EuroDIG

European Dialogue on Internet Governance

Messages from Brussels
9 – 10 June 2016

Embracing
the digital (r)evolution


bracing the digi


BRUNO PAILLARD

Content

About EuroDIG

The European Dialogue on Internet Governance (EuroDIG) is an open multi-stakeholder platform to exchange views about the Internet and how it is governed. The main aim of EuroDIG is to promote the engagement of Europeans in a multistakeholder dialogue in order to share their expertise and best practices and, where possible, identify common ground. This enables EuroDIG to pull together national perspectives and to apply and shape European values and views regarding the Internet. Culminating in an annual event that takes place in a different capital city each year, EuroDIG draws 'messages' from all sessions which will be presented to the UN-led Internet Governance Forum (IGF).

This year, the 9th edition of EuroDIG took place in Brussels on 9-10 June, hosted by EURid in cooperation with the European Commission, under the theme "Embracing the digital (r)evolution". Representatives from government, business, technical community, civil society, academia and interested individuals gathered in Brussels to address key Internet governance and policy issues. Located in the "heart" of Europe, the 2016 edition of EuroDIG benefitted from the presence of several European law makers and regulators who had a chance to interact directly with interested stakeholders. These participants included European Commissioner Oettinger, Vice President for the Digital Single Market Andrus Ansip, Secretary General of the Council of Europe Thorbjørn Jagland, Foreign Minister of Estonia Marina Kaljurand and several Members of European Parliament. Other high level participants included inter alia ICANN CEO Göran Marby, Kathy Brown President and CEO of ISOC and the Director General of the European Commission DG Connect Roberto Viola.

EURid's General Manager Marc van Wesemael reflected in his welcoming address on the spirit of the EuroDIG meetings reminding the audience that, "Internet Governance is a process that should remain open, bottom-up, accessible and affordable." Sandra Hoferichter, EuroDIG's Secretary General, added: "The *D* in EuroDIG stands for *DIALOGUE* ... to exchange and discuss ideas, to explore different points of view, to listen to each other." The following two days truly echoed this open and inclusive spirit as over 600 participants discussed topics linked to Internet privacy, security and access in different session formats. EuroDIG is a flexible forum guided by direct input from stakeholders. The topics discussed were submitted by the interested European community during the preparation phase and elaborated in an open planning meeting. Furthermore, the preparation and conduct of each session is guided by the participants and every individual is invited to contribute to this inclusive process. The topics of Internet economy and human rights emerged as the primary areas of interests and were addressed by talking about fragmentation, jurisdiction, Internet of Things, free flow of data, innovation and the evolution of the Digital Single Market.

Source: .eu Illustrated

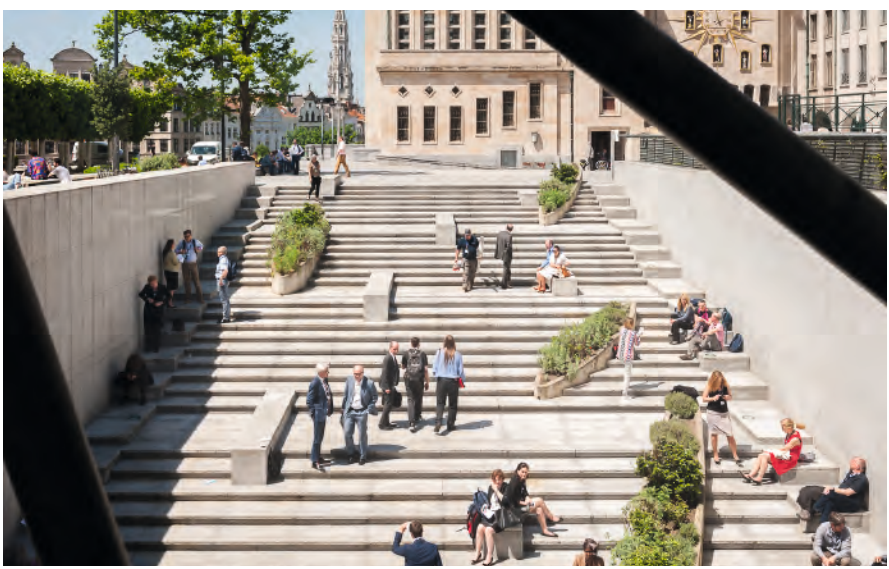
Programme overview

MAIN TRACK	SESSION TITLE
Welcoming	• Megan Richards, Principal Advisor, European Commission • Marc van Wesemael, General Manager, EURid • Sandra Hoferichter, Secretary General, EuroDIG
Keynotes	• Andrus Ansip, Vice President of the European Commission • Günther Oettinger, EU Commissioner for Digital Economy & Society, European Commission • Marina Kaljurand, Minister of Foreign Affairs of Estonia • Thorbjørn Jagland, Secretary General of the Council of Europe • Kathy Brown, CEO and President of ISOC
Open mic	Embracing the digital (r)evolution
Lightning talk	The future in 2026 – the perspective of a global player – Ross La Jeunesse, Google
Hot Topic	Right to be forgotten or to rewrite history?
Plenary	• P1 (part 1) – Will users' trust impact on transnational data flows? • P1 (part 2) – How do transnational data flows affect users' trust? • P2 – IoT; A sustainable way forward • P3 – The rules of the digital world – economy versus human rights • P3a – From cybersecurity to terrorism – are we all under surveillance? • P3b – Intermediaries and human rights – between co-opted law enforcement and human rights protection • P4 – Internet fragmentation and digital sovereignty: implications for Europe
Workshops	• WS1 – Content is the king revisited • WS2 – Confronting the digital divide (1) – Internet access and/as human rights for minorities • WS3 – Technical basics everyone should know before discussing online content control • WS4 – Your IG ecosystem may be out of date. Please check for updates • WS5a – Cybersecurity revisited, or are best practices really best? • WS5b – The future of cybersecurity in Europe - from state of play to state of art • WS6 – Uncovering the DNA of European IG(F) initiatives • WS7a – Zero rating what is it? • WS7b – Impact of zero rating • WS8 – Empowerment through education • WS9 – Signed, sealed – deciphered? Holding algorithms accountable to protect fundamental rights • WS10 – Confronting the digital divide (2) - Refugees, human rights and Internet access
Wrap up	• Concluding remarks: Megan Richards, Principal Advisor, European Commission • Outlook to the IGF in Mexico: Chengetai Massango, IGF Secretariat, Alejandro Martínez Peralta, Deputy Permanent Observer, Permanent Mission of Mexico to the Council of Europe

As well as 12 flashes held in parallel to the plenaries and workshops.
Details at www.eurodigwiki.org.

