REPORT
BY SOUTH EASTERN EUROPEAN DIALOGUE ON INTERNET GOVERNANCE
ON SEEDIG 8 ANNUAL MEETING

The 8th Annual Meeting of the South Eastern European Dialogue on Internet Governance (SEEDIG 8) was held on 6-7 November 2023 at WESPA Business & Lounge in Zagreb, Croatia. Following two years of online meetings during the COVID-19 pandemic and a gap 2022 year due to Russia's full-scale military invasion of Ukraine, this was the first in-person meeting of SEEDIG community after 2019. On the sidelines of annual meeting preparation, the Executive Committee has registered SEEDIG as a legal entity, adopted new statute, and completed SEEDIG rebranding.

SEEDIG 8 was organized under the overarching theme "Digital Beyond Borders: Regional Synergy for Community Advancement". This theme was chosen with careful consideration of SEEDIG's core values and commitment to foster community expansion and strengthen partnerships across the region. It emphasized the idea that in our increasingly interconnected digital world, the boundaries that traditionally defined countries are transcended by opportunities for collaboration and growth. SEEDIG 8 recognized that cooperation across borders is essential for empowering local communities, and offered a space where stakeholders from South Eastern Europe could connect, exchange insights about in-country projects and initiatives, and explore opportunities for enhanced synergies.

SEEDIG 8 was co-hosted by Politiscope, a Split-based privacy watchdog organisation committed to safeguarding digital rights and democratic processes. Politiscope's primary goal is to ensure citizens' data protection by advocating for the comprehensive implementation of the GDPR to reshape the digital public sphere effectively.

SEEDIG 8 agenda was carefully curated to provide an engaging experience for all participants. It was designed around a mix of dynamic formats, each offering a unique perspective and interaction style. SEEDIG 8 agenda featured a diverse range of topics critical to the digital future. From keynote on internet fragmentation to panel discussions on open-source intelligence during the war, interplay between data protection and artificial intelligence, as well as the importance of content moderation and cooperation with big tech. During the interactive workshops participants got hands-on experience on how companies deal with governmental requests for content take-down and practical tips about improving organizational cyber resiliency. SEEDIG 8 also piloted the first regional launches of the Freedom on the Net and

IDN World 2023 reports. On 6 November, SEEDIG hosted a business dating networking event, where all participants had a chance to briefly present their projects and initiatives and find opportunities for synergies with stakeholders from across the SEE region.

In total, 2-days agenda featured 1 keynote speech, 4 panel discussions, 2 workshops, 6 lightning talks, and 1 open discussion.

Moreover, during SEEDIG 8 the Executive Committee presented new strategy and vision for the future of SEEDIG.

SEEDIG 8 was supported by six strategic partners, namely the Council of Europe, the Organization for Security and Co-operation in Europe (OSCE), Serbian National Internet Domain Registry Foundation (RNIDS), Serbia's Commissioner for the Protection of Equality, Freedom House, Internews,

SEEDIG 8 STATISTICS

2 days

74 onsite participants

272 followers of Day 1 live stream

126 followers of Day 2 live stream

22 countries, with most participants coming from Croatia and Serbia

Stakeholders:
18 civil society, 15 private sector, 15 technical community, 11 government, 8 academia, 4 media, 3 intergovernmental organizations

Gender:
37 women, 36 men, 1 preferred not to answer

11 youth participants

Previous engagement with SEEDIG:
54 first-timers, 20 attended SEEDIG meetings before

