Digital Outlook Europe

2019 – issue 01 , update 3

What and why?

The digital ecosystem is one in continuous flux. As the Internet continues to evolve and intersect with other digital technologies, new opportunities appear, existing challenges gain new dimensions, and new challenges arise all together.

The year 2018 saw considerable focus on issues such as cybersecurity, online misinformation, and data governance. Governments, intergovernmental organisations, industry, technical community, academia and civil society explored possible solutions, in an attempt to create a safer and more accessible Internet. While it is probably safe to say that their efforts will continue in 2019, one question also arises: What will be the main issues in 2019? What will all these actors discuss in the framework of events and processes such as the WSIS Forum, the Internet Governance Forum, the UN General Assembly meetings etc.?

In an attempt to anticipate the answer, this paper summarises the 2019 priorities of several European entities – partners and supporting organisations of EuroDIG and SEEDIG. As we prepare for our 2019 meetings, we intend to rely on this paper in our efforts to better anchor our annual debates in the European realities. And we will be looking carefully into whether and how our meetings could help advance the discussions around the identified priority topics.

Digital policy in 2019: Focus areas

Council of Europe

In 2019, the Council of Europe (CoE) will elaborate a follow-up to its Internet Governance (IG) Strategy 2016-2019, which will place IG issues into the broader CoE approach towards emerging technologies and digitisation.

The Council will continue its efforts aimed at addressing the impacts of artificial intelligence (AI) and emerging technologies on democracy, human rights and the rule of law. In the Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), work will be concluded on the draft study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework, as well as the draft Committee of Ministers recommendation on human rights impacts of algorithmic systems.

In its Committee of experts on quality journalism in the digital age (MSI-JOQ), the CoE will conclude work on a draft Committee of Ministers recommendation on promoting a favorable environment for quality journalism in the digital age and will present a study on media and information literacy in the digital environment. Further development of the Platform for the Protection of Journalism and Safety of Journalists will remain among the key priorities of the Council of Europe.

In the field of cybercrime, the Second Additional Protocol to the Convention on Cybercrime (ETS 185) is expected to be elaborated by the Budapest Convention Protocol Drafting Group, addressing issues of enhanced international cooperation on cybercrime and electronic evidence.

The Council will further strengthen its cooperation with Internet and telecommunications companies in order to promote an open and safe online environment where human rights, democracy, and the rule of law are respected. The list of bilateral projects developed under this framework includes among others the elaboration of a study on self-regulation and assessment of hate speech by Internet businesses in line with human rights. A follow-up to the 2017 Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content is also expected for 2019.

The CoE will also continue its work on current challenges of the communications environment and the impacts of misinformation and targeted disinformation campaigns on democratic processes, including elections.

European Telecommunications Network Operators Association (ETNO)

The Open Internet has come under increasing pressure due to fake news, disinformation, hate speech and terrorist-propaganda. Consequently, mechanisms for increased content monitoring and removal are on the political agenda, in Europe and elsewhere. As an association of European telecom companies, providing a range of services (Internet access providers, cloud service, media and content services), ETNO takes a broad outlook on IG. We recognise the need for enhanced cooperation between governments and all other stakeholders to address these threats and assume shared responsibility.

The Internet must remain an open, innovation-friendly environment built on security and trust. The key question for 2019 is how to assure this openness while effectively removing illegal content and malware. In the absence of an international institution capable of enforcing 'Internet rules' worldwide, the multistakeholder model faces a new challenge: How to distribute and share responsibilities without over-burdening or unduly empowering individual actors? It is very likely that the multistakeholder approach needs to be applied in combination with multilateral treaties that define policy standards – if not universally then at least at the regional level.

ETNO will continue to promote a multistakeholder approach, taking into consideration regional differences on digital policy.

