

EuroDIG

European Dialogue on Internet Governance

Messages from The Hague
19–20 June 2019

Cooperating in the Digital Age



Thanks to our Host team!



Content

EuroDIG 2019 – Highlights from The Hague	4
EuroDIG 2019 programme	8
Welcome messages and keynotes	11
Messages from plenary sessions	15
Messages from workshops	23
YOU th DIG Messages	37
Assembly of National and Regional Initiatives on Internet governance (NRIs)	41
Participants say: Great opportunity for networking.	45
Facts and figures	49

About EuroDIG

Launched in 2008, EuroDIG, the European Dialogue on Internet Governance, is a unique annual event that brings together Internet stakeholders from throughout Europe (and beyond), and from across the spectrum of government, industry, civil society, academia and the technical community. Stakeholders and participants work over the course of each year to develop, in a bottom-up fashion, a dynamic agenda that explores the pressing issues surrounding how we develop, use, regulate and govern the Internet. EuroDIG participants come away with broader, more informed perspectives on these issues and new partners in responding to the challenges of the information society.

EuroDIG 2019 – Highlights from The Hague

Cedric Amon, Geneva Internet Platform

The challenges in the digital sphere are met with a multitude of calls for action and declarations worldwide. In this spirit, EuroDIG 2019 has sent a strong signal on the need for stakeholders to strengthen their co-operation within the digital ecosystem. Here are the most important updates, trends, and discussions from the annual conference:

Co-operation is key

This year's theme, 'Co-operating in the Digital Age', featured across many sessions. The discussions emphasised the need to further address topics such as 'universal acceptance' (UA) to make software accept all valid domain names and addresses. Improving UA and streamlining digital processes has the potential to greatly improve the cooperation between the private sector and civil society and the scientific community. Moreover, it bears the chance to foster the collaboration between members of the technical community and policymakers on issues such as the fight against disinformation.

European regulatory frameworks: a regulatory challenge

High on the agenda were also discussions on European regulatory frameworks. The Council of Europe (CoE) promoted its Budapest Convention on Cybercrime and the Second Additional Protocol to the Budapest Convention, which is currently being negotiated in Strasbourg. Furthermore, the Council representatives expressed concern regarding the risk of deepening discrimination, particularly through the increased reliance on artificial intelligence, and the loss of human oversight over new technologies. To address these issues, the CoE has started aligning ethics frameworks to create a more coherent framework across its member states. Another concern was the deepening of digital gaps among people in different social classes but also among nations, given that digital technologies still strongly favour developed countries.

The European Commission (EC) highlighted that with a wider acceptance of the multistakeholder model, tensions between the latter and multilateral approach, between bottom-up and top-down approaches, and between a purely market-based approach and state intervention should be overcome in order to focus on pressing challenges for the EU and its citizens. These include the centralisation of data, privacy issues, and the lack of trust, as well as new means of governance for new technologies.

The EC acknowledged its responsibility in contributing to solution finding of these issues and to finding regulatory approaches which will guarantee the openness and fairness of the Internet. The collaborative aspect is thus a priority for the European Commission as well.

The first regulatory steps such as the General Data Protection Regulation (GDPR) were well received and lauded for its consequent stance on ensuring privacy protection. Panellists highlighted the success of the EC for adopting a regulatory approach which reflected the will of a group of states with common values. In general, the debate around norms and how to implement them was a preoccupation for many participants and so the upscaling of regional approaches, such as the one of the EC, was seen as a promising avenue for the finding of global solutions.

However, some of the EC regulations and directives such as the European Copyright Reform or the e-Evidence Proposal were heavily criticised by a number of panellists. The Directive on Copyright in the Digital Single Market came under fire for having sided too strongly with the interests of rights holders such as publishers and record labels and thereby accepted the risks of over-blocking online content.

Similarly, the EC e-Evidence Proposal was contested for exposing platform providers to requests from all European member states as opposed to complying with orders from the national authorities where the companies are located.

How should IoT and AI be governed?

Debates on new technologies such as artificial intelligence (AI) and the Internet of Things (IoT) revolved mainly around the need to find new ways to govern them without hampering innovation. Emerging challenges needed to be addressed through ethics implementation, the elaboration of guiding principles and 'by design' measures. Ethics and trust 'by design' measures seem to gradually become viewed as the most promising way to ensure privacy and data protection.

While generally, the discussions around the need for more regulations and norms about the Internet were much divided, opinions converged around the need for norms and frameworks regulating the development and application of new technologies. Their high reliance on data and often personal information makes it critical for them to be placed under accountability mechanisms, a view shared by the Report of the UN High-Level Panel on Digital Cooperation.

EuroDIG and the UN High-Level Panel on Digital Cooperation

In the two sessions dedicated to the recently launched report of the High-Level Panel (HLP) on Digital Cooperation, participants highlighted that multistakeholderism and multilateralism should not be viewed as fundamentally opposed

approaches to Internet governance but rather to see them as complementary in order to take advantage of the benefits of both approaches. Co-operation should therefore not be viewed as something to be imposed on different processes, but rather as a way to ‘connect the dots’ and exchange information and views about the existing processes and initiatives.

Participants furthermore welcomed that EuroDIG is providing a space to discuss and assess the HLP report and collate views from all stakeholders from all over Europe on the report and its recommendations. EuroDIG is going to summarise the received inputs and make them available to the global public for further discussion at the UN Internet Governance Forum in Berlin in November or at any other occasion

Fighting misinformation

The discussions found that the many challenges originating from mis/disinformation require a wide range of responses such as making online platforms responsible for the management of online content, as well as ensuring the financial and political independence of news outlets.

Other ways of avoiding misinformation included privately-owned fact-checking tools or the creation of public support teams for specific types of journalism (such as investigative journalism) and redistribution mechanisms for online platforms to finance the production of quality media content.

All-rounded discussion on digital literacy

A topic which transcended most of EuroDIG sessions was the importance of digital literacy. The subject was discussed from various angles, namely through providing personal cybersecurity, reducing information asymmetries which are very significant in the field of new technologies, to protecting children from online harms. Similarly to ethics ‘by design’ protection measures, digital literacy was recognised as one of the most effective ways to strengthen cybersecurity.

A stronger role for digital policy?

The debate around the need for increased regulation and more norms in the digital fields such as cybersecurity, content regulation, as well as the creation and circulation of misinformation remained contested.

While many discussants argued that there are already many norms and declarations in the digital field, an increasing majority argued that the application of soft law and non-binding regulations is not enough to tackle the challenges in the digital sphere.