SEEDIG 8 WEBPAGE & AGENDA WITH SPEAKERS

https://seedig.net/seedig-8/

SEEDIG 8 RECORDING

Day 1: https://www.youtube.com/watch?v=IlXcLDdDChI

Day 2: https://www.youtube.com/watch?v=pgJbZ-__G_Q

SEEDIG 8 PHOTOS

Day 1: https://www.flickr.com/photos/140582891@N02/albums/72177720312689932/

Day 2: https://www.flickr.com/photos/140582891@N02/albums/72177720312707628

SEEDIG 8 MESSAGES

How to Stop Internet Fragmentation: Technical Perspective | Keynote Speech

- It's important to preserve the essence of the internet and working together to promote sustainable progress, as well as ensuring that everyone has access to this digital transformative realm.
- Internet is not immune from disturbances and censorship and is not free by nature, and the democratic governance means an obligation on states to enable unhindered access to an open, inclusive, and non-fragmented internet.
- Industry, civil society, academia, and digital gatekeepers should work together through multi-stakeholder efforts to promote an open and inclusive internet that is respectful of human rights.
- Governments and private sector should be responsible for protecting fundamental freedoms, personal data, and privacy of communication.
- While statistics about the internet's contribution to the economy and job creation are important, they are no longer standalone figures and must be factored into many cases.
- Technical coordination and bottom-up consensus-driven multistakeholder models should foster the evolution of internet technologies and innovation in the domain system to make it more responsive and inclusive.
- The digital sovereignty is an important national security concept, but states imposing digital sovereignty on the internet's identifiers would risk internet fragmentation or splinternet,

which would defeat the purpose of having a global internet. There must be a distinction between the technical and content layers of the internet. Any solutions to issues on the content layer should not involve changes to the technical layer.

- Interacting with local legislators and starting local chapters or initiatives is crucial for a more stable and secure internet globally.
- Global data must be available to scientists and computer models worldwide to equip them to address challenges of vaccines development, climate change, and sustainable development.
- There is a hope and optimism for the future of global collaboration, inspired by the internet and its role in connecting people and facilitating human endeavours.

The Interplay of GDPR and the EU AI Act | Panel Discussion

- The need for regulation on Artificial Intelligence (AI) systems, particularly considering their increasing use and potential risks to human rights, is widely acknowledged. AI systems already make decisions that affect employment, social benefits, and even prison outcomes, making it necessary to regulate them appropriately.
- The European Union has developed regulations for AI through the EU AI act, which has a risk-based approach. One notable case of regulation and violation of privacy laws was that of ChatGPT, which was banned in Italy due to violations of the GDPR.
- AI models represent a paradigm shift in innovation, but pose serious risks including data breaches, bias, and manipulation, and should be designed and deployed in a responsible and trustworthy manner based on principles of data protection, privacy, human control, transparency, and democratic values.
- The integration of ChatGPT and similar AI models into products and websites of other companies also raises questions regarding accountability and responsibility for demonstrating compliance with GDPR.
- There is a need to address cases of potential harm caused by generative AI, specifically chatbots, and ensure compliance with data protection legal frameworks such as GDPR.
- AI systems must exist and develop in a transparent regulatory framework with regard to collecting and processing personal data, that should be written in cooperation with developers, deployers, professional users, and non-users in the context of GDPR.

- As to the use of biometric surveillance in the European Union, data protection authorities need to monitor the processing of personal data in AI systems, even if they are not designated as supervisory authorities for the AI Act.
- With challenges faced by data protection authorities in terms of underfunding and a lack of resources, there must be a widespread learning and collaboration within the European data protection board.
- Overall, a centralized approach to data protection in AI systems should be taken, alongside the existing AI and GDPR roles, to provide legal certainty and clarity, strengthen data minimization and privacy by design and by default.

The War in Ukraine and OSINT – Impacts on Warfare, Technology, and Privacy | Panel Discussion

- The war in Ukraine has a visible impact on warfare technology and privacy, particularly for civil society organizations.
- It's important to identify Russian war criminals and hold individuals accountable for their actions in cooperation with other human rights organizations.
- A case of a Russian House of Science and Culture in Berlin turning to be a hotspot for Russian propaganda exemplifies the ability to use openly available information, social media and public archives to produce a report on Russian influence operations.
- Ethical and legal boundaries regarding the publication of personal data should be considered in cases of war. While the representatives of the aggressor state should be investigated and their names and faces should be published, there are grey areas where it may be difficult to provide a general opinion. Challenges arise also in reporting on Russian oligarchs who use shady sources to spread misinformation.
- OSINT organizations need to be prepared for legal battles and be ready to openly speak about the individuals who are working for the Russian government or intelligence.
- The truth behind war crimes must be shared and the responsible individuals need to be exposed, while also respecting privacy laws and ethical considerations.

Peeking Behind the Curtain: How GNI Companies Respond to Government Demands | Workshop

The workshop was arranged as an exercise to simulate government demands and responses, explore the compliance and non-compliance scenarios of telecommunication companies with data retention requests from the communication regulatory authority, and the legal implications of such decisions.