Pre & side events

DATE	EVENT
6. - 8. June 2016	New Media Summer School
8. June 2016	Roundtable on the contribution of GIPO to multistakeholderism in Internet governance
8. June 2016	Dynamic Coalition: Internet of Things
8. June 2016	Co-designing the Global Internet Policy Observatory (GIPO) 2016
8. June 2016	Knowing. The future of the Internet and how to reboot it
9. June 2016	NorDIG – the feasibility of a future regional IGF in Northern Europe
9. June 2016	Council of Europe platform between governments and major Internet companies on respect for human rights and rule of law online
9. June 2016	Blocking, filtering and take-down of Internet content in Europe. State of play in the Council of Europe 47 member States
10. June 2016	EuroDIG General Assembly



EuroDIG

European Dialogue on Internet Governance

KEYNOTES

Günther Oettinger

EU Commissioner for Digital Economy & Society, European Commission

"The multistakeholder model of Internet Governance has had to ensure that it is an innovative and dynamic source of growth in the digital economy, and we want to see that developed even further both now and in the future and that is why the European Commission is committed to working together with all stakeholders in the shared governance of the Internet based on clear, fair, and transparent rules."

"It is about ensuring a safer Internet that citizens can trust. [...] trust is indeed key to realizing the full potential of the digital era. It is in this spirit that in Europe, we are prioritizing privacy and data security within our digital single market strategy."

"According to estimates, the value of European citizens' personal data has the potential to grow nearly one trillion Euro a year annually by 2020. [...], consumers need to trust companies in order to take up the services they offer. [...] Privacy in the companies in this respect have a competitive edge and the privacy environment in Europe is an incentive that can bring innovative technology companies to set up in our European Union."

"Trust is indeed key in embracing the digital revolution, to grow this year's conference theme. The data initiative along with new data protection rules, are examples of how the European Union can contribute to boosting trust so as to ensure that citizens and companies can fully benefit from the digital revolution."

Andrus Ansip

Vice President of the European Commission

"The Internet is a common good: for the benefit of all humanity and of everybody who uses it, on an equal footing and not subject to the control of governments. It should be a single non-fragmented resource space where people enjoy the same rights as they do offline, and have the same degree of protection."

"Our Digital Single Market (DSM) strategy aims:

- *to make sure that all Europeans - people, industry, businesses – get the best from the online world;*
- *to open up digital opportunities, to make Europe a world digital leader;*
- *to remove barriers, to increase access, to get everyone connected – across society, and all sectors of the economy."*

"Building the DSM will take time and will not be easy. There is one aspect which is essential for its success and on which everything else depends: an open Internet which is robust, reliable and secure. And it goes way beyond Europe."

Marina Kaljurand

Minister of Foreign Affairs of Estonia (10 June 2016)

"EuroDIG is the biggest and most valuable platform for open discussion on Internet governance, freedom, digital market and cybersecurity in Europe by all stakeholders together."

"We should not imagine that security and freedom are in conflict. Cyber security, like the Internet itself, may have grown out of the defense sector, but cyberspace is so much more than a domain of warfare. [...] Cyber security as such needs to become part of our daily life. On all levels. We need to go beyond the thinking that any major development in cyber security requires a major catastrophe or incident. Security cannot be a luxury item; it needs to be a commodity."

"Europe will not benefit from protectionism. Europe may lose too many of our entrepreneurs and unicorns to Silicon Valley, [...], but the answer is more innovation-friendly policies and openness. Nor can we afford to use cybersecurity as a proxy for protectionism. Technology doesn't have a nationality. The development of new technology and technology-driven innovation can only flourish in free market economies. We need to embrace innovative companies and help them develop."

"When it comes to standards and industrial policy, we need to strike a balance. Europe should contribute to standardizing key technologies, but we need to do so in a way that is open and inclusive. We need to avoid making standards the enemy of innovation and competition."

Thorbjørn Jagland

Secretary General of the Council of Europe

"The Internet relies on trust. All of the benefits I have described depend on citizens, entrepreneurs and companies believing that it is a safe space, where their interests, their privacy, their children, and so on, are protected.

And while I don't believe that the Internet will ever go into reverse: people will never stop using it, I do believe that if trust weakens, people will use it in more guarded ways than they otherwise would, diminishing its potential for good – for democracy, for social evolution, and for economic growth.

The answer to misuse of the net is not, of course, heavy-handed regulation. This would kill the Internet. But, equally, a free Internet is not a free-for-all. An open Internet does not mean completely open to abuse."

"Different countries, including in Europe, employ different approaches, meaning that, currently, how free and open your Internet is depends on where you live. And these imbalances are something the Council of Europe is trying to correct."


This keynote is
locking
ALdmNOu4i
ut why the interne
olutionary, becaus
get it. What I'd l
ut instead is wher
olution is headed.
if I can make this
ere we go. For the
ars, a focus


Raise your voice!
fined by the
f not more

EuroDIG

European Dialogue on Internet Governance

KEY MESSAGES FROM PLENARY SESSIONS

Plenary 1 — 9th June

Part 1: Will users' trust impact on transnational data flows?

Part 2: How do transnational data flows affect users' trust?

Reporter: Thomas Grob, Deutsche Telekom AG

1. There is no trade-off between privacy & security

2. Security needs to be a collaborative effort / Subsidiarity works: intervene at the least intrusive level possible!

3. The multistakeholder model offers the tools to solve complex issues. The approach needs to be open, transparent, inclusive, accountable. It also needs active engagement; we need to do more!

4. Transparency and Openness are meaningless if people do not understand what is being disclosed or in case there is no alternative option.

5. Openness requires shared responsibility: companies and governments may not solely and completely be held responsible for what people do online.

IoT - A sustainable way forward

Reporter: Avri Doria, Researcher, Technicalities

IoT is already very present, today. Recognising that IoT is part of the continuum of the Internet growing, issues come up that need to be tackled at global level and by all stakeholders together. And we need to start thinking about a sustainable way forward: what if maybe not 10 years from now but 15 years from now, our environments are fully IoT enabled? And they're not only observing us but also doing things for us, and learning how to take care of us. They're learning what is best for us, and act, partly autonomously, based on what they learn. What would such an environment be like? Do we need a law of ethics for the learning IoT networks for the future? And how do we move forward in a responsible way?

The following points came up during the session for consideration:

1. Transformational: IoT is transformational and has impact on how the world works. In order to ensure this transformation helps us move towards a (human) world we want to live in all stakeholders need to keep the focus on people, their rights and their choices. Most dialogues today are with industry only or with industry and government: how do we get civil society at the table?