The Internet Governance Forum (IGF) was regarded as an ideal venue to discuss and further advance norms at the global level in a number of sessions. In line with the many calls for more tangible solutions at the IGF, participants cautiously raised the possibility of allocating the forum with greater norm-proposing powers. Particularly in the cybersecurity domain, the panellists favouring binding approaches argued that an updated IGF would be a good way to shape the future of the global cybersecurity architecture through the elaboration of norms in a multi-stakeholder fashion. The IGF was also identified as one of the best suited forums to discuss future challenges posed by AI and IoT.

This discussion was well reflected by the recommendations of the UN High-Level Panel on Digital Cooperation which proposed three updated mechanisms for global digital cooperation. The aim of the IGF Plus (IGF+) model would be to build on the strengths of the existing IGF and to address its shortcomings including those related to norm-making and state participation.

EuroDIG 2019 – Programme

- Access & literacy
- Development of IG ecosystem
- Human rights
- Innovation and economic issues
- Media & content
- Security and crime
- Technical & operational issues
- Cross cutting / other issues

16-18 June 2019

Time	Pre-Events
	YOU th DIG – Youth Dialogue on Internet Governance, 16-18 June 2019, The Hague / Netherlands

Day 0 | 18 June 2019

Time	Pre-Events
12:00 - 14:00	PRE 1: Digital cooperation in action – A collaborative case study
14:00 - 14:30	Coffee break
14:30 - 16:00	PRE 4: NRI ASSEMBLY • Getting citizens on board • Intersessional work and cooperation among NRIs
16:00 - 16:30	PRE 5: Newcomers briefing session with Subject Matter Experts
16:30 - 18:00	EDU 1: Opening the black box – How technology and policy shape the internet?
18:00 - 20:00	Welcoming cocktail

Day 1 | 19 June 2019

Time	Sessions
9:00 - 9:15	Welcome • Ms. Pauline Krikke, Mayor of The Hague • Ms. Sandra Hoferichter, Secretary General EuroDIG
9:15 - 10:15	What's up in the Netherlands? – Showcase of Dutch best practices in the digital domain
10:15 - 10:30	Opening keynote • Ms. Mona Keijzer, State Secretary for Economic Affairs and Climate Policy of the Netherlands
10:30 - 11:00	Coffee break
11:00 - 12:20	Lightning talk: The technological edge in 2030 – What role for technology in society? • Jonathan Cave, Turing Fellow • Jaya Baloo, Chief Information Security Officer, KPN Telecom
12:20 - 12:45	Keynote The technological edge in 2030 – What role for technology in society? • Ms. Mariya Gabriel, European Commissioner for Digital Economy and Society
12:45 - 14:00	Lunch break

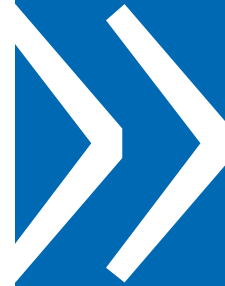
14:00 - 15:30	PL 2: Intersection between public policy and technical standards	WS 2: GDPR Implementation – Blind spots, opportunities, and the way forward	WS 3: Regulation and the Internet economy – How to create the right building blocks for 5G networks	WS 4: Children in the digital age – How to balance their right to freedom and their right to be protected?	WS 1: Internet consolidation – Opportunities and challenges	Flash 3: Coordinated vulnerability disclosure – The government is here to help?
15:30 - 16:00	Coffee break					Flash 4: Chances and challenges of single sign-on digital identities for citizens.
16:00 - 16:30	Digital Cooperation – Report of the UN high level panel – PART I					Flash 5: The post-apocalyptic world without IPv6
16:30 - 18:00	PL 3: Emerging technologies and human rights				EDU 2: Advanced literacy – Basic education for the digital age	Flash 6: Digital national sovereignty and Internet fragmentation
18:30 - 23:00	Social evening at Boomerang Beach Club					Flash 7: Accountability in the Digital Age
						SEEDIG community informal gathering

Day 2 | 20 June 2019

Time	Sessions
9:00 - 9:30	Digital Cooperation – Report of the UN high level panel – PART II
9:30 - 10:30	PL 4: Making norms work – Pursuing effective cybersecurity
10:30 - 11:00	Coffee break
11:00 - 12:30	PL 5: Ethics by design – Moving from ethical principles to practical solutions
12:30 - 14:00	Lunch break
14:00 - 15:30	PL 6: The European Copyright Reform – What just happened, what's next, and what does it mean for the Internet?
15:30 - 16:00	Coffee break
16:00 - 16:30	Presenting Youth Messages
16:30 - 17:30	PL 7: Tackling online harms – A regulation minefield? Present and future.
17:30 - 18:00	Wrap-up

“Messages from The Hague” compile the conclusion of plenary sessions and workshops and were drafted by reporters from the Geneva Internet Platform (GIP) in coordination with the Org Team of each session.

Additional reports, transcripts, video records and further reading recommendations for each session can be found on the EuroDIG Wiki: <https://eurodigwiki.org/>



Welcome messages and keynotes



Pauline Krikke Mayor of The Hague



... only a free and safe Internet will help to build a better world. Attempts to nationalize it, and place it under government control will rob the Internet of its unique power, the dynamism that comes from the fact that everyone can put something on it. Of course, we all want to see crime and abuse banned from the Internet, but that should never be a pretext for censorship.

Mona Keijzer State Secretary for Economic Affairs and Climate Policy of the Netherlands



And now that the Internet has grown up, it's becoming even clearer: cooperation is critical. Many different actors keep the Internet going: research institutes, standardisation and technical organisations, the business community, civil society, user organisations and governments. But none of these parties have complete authority over the Internet. And none of them can substantially influence the way the Internet works. At least, that's how it should be. The Internet belongs to nobody and everybody at the same time. This makes the Internet a fertile ground for creativity, free speech and flexible trade.

Mariya Gabriel European Commissioner for Digital Economy and Society



The idea that the technical community, civil society, academia and private sector all have a role to play in the governance of a core infrastructure like the Internet was really ground-breaking. This idea is now mainstream, however, having been right once, it's not enough. We need to be lucid about current and future challenges on the concrete implementation of this multi-stakeholder principle. ... 14 years after, we are indeed entering a new phase. A new phase where a synthesis is possible between historical oppositions, opposition between the multi-stakeholder model, and the multilateral approach, between bottom up and top down, between a purely market-based approach and state intervention. Indeed, I believe a synthesis that's not only possible but also much needed.