- The Global Network Initiative's goal is to provide a framework for responsible decision-making creating a safe space for civil society organizations and big tech companies to discuss their ideas and issues.
- The biannual assessment process helps hold big tech companies accountable in terms of how they respond to government demands for data in the evolving regulatory landscape.
- Members of GNI should follow the implementing guidelines for freedom of expression, privacy, and responsible decision-making.
- Responding to government demands is a complex issue with a need for a strategic and thoughtful approach in responding to such demands. The workshop demonstrated the importance of the GNI principles in guiding member companies in such cases, while non-member companies may not have this framework.
- It is important to analyse the situation carefully and avoid ‘upsetting’ the government too much; clarifying information about the request is more effective than blatantly denying them.
- Always, the principle of proportionality, the law, and respect for human rights should be considered when handling data collection and the shutdown of the internet.

Technical Implementations of Internationalised Domain Names and Linguistic Diversity Online | Lightning Talk

- Preserving cultural and linguistic diversity on the internet is one of the EURid’s objectives to make the digital space more inclusive, as the concept of universal acceptance and multilingualism online is considered a main pillar in the European values of a safe and open internet.
- The Internationalized Domain Name (IDN) initiative is important for raising awareness in the field of IDNs, arranging the first Universal Acceptance Day in March 2023 and forming of a Universal Acceptance Committee under ICANN ccNSO.

- IDN World Report is an online tool that provides updates on the state of IDNs. The report focuses on ccTLDs and provides insights into the adoption rates of the initiative among ccTLDs, including the popularity of various scripts and technical parameters.
- Survey that was conducted among Registries for ccTLDs to evaluate user awareness of IDN and the support provided by the Registries demonstrated that the awareness of IDN was rated at an average of 2.5/5 while the support provided by Registries was rated at 4/5.
- Another survey is planned to be sent out in January to update the website with new results and conduct case studies on IDN implementation, particularly in countries with indigenous languages.
- The Universal Acceptance Initiative is also a potential EURid partner in spreading awareness and providing training materials to Registries.

Should Media and Journalists Be Included on Critical Infrastructure List? | Lightning Talk

- Protecting journalists and media outlets as critical infrastructure implies the need for confidentiality, integrity, and availability of journalists and media even lacking the definition of "journalist" and "media".
- Even social media should be included in the discussions about digital security and critical infrastructure.
- Bosnia and Herzegovina experienced serious consequences due to a lack of a strategic approach to cybersecurity issues, highlighting the need for better protection for journalists and media in other countries in the region.
- While considering media as critical infrastructure, governments should not interfere with media freedoms, their financial support, what would lead to media losing their independence.
- The Balkan Media Assistance Program was started in 2017 and aimed to develop resilient media and infrastructure. Now, BMAP works with 16 key media partners in five countries covering 20 million people. Media partners include TV channels, radio stations, online news portals, and journalists. The goal is to spread lessons and best practices to the wider media communities in the Balkans. The BMAP is the central hub for sharing resources and information. Media partners are not imposed upon, and the program aims to address the challenges faced by media organizations of all sizes.

- Journalists and media are facing many challenges in the region, particularly in Serbia, where there has been proven surveillance of journalists and political elites. The government cannot protect journalists as a critical infrastructure if it is working against them.
- The concept of digital security should be expanded to include physical security. In practical terms, it may include providing additional funds for securing the homes of journalists.
- Governments should consider media as a critical infrastructure element. To that end, more has to be done to educate partners about the issues facing journalists and media and empower national and regional organizations to represent the media community in discussions with the government.
- More collaboration is needed with social media companies to help advocate for journalists and improve the status of news media owned sites, as well as to get control over sites lost by media or journalists, mostly due to the algorithms of Meta or Alphabet.
- Coordinate with different national or regional initiatives is necessary to influence government policies related to social media communication and the inclusion of media and journalists on the critical infrastructure list.