2. Trust: we can only reap the benefits of IoT fully if people keep trust in the systems that they bring more good than harm. Life unobserved will disappear. Technology itself will need to help to deal with the complexity that is growing. It needs to be open, interoperable, safe and reliable. What choices will people have and what can we do to protect people's rights? Are existing privacy rules adequate?

Plenary 3 — 10th June

The rules of the digital world – economy versus human rights

Reporter: Luukas Kristjan Ilves, Counselor for Digital Affairs at the Estonian Permanent Representation to the EU

1. It is not the job of private companies to solve public policy problems, especially the small startup that needs room to innovate. Hold big vs small companies to different standards? We expect responsible behavior from companies.

2. Regulation also provides predictability and legal clarity. Courts in Europe making more waves than legislator.

3. The CoE study on filtering, blocking and takedown of illegal Internet content is useful to companies. Could put in a database and updated continuously. Benchmarking, standards, capacity building?

4. We need to get security services in the room talking with us. Government responsibility is not to violate trust we have in them, which is what US did with PRISM. U.S. citizens want privacy too.

Plenary 3a — 10th June

From cybersecurity to terrorism – are we all under surveillance?

Reporter: Valentina Pavel, Association for Technology and Internet, Romania

1. Lowering privacy and data protection standards is not the solution for combating terrorism.

2. Gathering of data should not be confused with requests for information when investigating crimes committed in cyberspace.

3. Transparency, privacy, security and encryption are essential for Internet users and more and more focus should be afforded to them.

4. National exceptions should be eliminated and human rights should be enforced. It is time to solidify frameworks both from a technical as well as political point of view.

5. The lack of harmonization for legal and lawful investigations is one of the biggest problems of the law enforcement community.

6. Authorities have a wide margin of appreciation in deciding who is a terrorist, therefore surveillance measures are sometimes exceeding the proportionality, adequacy and predictability principles.

7. The definition of cybersecurity should include and focus both on the end user as well as on the technical community as well as the justice department. Cybersecurity means protecting the end user and with secure systems, not against them.

8. It is crucial to protect a free and open Internet.

9. All legal principles apply to surveillance measures, therefore the rule of law is incremental applied to targeted surveillance. More training and skills are needed to correct the information management of both intelligence agencies and police.

Plenary 3b — 10th June

Intermediaries and human rights – between co-opted law enforcement and human rights protection

Reporter: Ana Gascón-Marcen, Council of Europe, France

1. Intermediaries have a crucial impact in how we exercise our human rights online.

2. Intermediaries cannot be the cheap police of the Internet, they cannot substitute the primary responsibility to protect human rights of the state although they have to act responsibly.

3. Limitations to intermediaries' liability are basic to promote freedom of expression online and avoid the risk of over compliance.

4. It is necessary to assess the impact on human rights of laws applied to intermediaries.

5. All stakeholders should be heard to find solutions to the different issues.

6. More transparency is needed at all levels.

Plenary 4 — 10th June

Internet fragmentation and digital sovereignty: implications for Europe

Reporter: Anja Gengo, Fellow, Internet Governance Forum

1. All stakeholders have a responsibility regarding the Internet and it is essential to work together for the purposes of sustaining the future.

2. The mechanisms on how to apply the rule of law online in a more horizontal manner should be developed in line with the principles of openness and universality of human rights.

3. The stakeholders should aim for creating the digital single market without borders in order to overcome the fragmentation. More visions and ideas are needed.

4. There is a need for good regulations. Within European institutions, there are recognised good practices that are in line with the most important human rights principles.

5. Variations in laws, legal traditions, political systems and languages should not be perceived as fragmentation. The fragmentation should be discussed in a context of inability to connect end points.

6. The need to negotiate needs to be developed on all levels. Cooperative sovereignty is needed so that we meet important social values in a democratic process.

7. We should work on models on how to extend trade to protect open Internet in line with connecting economic interests of nation states to an open Internet.


(Small group discussion).

EuroDIG

European Dialogue on Internet Governance

KEY MESSAGES FROM WORKSHOPS

Workshop 1 — 9th June

Content is the king revisited

Reporter: Yrjö Länsipuro, ISOC Finland

1. Who's the king now: Platforms? Advertising? Money? Soundbites? Or content, but defined differently. Or down with the king, long live the people?

2. Content can now be produced and distributed by "everybody" and recycled without checking facts. Information inflated by recycling occupies space and pushes out other content.

3. Do we need gatekeepers back? Or should some hierarchy be imposed on the information deluge? More information doesn't lead to better informed people. Would quality control be needed?

4. How to police hate speech? Media literacy training might help. But it should be made with an open mind. Angry speech is not hate speech.

5. Code of conduct for big platforms. Unity of the net under U.S. law?

6. Has the Internet been good for democracy? It has taken out the economic basis of quality journalism. Even if we like free content, there's a price to pay.

7. Content will be produced and producers should be paid, but the structures don't necessarily remain the same.

Workshop 2 — 9th June

Confronting the digital divide (1) – Internet access and/as human rights for minorities

Reporter: Minda Moreira, Internet Rights and Principles Coalition

1. Each one of us is, or can be part of a minority at any one time, the term therefore is not just about numbers, rather is about resources and relative position.

2. Access is not just about a physical connection or terms of use, but also about informed consent, related skills and education, and therefore about having the capacity to fully participate online.

3. Commercial and regulatory designs need to consider much more creatively the needs of all minorities in order to facilitate full access and enjoyment of the Internet. Internet companies share this responsibility whilst governments have a duty to enable the full enjoyment of human rights online for all users.

4. Libraries play an important role in enabling and sustaining public access. Despite cuts in funding librarians can help provide people with the knowledge and skills to acquire capacity to fully participate online.

5. We should all care about minorities, human rights, and Internet access. The more included people can be to necessary Internet services, the more they can make a contribution to society, generate innovation and sustain socioeconomic well-being.

6. Governments have a positive obligation to support full access for all communities to the online environment based on an Internet that is affordable, accessible, diverse and inclusive, hence multilingualism and interoperability are integral features.

Workshop 3 — 9th June

Technical basics everyone should know before discussing online content control

Reporter: Owen Bennett, EuroISPA

1. Networked system defined by open, scalable standards (DNS, IPv4, IPv6).

2. Internet architecture renders access blocking technically infeasible.

3. Content control necessarily entails complex questions surrounding free expression, legitimate interest of law enforcement, and infrastructure providers' right to conduct business.

Workshop 4 — 9th June

Your IG ecosystem may be out of date. Please check for updates.

Reporter: Erwin Yin, Global Partners Digital

1. Internet governance for cybersecurity
Differences in the understanding of basic terms within cybersecurity between different actors are a major stumbling block to progress on Internet governance for cybersecurity. Before sound progress can be made, all parties must form a common understanding of cybersecurity. Cybersecurity should also not be seen as adversarial to human rights, rather they should complement each other.

