting to raise the possibility of multistakeholders' war. Will we have the fragmentisation of the Internet?

We will need to answer the question of data distribution and their transfer in the future. It will be also the concern of their hosting and the location. How to find the data? Will it be a real service?

Our society does not need to create barriers to innovation in order to go forward and in order to focus not only on the dark side of the progress, but also and especially on the bright side of it.

Appendix: Youth report

Side event: Internet Governance and Youth: Media literacy, e-Participation and Privacy Participants

Participants were among others representatives of the Finnish Children's Parliament, the Child Protection Center in the UK, of media regulators and authorities such as the Austrian Federal Chancellery and the Swedish Post and Telecom Agency, officials from the Council of Europe (Lee Hibbard, Franziska Klopfer and others), the European School Net, and the London School of Economics and Political Science (media and communications department).

Side event: Internet Governance and Youth: Media literacy, e-Participation and Privacy Participants

Moderators: George Kipouros (European Youth Forum/ LSE, www.youthforum.org) and Maximilian Kall (European Youth Press, www.youthpress.org);

Rapporteur: Triin Rebane (European Youth Forum)

Core themes of the discussion

Challenges: Privacy and protection issues at stake from the perspective of young people. Focus mainly on ethical viewpoints rather than technical aspects.

Tools: Media literacy as a prerequisite for participation in society. Tools to empower youngsters, raise awareness and utilise the benefits of new media technologies as an every-day instrument in education, interaction and communication.

Aims: aspects of merging digital and real life participation in e-Participation projects.

Media literacy

Perspective: Workshop participants stressed an ethical rather than a technical approach. Media literacy is a major part of citizenship education, of integrating young people in a modern society. Critical thinking and understanding is the crucial factor. Media literacy offers a chance of reinforcing the dialogue within, but also between the generations and regions in Europe. New media must be considered a part of daily life, reflecting daily values and human rights, online and offline spheres need to be balanced. A functioning "real life environment" is also crucial for the online behaviour and interaction.

Aims: Everyone needs to be educated with the medium internet as an instrument rather than a subject in itself and be competent to deal with its tools and effects. These life competencies must be recognised in formal curricula and enhanced in non-formal education. Future teacher generations offer new chances in the near future for a change to a more natural use of new media and a critical assessment of media content in schools. Education must stress the opportunities of new media such as building friendships or staying in touch with friends from across Europe, or the ability of expressing opinions in an open and democratic discourse.

Discussion points: Media literacy is to be defined as the ability to access, analyse, evaluate and communicate content competently. Media literacy is about developing a critical attitude towards information: how media and journalists operate, how they work. Questions include how to search for information, how Google works, how information is privileged. However, most people still consume media, while relatively few actually produce content. Media literacy means cultural literacy, social literacy, digital literacy. School curricula need to be entirely reviewed. Media competencies are competencies to be learned, they are not natural. They have to be recognised, just as mathematics or other crucial competencies are. Media literacy and human rights are two sides of the same coin. It is about a transmission of values and education. Parents often lack time and the skills to educate their children, children are left alone.

Perspective of the young representatives of the Finnish Children's Parliament (13 year-olds): "We communicate with friends, chat, look what's happening with friends. Sometimes we see comments that are threatening, but most of them don't have a deep meaning. For us it is learning by doing, our mom helped to set up the profile.

We rarely experience bullying, some take it seriously. The next day at school is sometimes awkward. People sometimes write what they won't say face to face."

e-participation

The Internet is a tool for learning and participation. It facilitates participation in society, offers chances when real meetings and others means of participation are limited due to a lack of resources.

E-participation is complementary to offline participation. Tools such as online petitions have to lead to a certain actual influence. Institutionalised e-participation involving youngsters in a top-down-approach often doesn't work. In setting up platforms youngsters have to be involved already in the development and all stages of realisation. Building trust is crucial in this aspect.

Best practice 1 – Finnish Children's Parliament[1]

Adults facilitate, children chair, the municipality supports. Chats, discussion forums, surveys and other tools allow the online debating of issues such as education or health care. 400 children participate online, aiming at making things better and giving their contribution to the society. The Finnish Children's Parliament offers an opportunity to speak up, make conclusions and to spread these to decision makers.

Online participation must complement face-to-face participation. Pure e-participation might otherwise become an empty concept. On the role of adults in that process, the children's opinion is that they don't actually need their involvement in the discussions, but their support makes things a lot easier: "If the adults take us seriously, we take participation seriously."