Hate Speech and Online Threats as Cybersecurity Issue | Lightning Talk

- All forms of activism lead to the same goal of creating a better society for everyone. We need to re-establish the human element at the heart of internet-related topics, particularly in the realm of cybersecurity.
- Using an intersectional approach to the issue of cybersecurity, we should prioritize the well-being of individuals who interact with the digital realm and are impacted by it.
- The impact of online hate speech and threats on the physical and emotional well-being of individuals, particularly those who identify as LGBTQ+ or women activists, go way beyond the online world. Online violence can lead to physical harm, emotional distress, and mental health issues, and can even result in fear and insecurity in everyday life.
- We need to recognize the systemic failure in fighting hate harassment and threats in the online sphere and realise that online hate speech and threats are not just words on the screen, but have real-life consequences, and therefore should be approached as a matter of cyber security.
- Online security also relates to protecting people (end-users) and their social interactions within the network, not just the hardware, software, and information systems.

- Cybersecurity policies should be more comprehensive and nuanced in their approach, taking into account the different ways cyber threats can impact people based on their gender and other intersectional factors, and helping to address systemic inequalities and discrimination in society.
- All stakeholders, including journalists and content producers, have a responsibility to consider the gender perspective of cybersecurity and its impact on end-users. Raising awareness, providing support to affected individuals, and promoting a culture of respect and tolerance are key to protecting end-users and their integrity.
- We must encourage everyone to reject hate speech and threats in all forms and work towards a collective effort to promote understanding and acceptance of others.

A Deep Dive into Internet Freedom: Lessons from Freedom on the Net 2023 | Panel Discussion

- Artificial intelligence (AI) has increased the scale, speed, and efficiency of digital repression. However, when designed and deployed safely and fairly AI can help bolster internet freedom rather than contribute it to its decline.
- The global internet freedom declined for the 13th consecutive year in 29 out of 70 countries assessed by Freedom House in their annual Freedom on the Net report.
- The lessons learned from the past decade of deliberations on internet policy should provide a roadmap for the next era.
- Digital activism has huge potential to drive real-world changes for internet freedom.
- Independent judiciaries serve as a bulwark for human rights online.
- Individuals infected by Pegasus spyware often feel uncomfortable to reveal that out of a fear that others will avoid speaking with them openly. Even with proper cyber hygiene, there is no guarantee that person will avoid being infected. Similarly, it is very difficult to track who is behind attack.
- Capacity-building and awareness raising campaigns, especially for vulnerable groups, is crucial to combat disinformation, which usually intensifies around elections and other significant political happenings in the countries.
- Ukraine, unlike any other country in the region, has suffered significant infrastructural damage due to ongoing war, which requires significant investment to restore the capacities.

Reaching Social Media Giants: Perspectives from the Social Media 4 Peace Project | Panel Discussion

- Before addressing specific issues, it’s crucial to understand the roles and processes within social media companies, including who covers what and how technology facilitates these processes.
- Rather than asking generic questions like the number of content moderators, it’s essential to formulate specific and effective questions that yield meaningful responses from AI algorithms and infrastructure.
- Recognize the diverse range of issues, from gender-based violence to intersectionality, and emphasize the need for collaboration among different organizations, including media, academics, and human rights advocates.
- Gain insights into the internal structures of social media companies to know which departments handle specific issues. This knowledge is vital for effective communication and issue resolution.
- Encourage social media companies to localize their policies, guidelines, and media literacy campaigns to better serve diverse linguistic and cultural contexts, addressing issues related to content moderation effectively.
- Promote the concept of multistakeholder digital coordinators to ensure a balanced and inclusive approach to addressing challenges posed by digital regulations, such as the Digital Services Act.
- Advocate for a unified voice and coordinated efforts among various actors, including civil society organizations, state authorities, and companies, to effectively implement and align with regulations like the Digital Services Act.
- To ensure the success of the principles, there is a need for concrete actions, clear guidelines, and a focus on capacity building for local organizations, promoting collaboration among donors and avoiding duplication of efforts.
- Cooperation among digital experts is essential, favouring collaboration over competition, especially at the local level.

Donor Principles for Human Rights in the Digital Age: Turning Principles into Action | Open Discussion

- The lack of coordination amongst government donors providing development funds leads to the risk of duplicating efforts and results in inefficient use of funds.