2. Regulatory/judicial challenges for the Digital Single Market
Individuals and countries do not have a common place to address their concerns, which raises difficulties as the economy transitions into the digital/online sphere. There is a vital need for debate surrounding whether companies have a duty to pay taxes to countries in which they provide services for the use of local infrastructure, with companies such as Uber and Airbnb as prime examples of this debate.

3. Human rights
Human rights issues are hugely broad and cannot be understood as a monolithic issue that exists unrelated to other Internet governance issues. Rather it should form the basis of Internet governance. Human rights should apply equally online and offline – all Internet governance discussions should keep this in mind. Education, particularly for the younger generation, is vital in ensuring human rights are understood and respected equally both online and offline.

Workshop 5 — 10th June

Cybersecurity revisited, or are best practices really best?

Reporter: Bastiaan Goslings, AMS-IX

1. People tend to cluster together and collaborate within trusted communities, because with a trusted relationship something can be done. How to broaden this cooperation by binding with other clusters/communities?

2. We need to collaborate to get things done, and the essential point is then to create trust between stakeholder groups: successful examples were when battling spam and cooperation between CERTS and LEA's. It can be done.

3. Diplomatic communities (with a so called 'military tradition') and technical communities often mean something completely different when talking about security. There is a massive gap. But they are talking to each other and there certainly is an intention to continue the dialogue.

4. How to keep the different 'clusters' open, where issues are discussed? More transparency is necessary when it comes to public-private-partnerships: all stakeholders should (be able to) participate.

5. There is a multitude of platforms and initiatives working on cybersecurity, all spending money and doing capacity building: but are they indeed open and transparent, and what effect do they have and how to bring them together? This is an open question.

Workshop 6 — 10th June

Uncovering the DNA of European IG(F) initiatives

Reporter: Ana Kakalashvili, giz GmbH

1. European IG Ecosystem is very diverse, but at the same time innovative and experimental.

2. Models, topics and processes depend on readiness / awareness of local stakeholders' issues and national needs, but the main aim for all is to raise awareness of the community and get different stakeholders engaged. There is no ideal IGF in policy making processes, whether on national, regional or global level. But there are best practices to look at, share and implement locally. Therefore, there is a need of to have common platform for stronger collaboration and communication between each local IGFs, in tandem with national, (sub) regional and global IGFs.

3. (sub) Regional IGF's are encouraging IG debates and IGFs setting the scene can serve as a catalyser in a region, but there are few strong national IGF who serve as a role model. International (support) organizations are the 'glue' for national / regional IG discussions; they encourage local community and are ready to support.

4. The global IGF is interested in input from national / regional IGF's in particular on:
a. Increasing the collaboration among all IG layers.
b. Fostering the use and the capacity of using the Internet.
c. Connecting citizens (Best Practice Forum - Connecting the next billion).
d. Developing the IGF 10 year strategy including the Sustainable Development Goal (SDG).

Workshop 7 — 10th June

Zero rating what is it?
Follow up: Impact of zero rating

Reporter: Konstantinos Komaitis, ISOC

1. Is it part of Network Neutrality or a business model or both?

2. Is Zero Rating protecting the Internet as a system of innovation?

3. Does zero rating affect customer choice and experience?

4. Should law makers provide a general rule on zero rating? What role does competition play?

5. Discussions on zero rating should focus on principles, e.g. exclusive vs. non exclusive, etc.

Workshop 8 — 10th June

Empowerment through education

Reporter: Claudia Stelter, University of Koblenz–Landau

1. Empowerment through education should be built on Media and Information Literacy Curricula based on an intercultural and intergenerational approach. The curricula need to be standardized and cover evaluation of the learning achievements in building their digital literacy.

2. Empowerment does not equal protection. Media literacy education should cover formal and non-formal learning settings (e.g. libraries) and address first of all critical thinking and critical evaluation of content. Education on human rights and democratic citizenship is strongly interrelated with media literacy education. Curricula should integrate the respective aspects.

3. Gender is not a female issue but one of society at large. It is of primary importance to overcome gender stereotypes in media literacy education and address the needs of all types of gender appropriately.

4. Although the content of Media Literacy Curricula is as debatable as are age limits for the usage of interconnected media like they are set in the EU General Data Protection Regulation now, there is a broad consensus on the concept of empowerment through education.

5. Ensuring equal access to education and equal opportunities should be a priority to Internet governance – vice versa a bottom-up multistakeholder process should provide for participation of all in Internet governance issues.

Workshop 9 — 10th June

Signed, sealed – deciphered? Holding algorithms accountable to protect fundamental rights

Reporter: Lorena Jaume-Palasí, Algorithm Watch

1. Regulators should focus on the social and economical aspects affected by algorithms.

2. There is a need for transparency with regards to how algorithms are used instead of transparency on how data is being processed.

3. There is a value in laws enabling users to request information on how algorithmic decision (supporting) processes are made, including the inputs and discriminatory criteria used, the relevance of outputs as well as purpose and function.

4. Humans use criteria that still cannot be emulated by machines when interacting in daily life.

5. In analogy to individuals who are accountable and supervised by others professionally and socially, algorithms should be held accountable to democratic control.

6. As societies we have defined issues of responsibility and liability in a long process. When it comes to algorithmic decision making we are just starting this process.

Workshop 10 — 10th June

Confronting the digital divide (2) – Refugees, human rights and Internet access

Reporter: Valentina Pellizzer, One World Platform

1. Acts of terrorism being used to justify excessive forms of control and denial of full access for refugees/newcomers in atmosphere of racism and xenophobia.

2. Now that Internet is crucial for right to information, education, health services, employment, and well-being need to denounce curtailment of full Internet access in detention centers that deprives refugees legal assistance and communication with families and thereby their human rights.

3. Public authorities and intermediaries cannot continue to delegate access provisions of key services to volunteers from civil society.

4. One size does not fit all e.g. need to recognize specific needs such as safe and equitable access for women, and young girls, safe spaces online and offline, to sustain learning, confidence and mental health.

5. All service providers and governments have a duty of care towards providing realistic access for these vulnerable communities. This includes not subjecting them to privacy intrusions, disproportionate monitoring of uses or restricting access to social media tools.

6. Need to generate alternative narratives to enable offline and online rights for refugees i.e. to combat cultural stereotypes or racist assumptions about needs at local and national level.

7. Outcome was initiation of an inventory of positive initiatives responding to the actual communication and information needs of refugees in Europe.