Best practice 2 – PlayDecide[2]

Offers role plays, youth consultations, and setting up your own educational module. It is thus useful for schools.

1. http://www.lastenparlamentti.fi/.

2. http://www.playdecide.com/.

Programme

Telefonica Headquarters, Madrid / Spain, 29-30 April 2010

Chaired by Sebastian Muriel, General Director of Red.es

Programme as it stands on 27 April 2010

Thursday, 29 April 2010

08:00 – 09:00 Registration

09:00 – 09:45 Welcome and introductions

Sebastian Muriel, General Director of Red.es (Chairman)
Alejandro Arranz, Madrid City Council
Carlos López-Blanco, International Office Director of Telefónica Corporation
Philippe Boillat, Director General of Human Rights and Legal Affairs, Council of Europe
Jovan Kurbalija, Director, Diplo Foundation
Cornelia Kutterer, Senior Policy Manager, Microsoft
Matthias Fiechter, European Youth Forum
Jorge Perez, IGF Spain

09:45 – 11:30 Opening session - **What is the public and economic value of the Internet for Europe?**
Round-table discussion between high-level representatives of governments, parliaments, institutions and organisations regarding European priorities and perspectives for the Internet as a space for democracy, economic growth and public value. Open dialogue between round-table participants and the audience on how European citizens/users see their role in using and shaping the Internet.

Moderator: Susana Roza, RTVE, Spain

Key participants:
Prof. José Mariano Gago, Minister of Science, Technology and Higher Education of Portugal
Birgitta Jónsdóttir, Member of Althingi for the Reykjavík South Constituency, Party Group Chair Person for the Movement
Visho Ajazi Lika, Deputy Minister for Innovation and the Technology of Information and Communication of Albania
Sebastian Muriel, General Director of Red.es (Chairman)
Gregory Paulger, Director, DG-Information Society and Media, European Commission
Frédéric Riehl, Vice-Director, Swiss Federal Office of Communication
Jeroen Schokkenbroek, Head of Department on Human Rights Development, Council of Europe
Lieven Vermaele, Technical director of EBU

Rapporteur: Vladimir Radunovic, DiploFoundation
Remote participants moderator: David Varona, RTVE Spain

11:30 – 12:00 Coffee Break

12:00 – 13:00 National debates on Internet governance
Dialogue between the audience and representatives from existing and emerging national IGFs. The dialogue will discuss inter alia the similarities and differences in national priorities regarding Internet governance and discern. Who are the key actors in national debates and what lessons can be learned?

Co-Moderators: Lee Hibbard, Council of Europe, Ana Olmos, IGF Spain

Representatives:
Laurent Baup, Forum Internet, IGF France
Martin Boyle , NOMINET / IGF UK
Anders Johanson, Swedish Regulator PTS
Prof Luis Magalhães, Ministry of Science, Technology and Higher Education, Portugal
Siv Mørch Jacobsen, IGF Denmark
Jorge Perez, IGF Spain
Leonid Todorov, CCTLD.RU
Stefano, Trumpy

Rapporteur: Giacomo Mazzone, EBU
Remote participants moderator: Anna Orlova, DiploFoundation

13:00 – 14:30 Lunch

14:30 – 16:15 Workshops 1-3

WS1: Cross-border cybercrime jurisdiction under cloud computing [Main auditorium]
Key issues that could be discussed: The purpose of this workshop is three-fold. First to discuss technical and European legal frameworks, policy and industry initiatives, and best practices surrounding aspects of jurisdiction in the area of cybercrime with special emphasis in the cloud-computing environment; second, to raise awareness on the importance of the intersection between cybercrime, Internet jurisdiction and cloud computing as an emerging Internet governance aspect at the European level; and third, to identify and put forward possible solutions for future policies in this area.

Co-Moderator: Cristos Velasco, Ciberdelincuencia.Org / IGF Spain Advisory Group, Ioana Bogdana Albani, Terrorism and Organized Crime Directorate at the Prosecutor's General Office of Romania

Key participants:
Cornelia Kutterer, Microsoft
Prof. Henrik Kaspersen, Vrije Universiteit Amsterdam
Francisco Monserrat, Spanish RED IRIS-CERT
Michael Rotert, EuroISPA, European ISP Association
Alexander Seger, Council of Europe

Rapporteur: Estelle De Marco, Inthemis – CRESIC
Remote participation moderator: Radu Roxana Georgiana, DiploFoundation

WS2: Geographical and other names of public interest as new TLDs? [CD Auditorium]
Key issues that could be discussed: Admission of new Top-Level Domains (TLDs) and the public interest. Who has the right to register and use which domain name? Which domains should be left to allocation via the market? What responsibilities for public authorities? Should there be different regimes for different categories of new TLDs?