RIPE Network Coordination Centre (RIPE NCC)

The RIPE NCC follows developments in Internet governance closely. The call from multiple governments for greater regulation of the Internet is an issue for all Internet stakeholders. When national policies and strategies start to impact the global nature of the Internet itself, it becomes relevant to us all. Our primary concern is the interests and needs of the RIPE community and our members. Our work ensures that all stakeholders, including governments and regulators, have the factual information to make informed policy decisions to foster a global Internet.
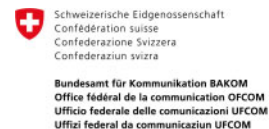
On more technical issues, the RIPE NCC is closely monitoring developments around the emerging IPv4 transfer market – with the limited stocks of IPv4 addresses available (and many networks still not using IPv6), many network operators are facing a shortage of IP addresses. While encouraging IPv6 deployment remains a priority for us, the IPv4 transfer market represents a new set of industry dynamics in the growth of the Internet. The shift from IPv4 addresses being freely available "as needed" to a scarce (and tradeable) commodity shows this.

Another key focus area for us is routing security, which has been the subject of growing attention. While technologies such as Resource Public Key Infrastructure (RPKI) and initiatives like Mutually Agreed Norms for Routing Security (MANRS) are important steps towards addressing some of the Internet's key vulnerabilities, it is vital that Internet governance discussions not lose touch with these practical, technical challenges to the Internet and Internet users.

Swiss Federal Office of Communications (OFCOM)

The Swiss Federal Office of Communications (OFCOM) deals – among other things – with issues relating to telecommunications, the media, the information society and Internet governance, and also represents Switzerland in the relevant international bodies.

In accordance with the Strategy 'Digital Switzerland' that was adopted by the Swiss government in September 2018, one priority for OFCOM in 2019 will be to actively support an open, constructive dialogue on the continuing development of global digital governance. In doing so, OFCOM will particularly support the work of the High Level Panel on Digital Cooperation that was established by UN Secretary General António Guterres in July 2018. The panel's aim is to identify gaps in the current global governance ecosystem of the digital world and make concrete recommendations on how cooperation can be improved for the benefit of all. The inclusive bottom-up dialogue in multistakeholder platforms such as IGF initiatives have laid important ground for the work of the panel. OFCOM will advocate for using synergies between these platforms and the High Level Panel on Digital Cooperation. Former President of the Swiss Confederation Doris Leuthard will continue to be an active member of this panel.

Another priority for OFCOM in 2019 will be to contribute to the development of basic conditions for the use of AI in such a way that algorithmic decision-making systems are transparent and verifiable, that responsibilities are regulated, and that the systems in use respect the prevailing values and legislation. The Swiss government has set up a working group within the federal administration for this purpose.

Furthermore, OFCOM will also be working with international partners to promote democracy, in which people themselves determine, how, by whom and for what purpose their data and their knowledge are used. As a result, human rights should not only to be promoted in the digital world; at the same time new innovative economic and social ecosystems and areas of activity should be created.

Finally, OFCOM will also contribute to further strengthening the potential of the international city of Geneva as global centre for digital governance.

European Regional At-Large Organisation (EURALO)

EURALO unites European Internet end-user voices within the At-Large community of the Internet Corporation for Assigned Names and Numbers (ICANN). The organisation is especially looking for increased input from the Eastern European region.

Some of the most important topics for 2019 are:

Compliance with the EU's General Data Protection Regulation (GDPR). A working group under ICANN's Generic Names Supporting Organization (GNSO) is in the Expedited Policy Development Process related to data protection and privacy matters of the Whois, with the aim to make it compliant with the GDPR.

Subsequent procedures. In preparation of the introduction of new generic top level domains (gTLDs), the lessons learned from the last round are being reviewed. The respective working group is halfway through their working cycle at the beginning of 2019. Based on their results, it will be decided how to undergo the next round of gTLDs. Their introduction is foreseen to happen in the timeframe 2019 to 2021. Input from end-users is solicited in order to introduce policies that serve them and their communities better.

Accountability and transparency. The Accountability and Transparency Review Team is working in its third round (ATRT3), starting from 1 January 2019 for the term of one year. It assesses ICANN's accountability following the IANA stewardship transition of 2016. The ATRT3 report will be subject to community input.