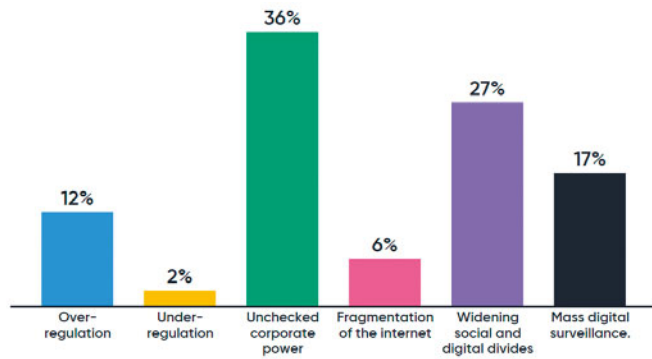
Sandra Hoferichter Secretary General EuroDIG



... cooperation is a big word, the good thing is it is better understood than Internet governance, because it is a universal word with a similar syntax across the globe. But opinions are wide spread how far cooperation goes. It bears a promise that can be broken, for instance when the commitment to cooperate remains lip service, or when the level of discussion is disconnected from the level of taking decisions.

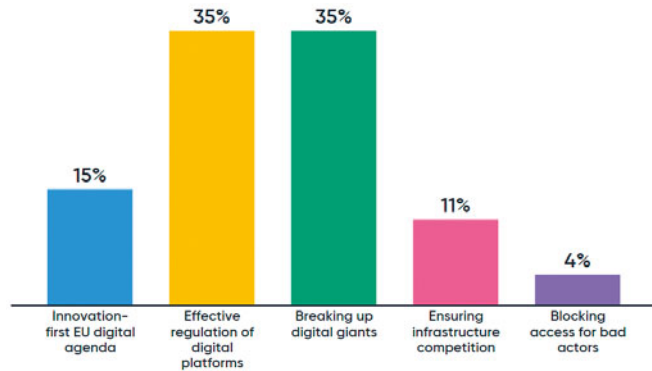
Audience poll (PL1):

Greatest threat to a healthy digital environment in 2030?



98

What to do *now* for healthy digital environment in 2030?



98

Plenary sessions



Global digital governance – can technical solutions respond to policy questions?

Report: Stefania Grottola

- The current status quo is featured by a variety of legal tools with various degrees of effectivity. Approaches should be principle based and facilitate statutory rules and restrictions with duties of care.
- Ensuring trust in hardware and software devices has long been focused on lengthy and expensive standard-setting processes and lengthy and expensive certifications which could undermine innovation. A different approach could consist in making users more responsible for their actions, being informed by standards, labels, and self-certification that is enforced by third parties. Being in charge of their online privacy and security would give control back to the users.
- The role of governments and policymakers should be a future-oriented one. Policymakers need to develop long-term strategies to address existing and future challenges, such as but not limited to, inequalities, the digital divide, and the impact of digitalisation on jobs. Such strategies need to have a long-term vision to ensure effectivity in an exponentially evolving digital and technological scenario.
- Due to the rapid evolution of technologies, regulation struggles to keep up with the pace of change. Therefore, regulation is not enough: there is a need for norms, standards, and safety nets. The approach needs to be human-centric, focused on the protection of individual rights and a global regime where human rights standards are respected.
- As a society, we should be aware of two existential threats: the destruction of the environment we are evolving within, and the automation of the exploitation of human psychological weaknesses at scale. Such industry-created threats need

to be tackled within the next ten years. In order to achieve a healthy digital environment by 2030, an effective regulation of digital platforms should be developed. Moreover, the excessive power and influence of digital giants should be tackled.



Intersection between public policy and technical standards

Report: Cedric Amon

- The intersection between public policy and technical standards does not rely on the implementation of standards alone, their adoption and recognition is equally important. This is where the dialogue between the policy-makers and code-makers comes in, it should be aimed at breaking down silos.



- It is essential to bring down the barriers between the policy-making and code-making communities. The multistakeholder model provides the necessary framework to achieve this and must be further enhanced to create more trust and better understanding between the communities. Trust between the stakeholders can be achieved once the respective stakeholders have a greater grasp of the complexity of the fields of their partners.
- Applying standards is not the only way to make the Internet work. There is an important role for each method and mechanism of the rule-making arsenal wherein good practices might provide very strong (but voluntary) mechanisms, without the (often) innovation-hampering elements of a law.

Emerging technologies and human rights

Report: Clement Perarnaud



- All stakeholders, including the private sector, agree that a form of regulation concerning the use of digital technologies is needed to protect individuals, build public trust, and advance social and economic development. However, divides remain on the scope and bindingness of such regulation, even if predictability and legal certainty appear essential. There is nevertheless a broad consensus on the need to initiate open-ended and inclusive debates to provide guidance and introduce new frameworks. For example, at the stage of product development, to address the significant impact of new technologies on individuals and the exercise of their human rights.
- States should take appropriate measures to ensure effective legal guarantees and that sufficient resources are available to enforce the human rights of individuals, and in particular, those of marginalised groups. There is a need to enforce mechanisms to ensure that responsibilities for the risks and harms for individual rights are rightly allocated.
- Due to the power of asymmetry between those who develop the technologies, and those who are subject to them, there is a need to empower users by promoting digital literacy skills and to enhance public awareness about the interference of emerging technologies with human rights.

Making norms work – Pursuing effective cybersecurity

Report: Andrijana Gavrilovic

- Norms need to be thought of and implemented in an interdisciplinary way. The engagement between disciplines should be brought into the discussion on norms on a meta level.
- Current norms have not been effective; more norms on state behaviour in cyberspace may be needed. Norms should not only remain voluntary, but also, non-binding.
- There is a need for more regulation on corporate behaviour.



- All stakeholders, the tech community in particular, should be involved in both the drafting and implementation of norms, though on different levels. The tech community should be brought to the table and be involved in the debate on norm building from the ground-up.
- Multistakeholder and multilateral mechanisms should not be put into an ideological contrast, but should be brought together.

Ethics by design – Moving from ethical principles to practical solutions

Report: Jana Misić

- The ethical guidelines ecosystem has grown extensively over the past years and includes more than 40 sets of guidelines. However, the challenge of creating a complementary balance between legislation, regulation, innovation, and the guidelines remains.
- The approach of self-regulation is not enough. There is a need for a new industry model that allows for working with data ethics, but does not pose a barrier for innovation and competitiveness. Data ethics should be a parameter on the market.
- While there are many common values in the guidelines, the base values that should be addressed are transparency and explainability. Mechanisms for providing transparency have to be layered, stakeholder-specific, and able to operate on different levels. Explainability should be defined in a multistakeholder dialogue because it includes explaining algorithms' decisions, as well as explaining what data ethics means in a specific context.