Moderator: Thomas Schneider, Swiss Federal Office of Communication

Key participants:
Amadeu Abri i Abril, CORE Internet Council of Registrars
Iratxe Esnaola Arribillaga, dotEUS Assiciation
Wolfgang Kleinwächter, University of Aarhus
Dirk Krischenowski, dotBerlin
Susan Reynolds, Asociación PuntoGal
Hubert Schöttner, Federal Ministry of Economics and Technology, Germany
Nick Wood, Com Laude

Rapporteur: Wolfgang Kleinwächter, University of Aarhus
Remote participation moderator: [tbd]

WS3: Internet as a platform for innovation and development of *new* business models [Lobby Auditorium]
Key issues that could be discussed: Digitization of content, ebooks, user generated content, use and re-use of existing content. What are the business models for delivering content online? What regulatory environments do businesses need?

Moderator: Martin Perez, ASIMELEC

Key participants:
Elfa Ýr Gylfadottir, Ministry of Education, Science and Culture in Iceland
Miguel Perez Subias, Internet Users Association
Rafael Sánchez, EGEDA
Olaguer Sarsanedas,TV3 Catalunya
Juan Zafra, ASIMELEC, Digital Content Commission

Rapporteur: [tbd]
Remote participation moderator: Alexandra Maria Vasile, DiploFoundation

---

16:15 – 16:45 Coffee break

16:45 – 18:30 PL1: Online content policies in Europe – where are we going?
Key issues that could be discussed: Is it ever 'right' to block content? What procedural and other safeguards exist in European states to prevent disproportionate blocking of content? How are these safeguard applied in practice? Are the reasons for blocking content always transparent and justifiable? Which duties do the different actors involved in creating and publishing content online have? Which rights and duties should they have? What internet governance infrastructure is necessary to avoid that content blocked in one country is is not also unavailable in neighbouring countries where it might be considered legal?

Co-Moderators: Nicholas Lansman, EuroISPA, Maja Rakovic, Ministry of Culture of Serbia

Key participants:
Meryem Marzouki, European Digital Rights & CNRS
Ženet Mujic (OSCE)
Jeroen Schokkenbroek, Council of Europe
Chris Sherwood, Yahoo
Andrei Soldatov, Agentura.Ru, Journalist
Avniye Tansug, Cyber-Rights.Org.TR

Rapporteur: Michael Truppe, Federal Chancellery Austria, Council of Europe
Remote participation moderator: Franziska Klopfer, Council of Europe

---

20:00 Reception offered by the City Council of Madrid / Patio de Cristales

---

Friday, 30 April 2010

09:00 – 10:15 PL2: Global privacy standards for the internet and working world
Key issues that could be discussed: Privacy by design for services and applications (e.g. social networks, cloud computing, etc.); privacy in the workplace.

Moderator: Eduardo Ustarán, Field Fisher Waterhouse LLP

Key participants:
Andreas Krisch, European Digital Rights
Kevin Fraser, Council of Europe Consultative Committee of Convention 108
Annette Mühlberg, United Services Union (ver.di) / EURALO Head of E-Government
Jesus Rubi Navarrete, Spanish Data Protection Agency

Rapporteur: Katitza Rodriguez, Electronic Frontier Foundation
Remote participation moderators: Sophie Kwasny, Council of Europe, Jean-Philippe Moiny, FNRS

10:15 – 11:30 Workshops 4-6

WS4: IPv6 transition – business impact and governance issues [Lobby Auditorium]

Moderator: Fred Harrison, Head of Telefónica Standards

Key participants:
Jacques Babot, European Commission
Marcelo Bagnulo, IAB member
Patrik Fältström, Cisco
Geoff Huston, Asia Pacific Network Information Centre (APNIC)
Martin Levy, Hurricane Electric
Roland Perry, RIPE NCC
Pedro Veiga, Foundation for National Scientific Computing

Rapporteur: [tbd]
Remote participation moderator: [tbd]

WS5: Children and social media – opportunities and risks, rules and responsibilities [CD Auditorium]