- There is a significant need to create sustainable long-term funding for projects and ensure matching between funder expectations and the reality of implementing the project.
- Smaller civil society organizations that do not have enough human and administrative resources to apply for funding and adhere to funder requirements are often passed up for funding support. To address these obstacles, it is recommended to build the capacity of local organizations to minimize resource competition and instead enable an environment where they feel secure to synergize on their specialties. Improved funding coordination and greater variety of grants is needed to enable direct access for smaller organizations.
- Freedom Online Coalition could explore opportunities for synergy with similar initiatives by the Organisation for Economic Co-operation and Development's (OECD), including the DAC Principles for Evaluation of Development Assistance, and the Principles for Effective Media Assistance currently being developed.
- Given that funds dedicated for technological development often go to private technology companies, it is recommended to create frameworks and guidelines for the implementation of the Donor Principles, which would be rooted in human rights and sustainability, and which would assist government donors in the region.
- Having an intermediate organisation that has a clear view of the rule of law, the CSO community, and what is happening on the local and regional level, may be a good approach to have the most impact when it comes to identifying recipients and identifying the needs for the implementation of projects. This would also help donors with diversifying funding recipients when allocating resources, and with considering the existing work that has already been done on relevant topics to avoid duplication of efforts and lack of synergy.

Training, Awareness, Resilience: Ecology and Digital Security | Workshop

- Combination of multiple activities through the digital security mentorship proves to be a successful tool to improve organizational digital security and synergise it with existing organizational workflow.
- SAFETAG, an information security assessment methodology adapted for civil society and media organizations, is recommended for digital security assessments of climate organizations.
- The digital security assessment should be a multi-step process, including questionnaire, risk assessment, training sessions, drafting organizational policies and procedures, and preparing a report with recommendations.

- A digital security report follows the audit and should provide a comprehensive overview of the organization's digital security practices, including vulnerabilities and identified risks, as well as a roadmap for necessary improvements.
- There should be expert organizations with a capacity to offer incident response help in the region.
- Cybersecurity regional cooperation is required to promote capacity building and knowledge sharing. Training programs, joint exercises, and the exchange of best practices can enhance the collective cybersecurity readiness of the entire region.

Cybersecurity Awareness – The Power of Synergy | Lightning Talk

- It is recommended to have a comprehensive approach to digital security, covering aspects such as understanding incidents, identifying possible risks, and assessing organization's digital infrastructure.
- Collaboration and joint efforts are crucial in achieving cybersecurity goals, bringing together individuals, organizations, and experts.
- It is advisable to utilize digital campaigns, such as video campaigns and articles, to raise awareness about various online threats and educate users about cybersecurity risks.
- Collaboration between different organizations is contributing to amplified expertise and knowledge in tackling cybersecurity challenges.
- The dynamic nature of cybersecurity requires continuous learning, adaptation, and cooperation to stay ahead of evolving threats.

AI Chatbots and Censorship in Authoritarian States | Lightning Talk

- Chatbots and image generators are already engaging in some kind of content moderation, similar to the one undertaken by social media platforms, by refusing to reveal personal data or to explain how to commit a crime. ChatGPT, for example, won't provide responses to answers that it deems as hate speech, and Bing Image Creator won't generate real people images. Similar limitations exist regarding terroristic content and violence.
- Results produced by chatbots fully depend on training data sets, and thus chatbots developed in authoritarian states (China's Ernie Bot, Russia's YandexGPT) usually offer very different definitions and concepts of democracy and freedom, as well as avoid responding to questions that are of political significance for the ruling regime.

- It is important to be on the lookout for the development of alternative chatbots in authoritarian states and to adopt regulation that requires transparency around the chatbots and AI image generators give users a better idea of the decisions they're making and any special interests they are taking into account that are leading to the removal of certain content.

Internet Landscape and Network Resiliency in Southeast Europe | Lightning Talk

- Internet in Ukraine proved to be highly resilient during the war due to its high level of decentralization and multiple ISPs operating in the country. Ukraine has 19 local Internet Exchange Points and almost all of them were active and provided interconnectivity for ISPs.
- Internet exchange points are important for mitigating traffic routing inefficiencies. SEE region has many efficient local internet exchange points, especially in Ljubljana, Zagreb, and Belgrade.
- The (former) state telecommunications operators still exert a lot of influence in the region. There are smaller numbers of independent providers than in some other parts of Europe.
- Routing within the region is generally efficient, although there are a few anomalies that likely reflect the various peering arrangements that different networks have in place.
- There is a modest amount of diversity in terms of the routes available to traffic flowing into the region, the dominant role played by incumbents.
- Consolidation of internet market and heavy reliance on a small number of larger providers can have a negative effect on innovation and market resilience.