South Eastern European Dialogue on Internet Governance (SEEDIG)

About SEEDIG

The South Eastern European Dialogue on Internet Governance (SEEDIG) is a sub - regional IGF initiative dedicated to open, inclusive, and informal dialogue on Internet governance issues among all interested stakeholders in South Eastern Europe (SEE) and the neighbouring area. The second annual meeting took place on 22 April 2016 in Belgrade.

Who governs the Internet in SEE?

• Internet governance (IG) is evolving with time. This evolution of IG makes the main actors be more open and inclusive.

• IG is mostly and mainly about dialogue and collaboration between different actors. And 'consensus' is the key word in IG.

• There is no single main actor in IG: governments are important, but so are users, the technical community, and the private sector. Civil society is bringing up a lot of important topics, but the governance of the Internet is further implemented together with other stakeholders.

• Multistakeholderism is not a single model, but a set of (good) practices and behaviours that helps to improve the governance process and make more voices being heard. Participating on equal footing and inclusiveness are key words for multistakeholder Internet governance mechanisms.

• Representativeness of stakeholder groups and 'legitimacy' are a matter of continuous discussion in IG. But, as long as the governance process is open and inclusive, we can call it multistakeholder.

• (Better) global IG discussions should be shaped in a bottom-up way: from national level to (sub-)regional, and all the way to the global level.

2016 MESSAGES

Bridging digital divide(s) with a #SEEchange in digital literacy

• There are many layers of Internet development in the South Eastern European region, from access and infrastructure (broadband included) to cost and affordability, literacy, content, and services. Deployment of infrastructure is insufficient in itself, and needs to be complemented by measures focused on education and development of local content, among others.

• Internet access solely via mobile technologies should be seen only as a temporary access solution. Mobile technology does not provide complete access to the breadth of the Internet, and, as such, must be reinforced by fibre networks and better use of spectrum, especially in rural areas.

• More efforts are needed in the region (both from the governments and the private sector) to improve the adoption of IPv6 and other Internet technologies that can contribute to bridging the digital divide.

• Digital literacy and awareness about content like e-services or e-government, specifically in local languages and scripts, are critical to bridging the digital divide.

• Internationalised Domain Names (IDNs) can contribute to bringing more people online. Supporting and encouraging the development and use of IDNs in the region is therefore extremely important.

SEEDIG

Discussing cyber(SEE)curity: global issues in regional context

• There are differences in understanding what cybersecurity is among different stakeholders, be they public or private. This lack of harmonised approaches to the cybersecurity definition is combined with the lack of clarity concerning the role of different stakeholders, such as state, private sector, and civil society. Thus, a dialogue between different stakeholders has to be based on clear understanding of the definition and possible roles.

• The role of various stakeholders in protecting cybersecurity will continue to be shaped by the major shift from the concept of security as the duty of the state, to cybersecurity and protection of individuals as a shared responsibility. The distribution of duties and responsibilities among different stakeholders in the South Eastern European region is not established yet, and has to be figured out taking into account rule of law, human rights, and the balance between public and private interests. Governments and other stakeholders have to work together to find the best mechanisms for safeguarding cybersecurity and for a more balanced cyber environment.

• Accountability of all players, especially governments and security services, is a precondition of any working multistakeholder solution.

• Since many of the cybersecurity strategies in the region do not include human rights issues, more attention and awareness is needed to develop the approaches that will implement human rights 'by design'.

• The rule of law is very important, especially when it comes to protecting humans rights and conducting criminal investigations in the digital environment. However, the law on paper is not enough – legal frameworks should be operational and functional.

• Governments are expected to play a vital role in protecting critical infrastructure, combating cybercrime, contributing to education (including through public-private partnerships), and protecting human rights. However, users should take their part of responsibility in protecting the security of their data and/or devices (for example through using end-to-end encryption), and not only rely on governments and private companies.

2016 MESSAGES

Come and solve the human rights puzzle with us

- Privacy is one of the most important human rights online. Privacy and anonymity are needed to ensure that other human rights, such as freedom of expression and assembly, are freely exercised and protected.

- Freedom of expression in every sense should be protected online.

- Access to information will help ensure equality online.

- An important question that needs further consideration is who should be more responsible when it comes to ensuring the protection of human rights online. Governments or the private sector?

- Remedies to issues regarding human rights online need to be discussed by all stakeholders in length and depth.

New Media Summer School (NMSS)

The New Media Summer School (NMSS) is a youth pre-event of EuroDIG lasting several days. At the NMSS young people (18-27 years old) from across the European continent network and prepare for EuroDIG. During the event participants have the opportunity to

- peer-learning with youths from other European countries and background,
- discussing and exchanging with experienced net politics practitioners,
- working on the yearly youth statement to be presented at EuroDIG and the global UN IGF,
- preparing with peers further actions and campaigns to raise their voices during EuroDIG.

The programme of the New Media Summer School is based on the EuroDIG programme and made bottom up by the youth. The NMSS took place from the 6th until the 8th of June. On the 10th of June the NMSS fellows visited the European Parliament.

Geo-blocking (limiting of access to content, based on your geographic location)* must be prohibited:

- Because it is discriminatory making it harder for linguistic minorities and all Europeans to access audio-visual material in different languages.
- Because it harms the economy. It is both inconsistent with the idea of the single market and it prevents consumers from accessing content.

Messages from the youth

Mass Surveillance violates human rights and cannot end cyber-crime and terrorism.

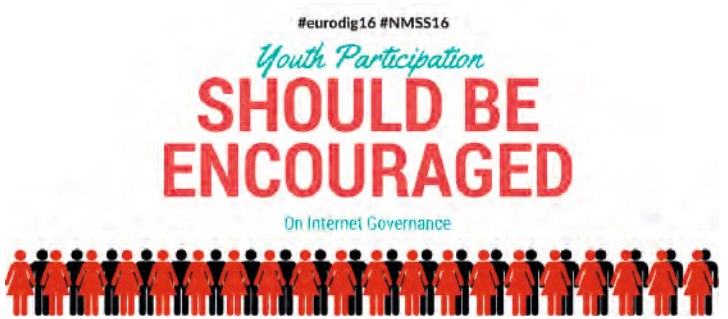
- Alternative tools for law enforcement exist which are compatible with human rights - governments should not collect personal data in bulk.
- Governments cannot meaningfully analyze massive amounts of data.

Open Access to academic content must be freely available.

- When the research is already paid for by citizens through taxes.
- We believe that knowledge must be public.

Youth Participation must be encouraged in the Internet Governance dialogue through mentorship, resources and capacity building.

- Longer-term projects and mentorships would ensure engagement and involvement of young individuals rather than one-off fellowships and grants.
- Youth participation must have the aim of transforming youth into strong actors in the Internet governance debates and processes.
- Digital literacy must be on the agenda of all stakeholders.