- Not all machine-learning systems operate with the same algorithms, have the same application, or are used by the same demographics. Developing tools for the practical implementation of data ethics has to be highly context-specific and targeted.
- Data ethics standardisation through certificates and seals for business entities should be explored as an instrument of ensuring trust. Other instruments include an obligation to report data ethics policies in the annual reviews and in the corporate social responsibility policies. Sharing best practice cases is crucial.

The European Copyright Reform – what just happened, what's next, and what does it mean for the Internet?

Report: Cedric Amon

- The debate surrounding the EU Copyright Directive is not over, despite its adoption, and many uncertainties remain. However, among others, the Directive has uncovered a very important debate on intermediary liability.



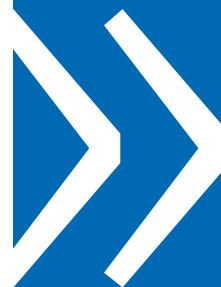
- It is up to the member states to mitigate some of the most critically viewed elements of the Directive (i.e. overblocking due to upload filters) by making use of the flexibility they have in implementing it. However, this will be challenging given that the member states have significant leeway in adapting the rules to their respective jurisdictions.
- The application of proportionality and the respect of exceptions to liability rules will play a crucial role in the successful implementation of the Directive.

Tackling online harms – a regulation minefield? Present and future.

Report: Cedric Amon



- Identifying the scope of online harms, as well as having a clear understanding of the terminology, are crucial in order to choose the right response. These include regulatory measures (e.g. legal frameworks based on self-/co-regulation) and the fostering of digital literacy.
- It is important not only to look at how to develop new laws, but rather, to consider existing regulations and human rights frameworks through which content and online harms can be evaluated and enforced.
- We must not overlook the less visible and more difficult-to-identify issues such as cyberbullying or the outsourcing of content filtering conducted by humans.



Workshops



Internet consolidation – opportunities and challenges

Report: Clement Perarnaud

- There is a growing consensus on the existence of patterns of Internet consolidation in the various sectors of the digital economy. The fact that a handful of platforms facilitate most online activities has societal consequences. Though they provide a myriad of opportunities, they also tend to mobilise US-based values and norms, and thus fail to adapt to individuals' specific needs globally.



- Competition rules need not only to be enforced, but also adapted to the challenges of the new digital environment. Rules need to be updated in order to better monitor platforms' market power and acquisition strategies. States should address the issue of the responsibility of these players, and ensure the same level playing field for all actors.
- Consolidation results from market trends, but it is also affected by the nature of the technologies. Centralisation of services creates new security threats and vulnerabilities. At the technical level, industry actors should increase the interoperability of their interfaces, encourage greater collaboration between small players, as well as ensure stronger security measures (end-to-end encryption and data minimisation).
- The concentration of market power needs to be better understood. The root causes of Internet consolidation, as well as ways to measure its scale, need further study. Such research could feed into policies supporting models of co-operative platform economy. However, regulatory responses must not interfere with the Internet's underlying principles.

GDPR Implementation – Blind spots, opportunities, and the way forward

Report: Ana Maria Correa

- The GDPR came to harmonise data protection in the EU and enforce privacy rights. Businesses recognise its importance in our current data driven economy, but there is still some legal uncertainty around it. A standard interpretation of the GDPR should be suitable for companies' activities. More guidance is also required from data protection authorities. Moreover, a potential blind spot of the GDPR is that it could be harming smaller companies that cannot afford to pay large fines relative to their annual revenue, in contrast to larger companies that can absorb the cost of non-compliance and have the resources to (potentially) provide a remedy.
- The GDPR involves multiple stakeholders and should take into consideration vulnerable groups, such as university and school students, patients, and refugees. Even if the GDPR represents a global standard on privacy, it is not enough to address the excessive collection of data. Citizens should be offered minimum training at schools, universities, and hospitals to understand the impact of the collection of personal data.
- In terms of impact, the GDPR makes people more aware of privacy rights. There is a major compliance effort with more than 500 000 data protection officers in Europe that aim to guarantee privacy. However, more transparency about its application and remedies is required. Codes of conduct could be a solution for clarifying the purposes and application of the regulation.
- Convention 108 is often seen as a bridge between the GDPR, the EU Police Directive, and the rest of the world mainly due to its data transfer regime, and the opportunity it offers to countries for meaningful co-operation within its conventional committee. The convergence towards a high set of privacy principles and rules to which Convention 108 seems to be a good basis needs to be speed-up in order to tackle collective challenges in the digital age.



Regulation and the Internet economy – how to create the right building blocks for 5G networks

Report: Marco Lotti

- 5G is the new standard for advanced digital communications and it promises to bring together fixed and mobile networks into one smart network. However, there are still some challenges when it comes to finding the right balance between innovation and regulation.
- The conflicting interests of the telecom and policy worlds still represent a big challenge. On the one hand, the industry is promoting innovation and a specific business model, and on the other, policy is trying to address the impact of a given technology in society. A fully comprehensive understanding of a technology's impact is difficult to reach. It is important to have more inclusive discussions among the different stakeholders (telecoms, manufacturers, regulators). Moreover, we also need more inclusive approaches in addressing the potential uses of 5G, its possible linkages with other technologies such as artificial intelligence, and its limitations in terms of security, the protection of data, and health concerns.
- There are regulatory challenges concerning the inclusion of the different stakeholders in the discussions (e.g. not only vendors but also the tech industry) as well as paying close attention to balancing the different issues that are on the regulators' table (e.g. competition, cybersecurity, data and consumer protection).
- It will be easier for the private sector to grasp and appreciate the potential of 5G technology as in the case of campus networks', for example. However, implementation challenges regarding infrastructure (such as the coexistence of private and public networks), capacity, auctions and spectrum allocations, as well as net neutrality concerns, remain to be fully addressed by the regulators.



implementation challenges regarding infrastructure (such as the coexistence of private and public networks), capacity, auctions and spectrum allocations, as well as net neutrality concerns, remain to be fully addressed by the regulators.

Children in the digital age – How to balance their right to freedom and their right to be protected?