Moderator: Matthias Traimer, Information Society, Austrian Federal Chancellery

Key participants:
Roberto Aparici, Universidad Nacional de Educación a Distancia, Spain
María José Cantarino, Telefonica, Teachtoday.eu
John Carr, eNACSO – European NGO Alliance for Child Safety Online, Copenhagen
Jutta Croll, Digital Opportunities Foundation, Managing Director
Javier Garcia, Madrid Office of the Ombudsman for Children
Silva Järvinen, The Finnish Children's Parliament
Anders Johanson, Swedish Regulator PTS
Birgitta Jónsdóttir, Member of Althingi for the Reykjavík South Constituency, Party Group Chair Person for the Movement
Nadine Karbach, European Youth Forum
Narine Khatchatryan, Media Education Center
Georgios Kipouros, European Youth Forum
Yuliya Morenets, TaC – Together against Cybercrime
Rauna Nerelli, The Finnish Children's Parliament
Sara Reid, The Finnish Children's Parliament
Graham Ritchie, CEOP – Child Exploitation and Online Protection Centre
Yolanda Rueda, Fundación Cibervoluntarios

Rapporteur: Jutta Croll, Digital Opportunities Foundation
Remote participation moderator: Franziska Klopfer, Council of Europe

WS6: Sovereignty of states and the role and obligations of governments in the global multi-stakeholder Internet environment [Main Auditorium]
Key issues that could be discussed: What expectations of good neighbourliness and mutual solidarity does the transnational nature of the Internet give rise to in the international community? Is there an obligation in

international relations to protect and preserve the in frastructure, functioning, openness, and neutrality of the Internet in the public interest? To what extent do states bear it? If Internet governance entails a system of shared responsibilities for a common global resource, how does the concept of sovereignty reflect this power and duty allocation reality?

Moderator: William Drake, Graduate Institute of International and Development Studies, Geneva

Key participants:
Birgitta Jónsdóttir, Member of Althingi for the Reykjavík South Constituency, Party Group Chair Person for the Movement
Wolfgang Kleinwächter, University of Aarhus
Michael Rotert, EuroISPA, European ISP Association
Rolf Weber, Zürich University, GIGA Net
Michael Yakushew, Russian Internet Coordination Center

Rapporteur: Elvana Thaci, Council of Europe
Remote participation moderator: Biel Company, Universitat Oberta de Catalunya

WS7: Open hour on cloud computing : from fog to secure cloud – a regulatory perspective [CD Camelot]
Key issues that could be discussed: This workshop will address regulatory issues arising from cloud computing, more specifically concerning data protection, jurisdiction issues and the use of Service Level Agreements (SLAs). How do the traditional actors in the field of data protection (data controller, data processor and data subject) fit in the cloud and what are their duties, responsibilities and rights? Where do we stand in case of change of control of the cloud provider?

Moderator: Kevin Fraser, Council of Europe Consultative Committee of Convention 108

Key participants:
Paolo Balboni, Baker & McKenzie (Milan)
Rosa Barcelo, European Data Protection Supervisor
Cornelia Kutterer, Microsoft
Jean-Philippe Moiny, FNRS
Katitza Rodriguez, Electronic Frontier Foundation

Rapporteur: Kevin Fraser, Council of Europe Consultative Committee of Convention 108

11:30 – 11:45 Coffee Break

11:45 – 13:00 PL3: Principles of "network neutrality" and policies for an open Internet
Key issues that could be discussed: What are the arguments for maintaining an open Internet? What are the key principles for equal access and key requirements for maintaining a functional Web? How to define what is (non-)appropriate management of network traffic? From the European perspective, how will the key principles be implemented in reflection to existing regulation frameworks, and what will the implications be? What could be the global impact of European perspectives? What are the emerging challenges: the relation of neutrality principles and mobile internet, social networks, cloud computing and search engines?