NMSS

Affirmative Action in Multistakeholderism is necessary to truly empower the people.
• There are structural differences in power between civil society actors, powerful corporations and governments.
• These need to be addressed at a fundamental level to ensure truly equitable multistakeholderism.

Net Neutrality (The carrying of data without discrimination based on origin, destination or type of data) without exceptions!
• All data must be treated equally.

Access to the Internet is a human right and a public good, and digital literacy is key for all users.
• We demand that each person has access to the Internet.
• Every person must have the opportunity to become digital literate and understand their rights as an Internet user, how the Internet works and be aware of the issues of the Internet through education from an early age in school or at home.

These messages are available in Armenian, Catalan, French, German, Greek, Spanish and Turkish on http://www.eurodig.org/eurodig-2016/youth/y-messages-16/

We thank AT&T, CCIA, Google, ICANN, Microsoft, MEP Julia Reda and MEP Sabine Verheyen for their support!

Policy options for connecting and enabling the next billion – phase II

Contribution to the IGF 2016 community intersessional programme

There was no session particularly dedicated to "Connecting and Enabling the Next Billion" but it was an underlying topic in many workshops and plenaries. No doubt also in Europe there is a great potential of connecting more people. Whilst in some European countries Internet usage and connectivity is close to 100% there are regions, even in economically well developed countries, still lacking of a sufficient infrastructure.

There was agreement that the Internet will be only beneficial if it is free, open and secure. Trust is key in embracing the digital revolution. The role of the industry and governments as key players has been raised in many sessions and a better collaboration was demanded when discussing privacy and security.

Related messages on the role of the industry and governments as key players:
1. There is no trade-off between privacy & security. Security needs to be a collaborative effort. Openness requires shared responsibility: companies and governments may not solely and completely be held responsible for what people do online. (PL 1 Will users' trust impact on transnational data flows?)

2. Law is not enough to protect and is not the main factor. Regulation is important, but most important is an ethical approach from the design phase onwards and the development of technical tools to deal with complexity in protecting privacy. (PL 2 IoT - A sustainable way forward)

3. It's not private companies' job to solve public policy problems, especially the small start up that needs room to innovate. Hold big vs small companies to different standards? We expect responsible behaviour from companies. (PL 3 The rules of the digital world – economy versus human rights)

4. The cybersecurity definition should include and focus both on the end user as well as on the technical community and the justice department. Cybersecurity comes with protecting the end user and with secure systems, not against them. (PL 3a From cybersecurity to terrorism - are we all under surveillance?)

5. Intermediaries cannot be the cheap police of the Internet; they cannot substitute the primary responsibility to protect human rights of the State although they have to act responsibly. (PL 3b Intermediaries and human rights - between co-opted law enforcement and human rights protection)

6. We should work on models on how to extend trade to protect open Internet in line with connecting economic interests of nation states to an open Internet. (PL 4 Internet fragmentation and digital sovereignty: implications for Europe)

7. Commercial and regulatory designs need to consider much more creatively the needs of all minorities in order to facilitate full access and enjoyment of the Internet. Internet companies share this responsibility whilst governments have a duty to enable the full enjoyment of human rights online for all users. (WS 2 Confronting the digital divide (1) – Internet access and/as human rights for minorities)

Another important aspect when connecting the next billion is the enabled Internet user who takes the responsibility for online activities. Participants discussed this matter in various facets.

Related messages on the enabled Internet user who takes the responsibility:
1. Content can now be produced and distributed by "everybody" and recycled without checking facts. Information inflated by recycling occupies space and pushes out other content. Media literacy training might help. But it should be made with an open mind. Even if we like free content, there's a price to pay. (WS1 Content is the king revisited)

2. Access is not just about a physical connection or terms of use, but also about informed consent, related skills and education, and therefore about having the capacity to fully participate online. Libraries play an important role in enabling and sustaining public access. [...] Librarians can help provide people with the knowledge and skills to acquire capacity to fully participate online. (WS 2 Confronting the digital divide (1) - Internet access and/as human rights for minorities)

3. Education, particularly for the younger generation, is vital in ensuring human rights are understood and respected equally both online and offline. (WS 4 Your IG ecosystem may be out of date. Please check for updates)

4. Media literacy education should cover formal and non-formal learning settings (e.g. libraries) and address first of all critical thinking and critical evaluation of content. Education on human rights and democratic citizenship is strongly interrelated with media literacy education. (WS 8 Empowerment through education)

EuroDIG

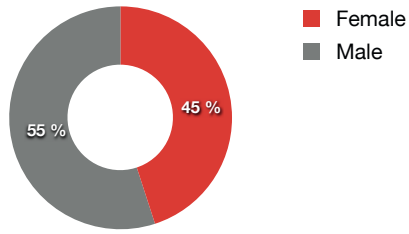
European Dialogue on Internet Governance

FACTS & FIGURES

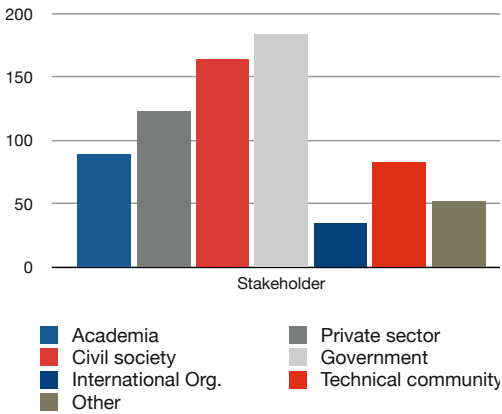
Participation

We received **730** online registrations. There were **601** registered attendees out of whom **443** were those who pre-registered. The following numbers are based on the online registration list.

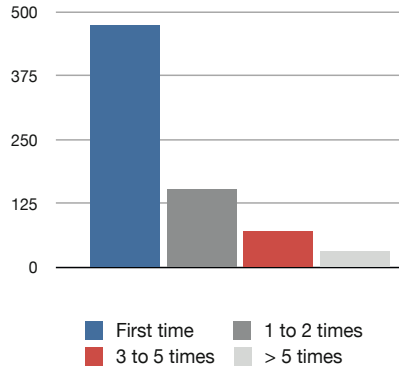
Breakdown of participants by gender



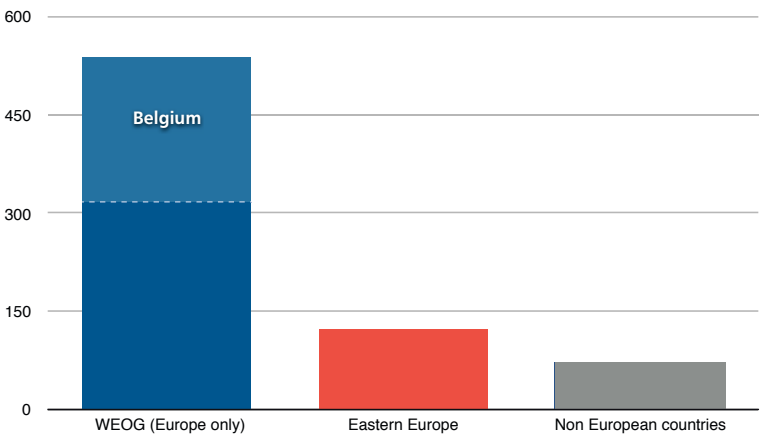
Breakdown by stakeholder group



Number of EuroDIG attended



Breakdown by country of residence (classified by the UN regional voting blocks)