Report: Andrijana Gavrilovic



- Policymakers and other stakeholders should give a greater voice to children and hear what they have to say about Internet governance at all levels. Policymakers must take the participation of children more seriously and enable them to take part.
- There is a need to understand what children are doing in order to engage with them about their online activities.
- Digital literacy is important for all age groups: children, teachers, and parents. It is necessary to understand the needs of children in order to conceptualise digital literacy in line with those needs, and in line with the complexity and the interests of the digital world. A balanced approach is needed to make children more resilient, but the industry and data controllers must be held accountable as well.
- We need to ensure Internet access to all children; it is not a given that all children have access to it already.
- We want SAPA (Smart Active Participation Algorithm) to be top priority discussion in a multistakeholder environment. The purpose of this algorithm is to replace some of the ads we are exposed to, while browsing on the Internet, with information about Council of Europe (CoE) initiatives. SAPA will suggest differentiated opportunities (by CoE) based on the age of the users, in order to empower the engagement of people of all ages towards CoE initiatives through the Internet. (*Message from YouthDIG*)

Transforming skills to meet innovation challenges

Report: Ana Maria Correa



- Our current digital-driven society requires new learning skills for building the necessary competence to meet technological innovation challenges. Policy-makers, businesses, and civil society should co-operate to create a sustainable working environment. Using the Netherlands as a case study, Dutch public authorities have recognised two challenges: (1) the need for new types of experts, and (2) that digitalisation has changed the entire labour market. The Netherlands fosters public-private partnerships to address digital literacy and have included the topic in primary and secondary education.
- Universities should consider implementing projects that can solve practical and emerging social issues, including cybersecurity challenges at both the local and international level. Capacity building should encompass private and public partnerships in order to tackle the cybersecurity workforce shortage. Under-supply and under-skilling in the labour market have to be addressed together, and not as separate problems.
- Public initiatives in Portugal have been created to enhance digital competences and address the challenges posed by technology to citizens' rights, employment, and knowledge. Action has been taken in terms of inclusion, education, qualification, specialisation, and research to improve digital literacy.
- Digital literacy can improve vulnerable people's lives. Cryptocurrencies, such as Bitcoin, could include refugees in the economic system. Digital identities could give refugees access to services that are denied by public authorities and traditional analogical systems. The challenge is that many refugees have no digital skills. Humanitarian groups, public authorities, and the private sector should invest on the digital training of vulnerable people to improve their lives.

DNS over HTTPS – What is it, and why should you care?

Report: Ilona Stadnik

- DoH protocol could affect the level of freedom that users have in choosing the way DNS will be resolved for them. It could provide more privacy by encrypting DNS queries; however, there are significant drawbacks such as the concentration of DNS traffic in the hands of a relatively small amount of remote DNS providers, as well as a possible predetermination of the list of DNS resolvers in apps.
- Another problem with DoH that leads to policy debates is how to ensure that local content is still under reasonable control. We should keep in mind that what works on the state level does not necessarily work for a particular user. We need to think about balanced policy with alternative options available: Who do we trust to resolve DNS issues for us and which jurisdiction should apply to DNS resolution?
- All stakeholders should participate in the discussion about DoH deployment and policies. The creation of a particular code of conduct for resolving services with standardised requirements for trustworthiness and data protection might be a good starting point.



Cybersecurity challenges ahead! How would you shape regulation to address changing technology?

Report: Stefania Grottola

- All stakeholders need to be represented at the table in their respective roles. Despite the fact that some issues have to be settled by a specific stakeholder group with expertise, conclusions can only be reached if all the stakeholders' perspectives are taken into account.
- Current technological challenges have created a global appetite for further regulation; nevertheless, flexibility is needed for understanding, on a case by case basis, whether further regulation is needed. Some of the challenges currently hampering the regulatory policymaking process are related to the false dichotomy that privacy and security are in contrast with each other. Security and privacy by design could be a solution.
- The current approach has promoted self-regulation. Debates on effective regulation need to consider and implement stronger enforcement mechanisms which existing institutions and tools tend to lack. In the absence of an independent judiciary for cyberspace, new mechanisms for dispute settlement should complement existing legal frameworks. Moreover, the implementation of best practices by like-minded countries can further strengthen the adoption of responsible behaviour to a larger number of actors.



- In order to address the challenges posed by emerging technologies, better transparency and accountability mechanisms are required. Digital literacy, security, and consumer awareness need to be better implemented for a more effective holistic approach.

Fending off trolls – Journalists in defence of democracy

Report: Marco Lotti



- Disinformation is a phenomenon that is evolving quickly, both in quantity and quality. Some solutions from institutions include a rapid alert system to timely flag disinformation and the implementation of voluntary codes of practice for online platforms.
- The interplay between populism and technology has witnessed the exacerbation of extremist and hateful online content. Closer co-operation between online platforms, fact-sharing networks, and independent researchers would help in gaining a comprehensive and analytical understanding of the (big) data behind the phenomenon of disinformation.
- The challenges posed by the spread of misinformation cannot be tackled by one actor alone but require a multistakeholder approach. Fact-checking activities should not rely solely on the users or media outlets, but should be the result of a collaborative effort between media outlets and online platforms.
- The current market model of the digital economy does not favour traditional media outlets which are facing important economic losses while the demand for and the spread of fake content remain high online. It is essential to stress the independence of the media as a benchmark for democracies, as well as fostering fact-based, quality, and ethical journalism. Solutions do not include a one-size-fits-all approach, but rather, locally-oriented responses.
- Despite the fact that misinformation is spreading and represents a challenge, it is not an immutable phenomenon. The importance of media literacy building programmes, the stress on transparency in collaboration among different actors – as well as on the content management decisions, are essential to the health of democracies.

Smart cities and governance

Report: Stefania Grottola

- Smart cities are not merely based on the technology involved, but also on the interaction between human beings and technology. Building on this interaction, two types of smart cities can be identified: prescriptive smart cities, doing mental harm to their citizens; and co-ordinating smart cities which stimulate people mentally by engaging them in addressing complex problems and human differences.
- Smart cities are human-centric organisations and systems featured by a variety of different stakeholders, ranging from users and individuals, to the public and private sectors. Due to the interconnectivity-based nature, debates on smart cities should adopt a multistakeholder, horizontal, and multi-layered (local, regional, national, and international) approach. They should also highlight the current dichotomy between smart cities, oriented towards funding and investment goals, and digital cities, redirecting the approach toward a citizen- and human-centric one.
- Smart cities represent enablers of the achievement of the sustainable development goals (SDGs). To facilitate the development of smart cities and address the related governance challenge, a multiplicity approach is required through a symbiotic combination of different stakeholders and technologies.
- Some of the smart cities governance challenges include data protection, privacy, and cybersecurity. As data collection represents an important resource for smart cities, awareness should be raised in a more effective way on the amount of information that individuals – knowingly and unknowingly – provide; on the distinction between personal, non-personal, and business data; and, on the concept of data sharing for good meant to foster the maximisation of societal



benefits of the technology involved. Additionally, trade secrets need to be taken into account and frameworks for mandatory data sharing by business entities should be further discussed.