Internet Society (ISOC)

The Internet Society believes an open, globally-connected, secure, and trustworthy Internet for everyone produces a positive impact on the lives of people. Our enduring goal serves as the organising principle for not only what we do, but also how we work. In 2019[1], we will continue to focus on connecting the world, on improving the technical security foundations of the Internet, and on building trust in those core Internet functions. These interrelated areas encompass the most important issues of access and trust facing the Internet today and we must anticipate upcoming challenges and opportunities. We will continue to work to understand and thereby be prepared to shape the Internet's future.

Connecting the world. In 2019, we will shift our work from creating community networks to establishing enduring technical, policy, and regulatory frameworks that will help communities of the world connect themselves. The culmination of our efforts will be a global summit at the end of 2019, providing a roadmap to advance community networks and a foundation for a community-driven organisation of community networks to implement the roadmap. We will also continue to strengthen interconnection and peering ecosystems around the world through our continued support and development of Internet exchange points (IXPs)[2], collaboration with Facebook in Africa, training and skills development, in collaboration with other capacity-development organisations, and continued support to forums like the African Peering and Interconnection Forum (AfPIF) and the Indigenous Community Summit (ICS)[3], including ensuring their evolution towards becoming true community events.

Improving technical security. Shared connectivity and trust infrastructure enables a trustworthy and secure Internet for everyone. Technologies such as encryption infrastructure, time security, and identity and authentication functions comprise the necessary infrastructure. To that end, the Mutually Agreed Norms for Routing Security (MANRS)[4] campaign, successful in 2018, continues in 2019, with a goal of doubling the number of MANRS members by the end of the year. We will also engage the community in discussions on establishing a governance model that supports a sustainable MANRS community. Beyond MANRS, we will work within various communities to create the technical and policy building blocks that allow trust infrastructure to be developed, promoted, and implemented.

Building trust. The Internet Society's policy agenda on trust is guided by our Policy Framework for an Open and Trusted Internet[5]. In 2019, we will prioritise improving the security posture of producers of Internet of Things (IoT) devices. We will use the Online Trust Alliance's (OTA) trust framework[6] as a cornerstone of an expanded IoT-focused effort.

[1] https://www.internetsociety.org/action-plan/2019/
[2] https://www.internetsociety.org/issues/ixps/
[3] https://www.internetsociety.org/events/indigenous-connectivity-summit/2018/
[4] https://www.manrs.org/
[5] https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/
[6] https://www.internetsociety.org/iot/trust-framework/

Topics at National and Regional Initiatives on Internet governance (NRIs) in 2018

In 2005, when the UN World Summit on the Information Society decided to establish a "new forum for multi-stakeholder policy dialogue – called the Internet Governance Forum" – the IGF was seen as an experiment. Today the IGF process is a well-recognized key element in the global Internet Governance Ecosystem.

The growing number of National and Regional Initiatives (NRIs) that follow the same principles set out for the IGF shows that this format is relevant for stakeholders even more on the national and regional level. In Europe 27 initiatives have been formed and that marks the biggest concentration of NRIs worldwide.

With the next IGF in Berlin being the third in a row that takes place in Europe, the EuroDIG Secretariat is looking at ways to strengthen collaboration and mutual support among European NRIs. Therefore, we asked NRIs which topics where of relevance and have been discussed in 2018 in order to consider them for the 2019 agenda.

The table below summarises the results we received so far but since the questionnaire is still open, we expect more replies which will be published at: https://www.eurodig.org/index.php?id=78

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	
Italy IGF	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
Switzerland 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

EuroDIG and SEEDIG are regional Internet Governance Fora. Whilst EuroDIG is a pan European forum, SEEDIG was established to serve in particular the communities in South Eastern Europe and the neighbouring area.

DIG stands for 'Dialogue on Internet Governance', and is the unique selling point of the annual events that bring together Internet stakeholders 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.Participants come away with broader, more informed perspectives on these issues and new partners in responding to the challenges of the digital society.

More details at eurodig.org and seedig.net.