Remote participation usage

Day 1	Adobe Connect attendees	Streaming viewers
Room 201	30	37
Room 211	43	32
Room 213	29	35
Room 214	28	30
Gold Hall	125	250
Total	**255**	**382**

Day 2	Adobe Connect attendees	Streaming viewers
Room 201	41	50
Room 211	29	26
Room 213	7	41
Room 214	55	32
Gold Hall	87	183
Total	**219**	**333**

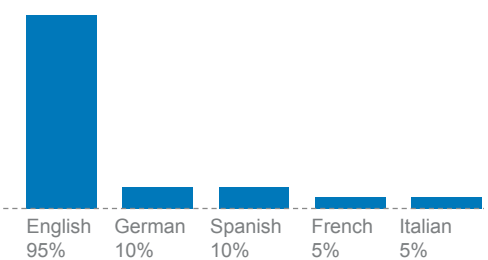
Twitter stats

Country ranking in social media

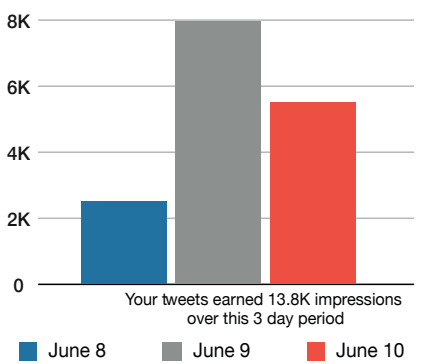
Country name	Percent of audience
Germany	11%
Belgium	10%
United Kingdom	8%
United States	7%
France	7%
Italy	5%
Spain	5%
Netherlands	3%
Switzerland	3%

Age category	Percent of audience
13 to 17	< 1%
18 to 24	4%
25 to 34	54%
35 to 44	25%
45 to 54	16%
55 to 64	< 1%
over 65	< 1%

Languages



#eurodig16 – 2467 Unique tweets



Break down of submissions

Submissions per category	No.
Access & literacy	13
Development of IG ecosystem	23
Human rights	38
Innovation and economic development	16
Media & content	7
Security	13
Technical & operational issues	11
Other	11
Total	**132**

Submissions per gender	No.
female	62
male	70

Submissions per stakeholder group	No.
academia	19
civil society	44
government	10
international organisation	10
private sector	15
technical community	21
youth	6
other	7

Submissions per region	No.
Europe (all regions)	113
SEE and EE region	41
other	19

Number of countries participating	No.
WE region	13
SEE and EE region	12
other	8

At EuroDIG we are not asking for sessions or workshop proposals, but we are asking for issues and topics of high interest to many stakeholders across Europe. In order to facilitate the structuring of the proposals, we are suggesting a number of categories for the EuroDIG programme.

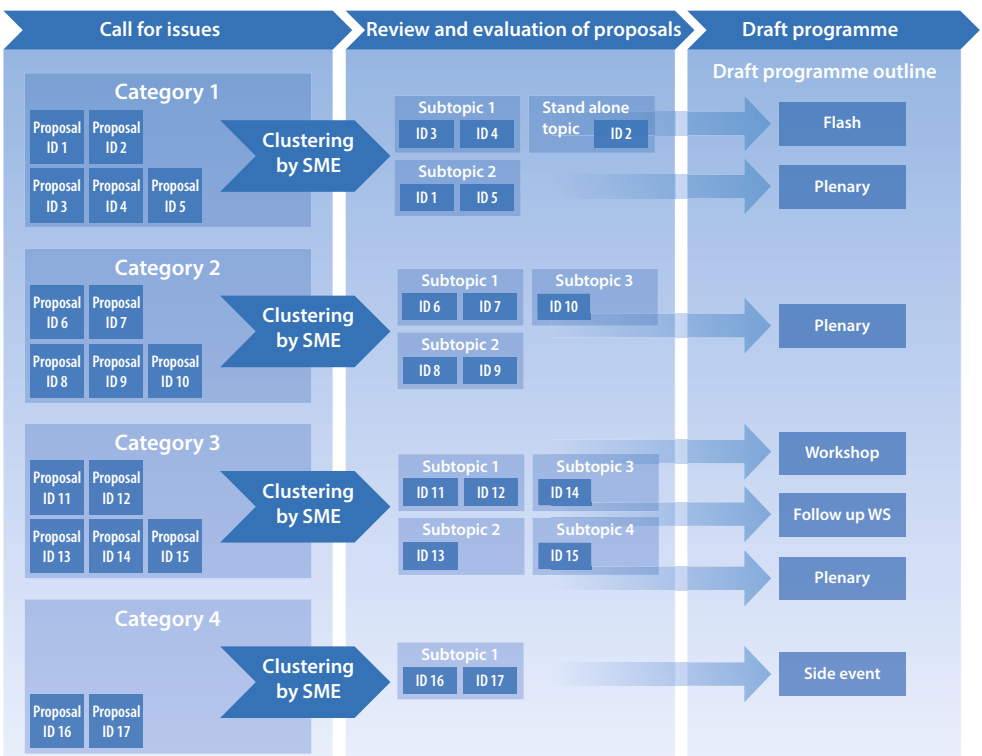
The EuroDIG programme planning process is open for everyone to join at any time!