Blockchain & Privacy

Report: Jana Misic

- The biggest threat to privacy is the huge collection of personal data that is controlled by single actors. By using blockchain technology, we can avoid the centralisation of data, therefore reducing the risks to privacy and respecting the right to be forgotten.



- In regards to our rights, freedoms, and responsibilities, the self-sovereign identity (SSI) is coming forward as the fundamental building block and a defining point of the future success of blockchain-enabled innovation. We should focus more on understanding the place of trust and 'trustworthiness' beyond one single actor.
- Greater focus should be put on advancing awareness and education about the complexity behind SSIs in particular, and blockchain technology in general.
- Education should be complemented by regulation in the long run. We should address the issue of the trade-off between user friendliness, simplicity, and privacy empowerment by the SSIs.
- Developing standards could help create a common language between the law and information technologies. This would reduce legal uncertainty around the use of personal data within blockchain-based systems.

Criminal justice in cyberspace – more of everything?

Report: Andrijana Gavrilovic



- Criminal justice instruments should provide for safeguards to ensure that the fundamental principles are respected, including principles of proportionality, necessity, legality.
- Increasing digital literacy in law enforcement, judiciary (prosecution and judges), and telecom operators is crucial.
- It is important that the Second Draft Protocol to the Budapest Convention on Cybercrime works for everyone, including non-EU countries, and conditions, safeguards, and notifications have to be present.

Play the villain – learn to fight disinformation with news literacy

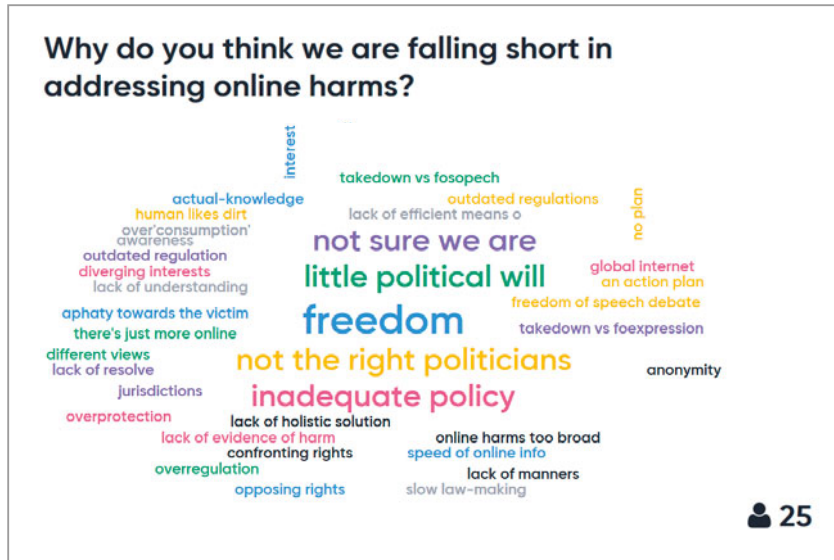
Report: Marco Lotti

- Media literacy and news literacy go hand-in-hand and are a solid solution to the disinformation crisis. To educate users – especially younger ones – effectively, the issue needs to be unpacked and correctly framed first. An important first step is to discontinue the use of the misleading expression ‘fake news’ and adopt ‘disinformation’ instead.



- Users are more likely to become critical towards misinformation if they see how such disinformation is constructed practically – by playing, for example, the Bad News Game (as the workshop audience did).
- Disinformation is usually characterised by impersonation, appeal to emotions, polarised framing, a conspiracy mindset towards institutions and/or the media, discreditation of institutions and/or individuals, and trolling behaviour.
- While building news literacy it is difficult to balance between critical thinking and destructive thinking, namely, to balance between awareness raising and a critical mindset towards misinformation on the one hand, and the danger of spreading mistrust or cynicism towards news per se on the other.

Audience poll (PL7)



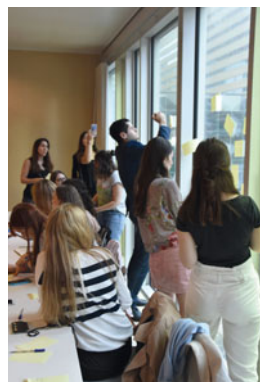
YOUthDIG Messages



YOUthDIG

– is the Youth Dialogue on Internet Governance to prepare young people for their participation at EuroDIG. The 3 days programme in The Hague from 16-18 June included inter alia the following elements:

- Human rights in the digital era
- Cybersecurity and how to balance human rights and security
- Access & literacy
- Remote participation training
- Visiting the Ministry of Justice and Security
- Meeting Subject Matter Experts
- Drafting Youth Messages
- Fun at a cooking school!



YOUthDIG Messages



Digital ethics & inclusion

- Internet Governance processes and policies about youth need to be better communicated, so that young people can be better informed and their participation strengthened through multistakeholder dialogue.
- Emerging concerns online, such as hate speech, fake news, privacy, and cyber bullying are not sufficiently discussed and taught at schools. We envision building a curriculum, that is enforced by regulation, focusing on raising awareness of the online environment and developing necessary digital skills and digital literacy of the youngest students.
- We want SAPA (Smart Active Participation Algorithm) to be top priority discussion in a multistakeholder environment. The purpose of this algorithm is to replace some of the ads we are exposed to while browsing on the Internet with information about CoE initiatives. SAPA will suggest differentiated opportunities by CoE based on the age of the users, in order to empower the engagement of people of all ages towards CoE initiatives through the Internet.
- Harmonisation of states' ethics codes on designing algorithms using digital co-operation including youth participation.
- We wish for the inclusion of teenagers through the Internet Governance youth ambassadors program in the decision making processes on local, regional and national level. Already existing youth parliaments should be strengthened to give the leaders of tomorrow a voice today.