Moderator: Vladimir Radunovic, Diplo Foundation

Panellists:
Ivan Brincat, Information Society and the Media, *(video message)*
Frédéric Donck, ISOC European Regional Bureau
Michael Rotert, EuroISPA / ECO
Michael Truppe, Federal Chancellery Austria, Council of Europe

Key participants:
Graham Butler, Bitek
Bart Cammaerts, Media & Communication Department, LSE
Angela Daly, European University Institute
Anders Johanson, Swedish Regulator PTS
Steve Jordan, Telefonica
Franziska Klopfer, Council of Europe
Ana Olmos, IGF Spain
Jean-Jaques Sahel, Skype, EMEA
Andrei Soldatov, Agentura.Ru, Journalist
Christoph Steck, Telefonica
Michael Truppe, Federal Chancellery Austria
Alejandro Vidal, Telefónica
Christopher Wilkinson, ISOC Wallonia

Rapporteur: Jean-Jaques Sahel, Skype, EMEA
Remote participation moderator: [tbd]

13:00 – 14:30 Lunch

14:30 – 15.30 PL4: Policy and decision-making and multistakeholderism – international, national and regional experiences. Is there an European vision?

Moderator: Ana Cristina Neves, Ministry of Science, Technology and Higher Education, Portugal

Key participants:
Bart Cammaerts, London School of Economics and Political Science
Frédéric Donck, ISOC European Regional Bureau
Georgios Kipouros, JEF – European Youth Forum – London School of Economics
Markus Kummer, IGF Secretariat
Prof Luis Magalhães, President of the Knowledge Society Agency (UMIC), Ministry of Science, Technology and Higher Education
Giacomo Mazzone, EBU
David Souter, ICT Development Associates / University of Strathclyde
Leonid Todorov, CCTLD.RU
Rudi Vansnick, ISOC Belgium – EURALO – ISOCC ECC

Rapporteur: Georgios Kipouros, JEF – European Youth Forum – London School of Economics
Remote participation moderator: Rudi Vansnick, ISOC Belgium – EURALO – ISOCC ECC

15:30 – 16.15 PL5: The Internet in 2020?

Key issues that could be discussed: How will the Future Internet with cyber-physical networks, cloud computing, other technologies and associated new services affect our daily lives? How will content be produced and exchanged in 2020? How will consumers access and use information? How will users communicate with each other? What challenges for human rights, rule of law and democracy? What will be the business opportunities? How will the public value of the Internet evolve?

Moderator: João Barros, Carnegie Mellon-Portugal Program, Portugal

Key participants:
Ilias Chantoz, Symantec Government Relations – EMEA and APJ
Oliver M.J. Crepin Leblond, ISOC England / EURALO / GIH Ltd
Wolfgang Kleinwächter, University of Aarhus

Yuliya Morenets, TaC -Together against Cybercrime
Ana Cristina Neves, Ministry of Science, Technology and Higher Education

Rapporteur: Yuliya Morenets, TaC -Together against Cybercrime
Remote participation moderator: [tbd]

16:15 – 16:30 Coffee Break

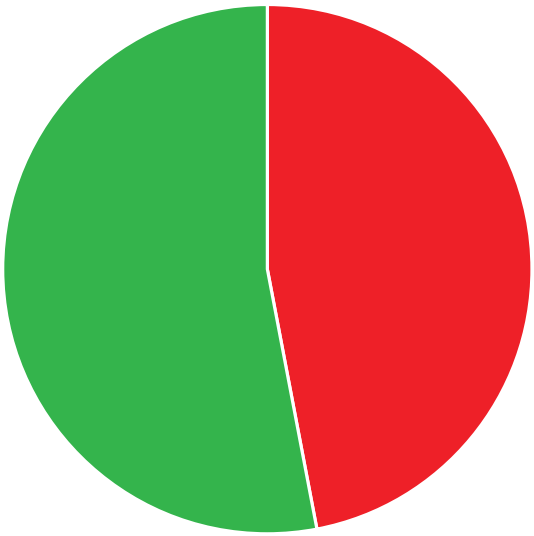
16:30 – 18:00 Wrap-up, reporting-in, take aways and conclusions
Wrap-up with reference to key messages that could be delivered to the IGF 2010

Co-Moderators: Lee Hibbard, Council of Europe, Thomas Schneider, Swiss Federal Office of Communication

Key participants:
Sebastian Muriel, General Director of Red.es (Chairman)
Jeroen Schokkenbroek, Council of Europe

Facts and figures

Participation



Remote participants: 47%
Attendees: 53%

Groups

academics: 12%
business: 26%
civil society: 14%
governmental: 23%
technical: 8%
other: 17%

- 330 registrations
- 291 attendees
- 253 remote participants
- 11 remote hubs in 10 European countries: Azerbaijan, Armenia, Belarus, Bosnia, France (2), Georgia, Moldova, Romania, Serbia, Ukraine

56 countries – participants by country