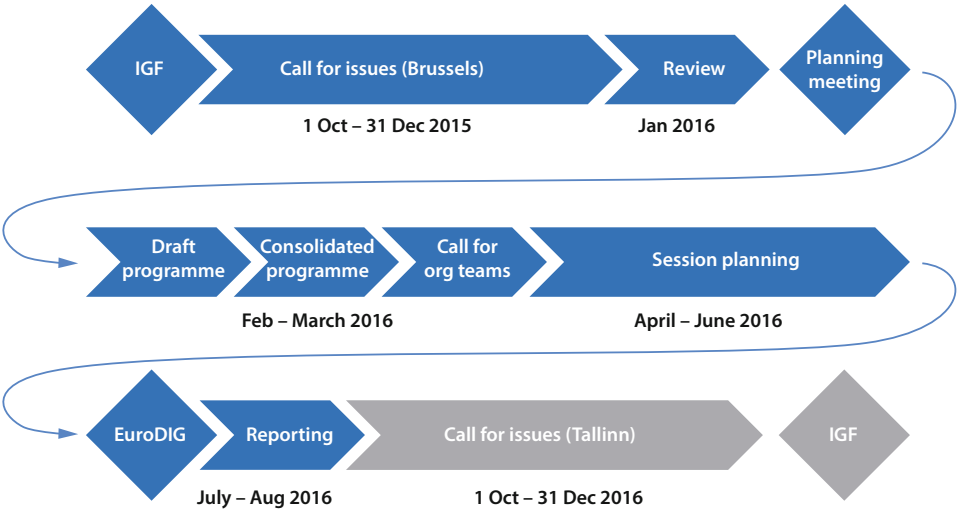

RT: @InterConnectIIG .@KathyCBrown, #ISOC: "No single legilsation or tech fix can ensure #security #online. We need collaboration." #eurodig16
7 minutes ago
Reply
ferdeline Ayden Ferdeline
RT: @BerinSzoka Same reactionary mentality drives moral panics over privacy and Uber, etc: SLOW DOWN change so we can "get comfortable" with it #EuroDig16
7 minutes ago
Reply
spinzo
RT: @BerinSzoka Typical precautionary principle nonsense: we can't embrace something new "until we're

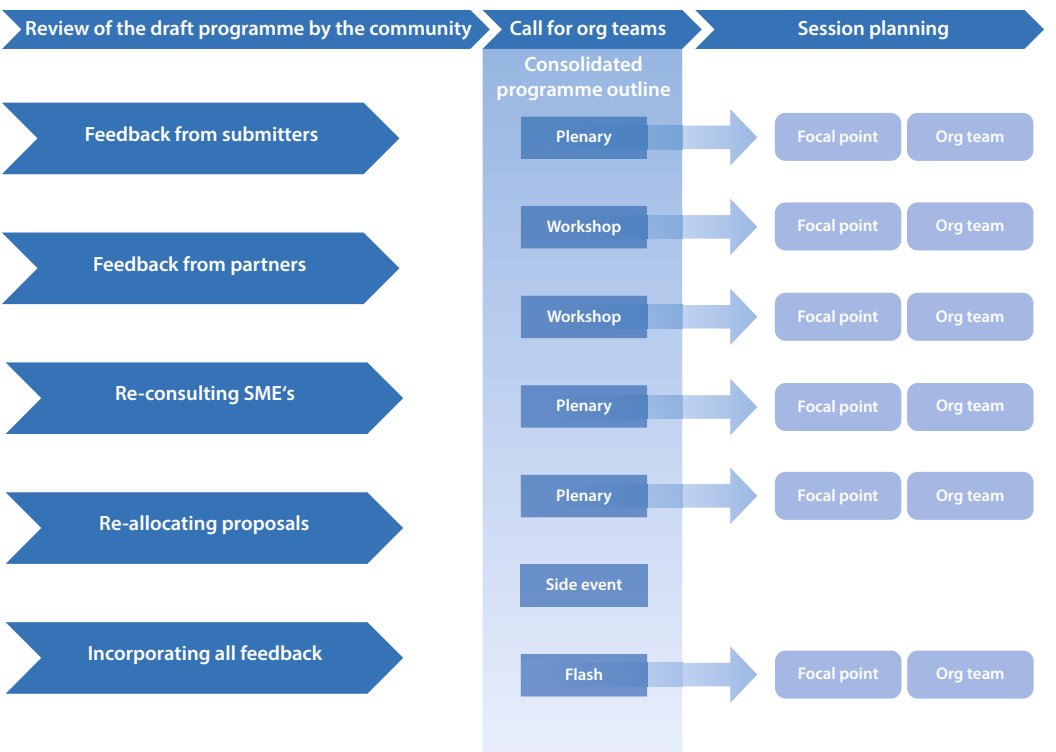
EuroDIG 2016 programme planning process

All submissions were compiled by Subject Matter Experts (SME's), presented and discussed during the open planning meeting where everyone was invited to participate. The aim was to identify topics which could be incorporated in one session, while reflecting different perspectives. Furthermore the EuroDIG community evaluated the draft programme outline before org teams started the session planning. Org teams were open for everyone interested to contribute at any stage of the process.

EuroDIG's key principles are "always open, always inclusive".




IGF
Call for issues (Brussels)
1 Oct – 31 Dec 2015
Review
Jan 2016
Planning meeting
Draft programme
Consolidated programme
Feb – March 2016
Call for org teams
Session planning
April – June 2016
EuroDIG
Reporting
July – Aug 2016
Call for issues (Tallinn)
1 Oct – 31 Dec 2016
IGF


Review of the draft programme by the community
Call for org teams
Session planning
Consolidated programme outline
Feedback from submitters
Feedback from partners
Re-consulting SME's
Re-allocating proposals
Incorporating all feedback
Plenary
Workshop
Workshop
Plenary
Plenary
Side event
Flash
Focal point
Org team
Focal point
Org team
Focal point
Org team
Focal point
Org team
Focal point
Org team
Focal point
Org team

Social events

Google kindly invited to a cocktail on 8th June 2016 where Alexander De Croo, Deputy Prime Minister of Belgium welcomed all participants.

EURid organised a fabulous night of the seventies at Hotel de la Poste on 9th June 2016 and handed over the EuroDIG flag to the next host, the Foreign Minister of Estonia Marina Kaljurand.

See you in Tallinn in June 2017 and celebrate the 10th anniversary of EuroDIG!

Stay informed and contact us!

EuroDIG
European Dialogue on Internet Governance

www.eurodig.org

office@eurodig.org

www.facebook.com/eurodig

@_eurodig

www.eurodig.org/
about/newsletter

Imprint

Published by:

EuroDIG Association
Rue Jehanne-de-Hochberg 16
CH-2000 Neuchâtel

Email: office@eurodig.org
www.eurodig.org

Graphic Design: Gerd Hoffmann, gidesign, Leipzig/Germany

HOST 2016

EURid
www.eurid.eu

IN COOPERATION WITH

European Commission

INSTITUTIONAL PARTNERS

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ICANN

Internet Society

EBU

EURALO
ICANN

SPONSORS

Google

Microsoft

SWITCH

VERISIGN

denic

SIDN

Afilias

nic at
the austrian registry

Telefónica
FUNDACIÓN

ERLEBEN, WAS VERBINDET.

eco
Verband der Internetwirtschaft e.V.

dns be

IGFSA
Internet Governance Forum Support Association

UNINETT Norid