Cybersecurity, trust & privacy

- To reclaim privacy of the many we want governments to have proactive involvement instead of reactive measures. In order to raise awareness on data protection and online user safety we call the governments to:
 - a. foster public discussion
 - b. mainstream digital literacy in basic public education
- Furthermore, we call on the private sector to make anonymity a viable option.
- Cybersecurity is a collective effort that requires a multistakeholder approach. We should achieve it with transparency while respecting our privacy. IoT is an important pillar in cybersecurity because it is in a continuous exponential development with growing capabilities and threats. We must raise awareness, enrich /and update education curriculum (to include) on IoT Security.
- Regulators should encourage technology to be open source to foster transparency.



Assembly of National and Regional Initiatives on Internet governance (NRIs)



NRI Assembly

It is a tradition that European National and Regional Internet Governance Initiatives (NRIs) are meeting at EuroDIG. Besides the opportunity to present the work of each NRI and the networking aspect this assembly also serve to identify tools and ways to increase the participation on a national level and to build a cooperation among NRIs in Europe.

Therefore, we focused on 2 main aspects – part 1: Getting citizens on board part 2: Start of an intersessional project.



NRIs across Europe

PART 1: Getting citizens on board

For this programme part we invited Missionspubliques an impact-driven consultancy (8 people) which works on improving governance by including ordinary citizens in the process of policymaking. Through this workshop, NRIs were able to learn from their methodology and discussed issues that are of concern for European citizens. Aim was to create synergies and find ways of cooperation between the NRIs and Missionpubliques.

PART 2: Start of an intersessional project on Digital Cooperation

There was a demand within the EuroDIG network to initiate a longer-term project that offers European stakeholders the possibility to contribute throughout the year. During the public planning meeting in January 2019 it was decided to formulate a European Response to the Report of the High-Level Panel on Digital Cooperation. This report was published shortly before EuroDIG and a consultation process to discuss the Panel's recommendations was initiated. All interested Europeans and people residing in Europe were invited to comment and the network of European NRIs is a significant source here. The intersessional project will result in a consolidated response by the European Community that will then be transmitted to the global IGF in November 2019 in Berlin.

Background: In July 2018, UN Secretary-General António Guterres established the High-Level Panel on Digital Cooperation. It consists of 22 international leaders from government, the private sector, academia, the technical community and civil society. Its goal is to identify good examples and propose modalities for working cooperatively across sectors, disciplines and borders to address challenges in the digital age. Between October 2018 and January 2019, the Panel conducted an open consultation process and collected inputs from all interested stakeholders worldwide.

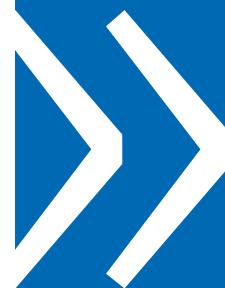


The IGF, EuroDIG and other inclusive multistakeholder dialogue platforms have laid important ground for the work of the Panel and play a key role in digital governance. Against this background, EuroDIG invited the European community to formulate a response to the Report of the High-Level Panel on Digital Cooperation.

List of topics from NRIs in Europe for 2019

Country/NRI	Topic	Topic	Topic	Topic
Albanian IGF	Internet Governance: promotion and awareness	Cybersecurity: Safer Internet in Albania	Infrastructures and technologies for digital innovation	Artificial Intelligence
Albanian YIGF	Cybersecurity and Cybercrime	Child Safety online	Hate speech online	E-skills & digital literacy
Denmark IGF	Data Ethics	Security in Society	Fake news & disinformation	Internet Infrastructure & Human Rights
Finnish IGF	EU Single Market Legislation in Terms of Internet Freedom	5G Technology & its Possibilities	AI, Algorithms, Platforms & Closed Networks – effects on trust and democracy	
France IGF	Cybersecurity & Resilience	Data Protection & Empowerment	Digital Humanities	Media & Content Regulation
Georgia IGF	Community network & Broadband Strategy	ccTLD and Georgian IDN market	Copyright & Intermediaries	Competition issues on Georgian Internet market
Italy IGF	Trust & Information Security	Digital inclusion & right of access	Privacy, rights & digital citizenship	
	Impact of emerging Technologies on Internet Governance	Youth education & inclusion on IG	Media & Content regulation	
Netherlands IGF	Internet Governance complexity	Innovation and ethics	Cybersecurity	Partnering trust
Portugal IGF	AI and Big data	Cybersecurity	IOT	Fake News
SEEDIG	Regional Digitalisation & Digital Policies	Data for innovation, economy & end-users	Network & Platform Neutrality	Cybersecurity
Spain IGF	AI	Blockchain	Innovation for human capital	E-Democracy & digital rights
Swiss IGF	Digital transformation process in the economy	Digital Democracy & Digital Identity	Media regulation	Cybersecurity
Turkey YIGF	Data-based Entrepreneurship & AI	Domain Name System	Youth in Internet Governance	Access to Information & Literacy
UK IGF	Online Safety	AI & Algorithms	GDPR & Data Exploitation	Cybersecurity & IoT

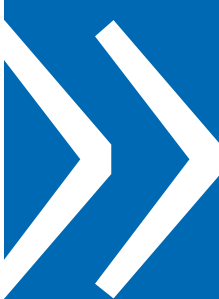
■ Access & literacy ■ Development of IG ecosystem ■ Human rights
■ Innovation and economic issues ■ Media & content ■ Security and crime
■ Technical & operational issues ■ Cross cutting / other issues



Participants say:
Great networking
opportunities





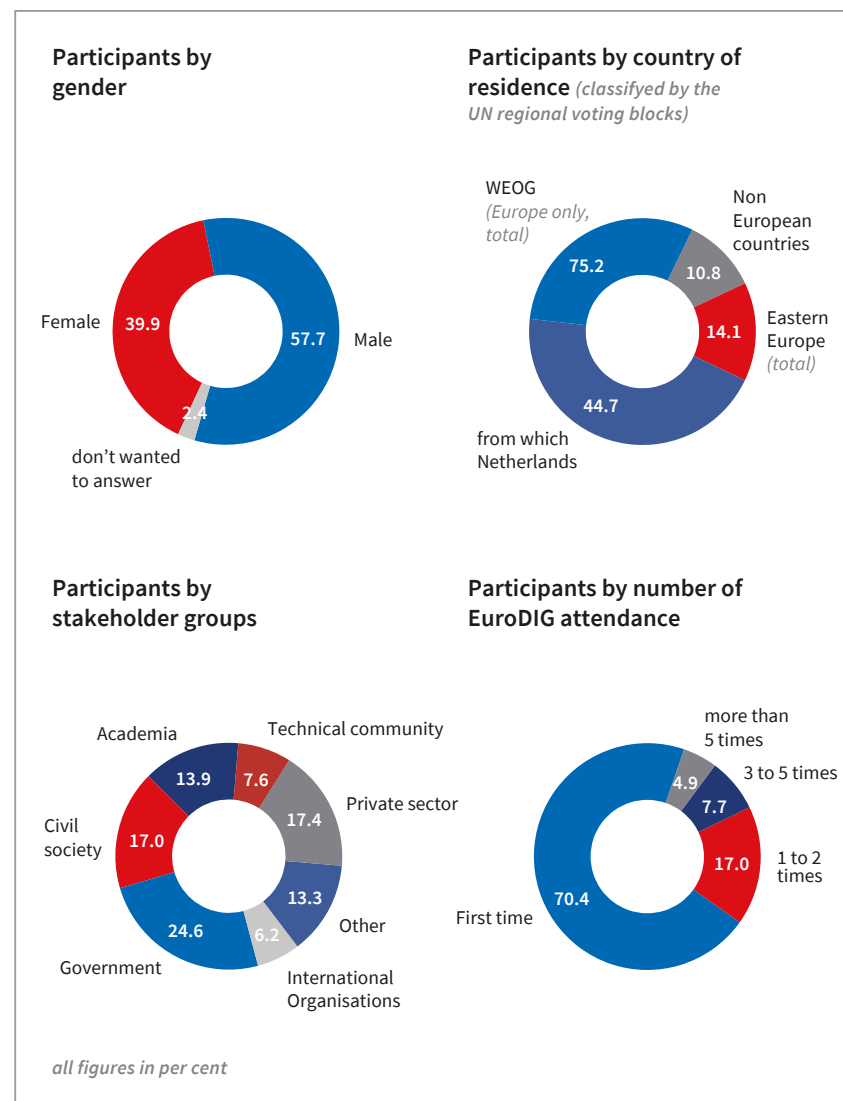


Facts and figures



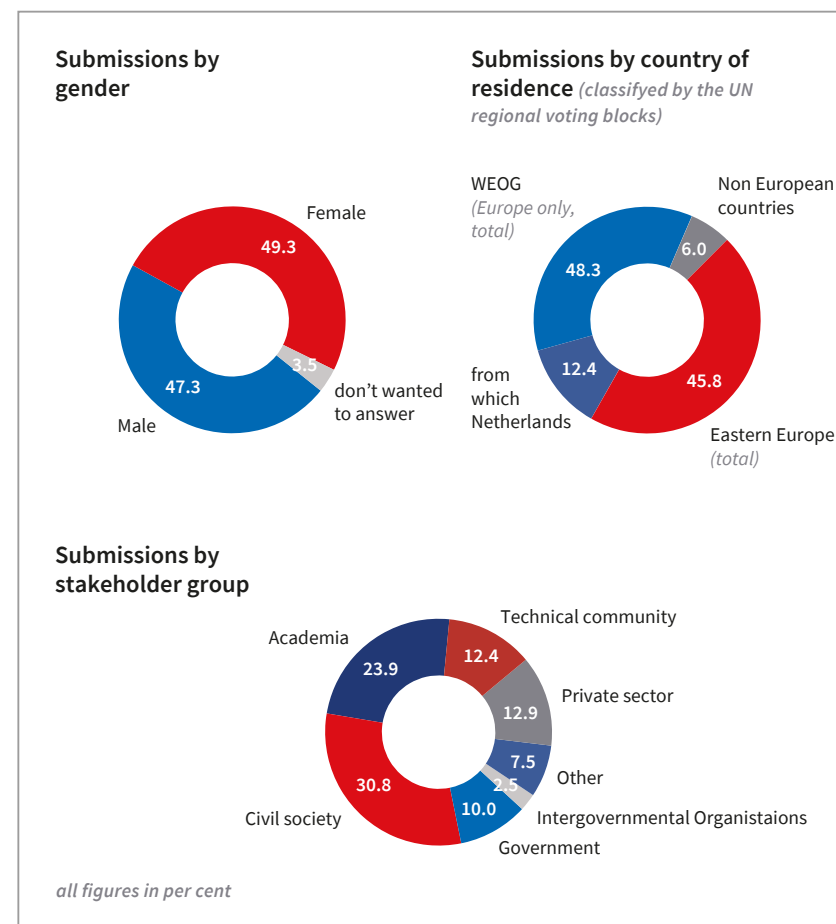
Break down of participation and submissions

We received 818 registrations (online and on the spot) and had about 600 participants picking up their badges. The following numbers are based on the total number of registrations.



During the joint call from 1 October – 30 November 2018 we received 201 submissions for the joint call for issues*, both for EuroDIG and SEEDIG – the South Eastern European Dialogue on Internet Governance (SEEDIG) in the following categories:

- Access & literacy (22)
- Development of IG ecosystem (20)
- Human rights & data protection (46)
- Innovation and economic issues (25)
- Media & content (27)
- Security and crime (31)
- Technical & operational issues (20)
- Other (10)



* The call for issues was one month shorter than in previous years and only 3 submissions per person were accepted.

See you on 10–12 June 2020 in Trieste, Italy!



The next EuroDIG will take place from 10 – 12 June 2020 in Trieste, Italy at The Abdus Salam International Centre for Theoretical Physics (ICTP).

Trieste will be the European City of Science (ESOF) in 2020 and EuroDIG will become a satellite event in the overall programme. More information at:

<https://www.sissa.it/news/trieste-will-be-european-city-science-2020>

Get an impression of the host city: <https://www.youtube.com/watch?v=HyMDIt6ua5U>

We are looking forward to welcome you there!



Stay informed and contact us!

 www.eurodig.org

 office@eurodig.org

 www.facebook.com/eurodig

 [@_eurodig](https://twitter.com/_eurodig)

 www.eurodig.org/about/newsletter

Imprint

Published by:

EuroDIG Association

Schächlistrasse 19, CH-8953 Dietikon

email: office@eurodig.org

web: www.eurodig.org

Graphic and production: monade · agentur für kommunikaton GmbH, Leipzig

Host 2019



Ministry of Economic Affairs
and Climate Policy
of the Netherlands

In cooperation with



Platform for the
Information Society



The Hague



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
Uffizii federal da communicaziun UFCOM



EBU



Geneva Internet Platform

Sponsors



SWITCH



Afilias

