



Supplementary Human Dimension Meeting

Safeguarding Civic Space in the Digital Age

Vienna, 11-12 May 2026

FINAL REPORT



Executive Summary

The second [Supplementary Human Dimension Meeting of 2026 \(SHDM II\)](#) took place in Vienna on 11 and 12 May 2026. It was jointly organized by the Swiss OSCE Chairpersonship, the OSCE Office for Democratic Institutions and Human Rights (ODIHR) and the OSCE Representative on Freedom of the Media (RFoM). The meeting examined how rapid technological advances are reshaping civic space and how these advances are affecting democratic processes, the rule of law and the enjoyment and promotion of human rights.

The event brought together 295 participants (168 women, 126 men, one undisclosed), including 136 representatives of OSCE participating States, seven representatives of international organizations, 139 representatives of civil society, as well as 20 participants from OSCE institutions and field missions, National Human Rights Institutions and others.

The first session focused on current digital threats posed to civic space, and emphasised the growing difficulties civil society organisations, activists, journalists and human rights defenders face when trying to carry out their work in this environment. The disproportionate impact on women and marginalised groups was noted as a particular concern.

The second session examined the implications of disinformation for human rights and democracy. Introducers discussed how disinformation and information manipulation can make participation in public debate unsafe or hostile, discourage engagement and contribute to the shrinking of civic space.

The third session focused on strengthening digital resilience for the protection of civic space. Introducers emphasized that digital resilience depends on concrete protective measures that help civil society actors, journalists and human rights defenders continue their work safely. Introducers also stressed the need for stronger collective responses and underlined the close link between digital and democratic resilience.

Opening Session

Opening remarks:

- *Ambassador Dagmar Schmidt Tartagli, Head of Human Rights, Democracy and Humanitarian Diplomacy, Federal Department of Foreign Affairs of Switzerland*
- *Maria Telalian, ODIHR Director*
- *Philippe Tremblay, Director, Office of the RFoM*
- *Anu Juvonen, Special Representative of the Chairpersonship on Civil Society*

Keynote address:

- *Gypsy Guillén Kaiser, Chief Global Affairs Officer, Committee to Protect Journalists*

The opening remarks affirmed that technological progress is reshaping the foundations of our shared security. From artificial intelligence to quantum technologies, new capabilities can strengthen resilience and prosperity – but they can also amplify risks and deepen divisions.

The discussion highlighted that artificial intelligence, social media platforms, big data and algorithmic decision-making have profoundly shaped democratic processes, the rule of law and the enjoyment and promotion of human rights in recent years. Digital tools were recognized as enabling new forms of investigative journalism, cross-border collaboration and civic participation.

At the same time, concerns were raised regarding the normalization of digital surveillance. Speakers noted that spyware, artificial intelligence, biometric technologies and large-scale data analytics are increasingly being deployed to monitor activists, journalists and human rights defenders. They underlined that such practices can be used for intimidation, deter individuals from engaging in public debate and create a chilling effect on civic engagement. Particular concern was expressed regarding the disproportionate impact on women and marginalized groups, whose withdrawal from public debate can weaken the inclusiveness and openness of democratic space. Alongside surveillance, coordinated information manipulation was identified as a tool to distort public debate and undermine trust.

Against this backdrop, opening speakers underlined the importance of protecting and strengthening democratic systems. The remarks emphasized that States must ensure that all individuals can safely exercise their rights and participate in public life, including in digital environments. This requires stronger safeguards, including stricter regulation of surveillance technologies, prohibitions on unlawful or indiscriminate mass surveillance, and robust judicial oversight of surveillance measures. Legal and policy frameworks governing new technologies must be aligned with international human rights standards. Civil society organisations, independent media and human rights defenders should also be supported through digital security training, resources to mitigate risks and mechanisms to respond to incidents.

Session 1: Digital Threats to Civic Space

Introducers:

- *David Elseroad, Head of Advocacy & Geneva Office, Human Rights House Foundation*
- *Alex Haché, researcher and independent expert on digital security, technology-facilitated gender-based violence and digital threats against civil society organisations*
- *Ronald Deibert, Founder and Director, Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto*

Moderator: *Andrew Gardner, Deputy Head, Human Rights Department, ODIHR*

In the first session, introducers noted that digital technologies are increasingly used to restrict civic space, intimidate dissent, and weaken democratic participation. They described a growing ecosystem of digital repression affecting human rights defenders and journalists across the OSCE region and beyond. Introducers expressed concern that these developments undermine the ability of civil society to organise, communicate, document human rights violations, and advocate effectively.

The rapid expansion of surveillance technologies and the normalisation of digital monitoring were raised as major concerns. New forms of monitoring include the exploitation of advertising data and weaknesses in telecommunications infrastructure, enabling a range of actors to track where people live, work, travel and communicate. Introducers highlighted that such surveillance can create a chilling effect, as fear of exposure may lead activists, journalists and organisations to self-censor, withdraw from international engagement and avoid documenting human rights violations.

Introducers also raised concerns about transnational repression. Digital surveillance can enable governments and affiliated actors to target critics, dissidents and diaspora communities beyond their borders. This can expose individuals in exile to continued intimidation and harassment, including through digital channels.

The discussion also addressed how technology companies can contribute to harmful digital environments. Certain algorithmic design choices and business models can incentivise the amplification of divisive or harmful content, including disinformation, misogyny, or polarising narratives. Introducers also noted that trust and safety teams have in some cases been reduced, while channels allowing civil society actors, journalists, public figures and other targeted individuals to escalate urgent threats have become less accessible.

Introducers further pointed to accountability gaps and weak oversight mechanisms. Regulation of spyware and surveillance technologies remains limited, while investigations into their use are rare. Victims are often unable to identify who is responsible for surveillance or to obtain effective clarification and redress. Public institutions frequently lack digital expertise and coordination, while survivors of online violence are often expected to bear the burden of proof. As a result, civil society organisations are regularly left to fill these gaps.

Session 2: Disinformation and Civic Space: Implications for Human Rights and Democracy

Introducers:

- *Rasto Kuzel, Executive Director, Memo 98*
- *Andriy Kulykov, Head, Ukraine's Commission on Journalistic Ethics*
- *Barbora Bukovská, Senior Director for Law and Policy, Article 19*

Moderator: Deniz Wagner, Adviser, RFoM

The discussion examined information manipulation as a challenge to democratic resilience across the OSCE region. Introducers highlighted that disinformation is not merely a communications issue, but a broader phenomenon that can undermine civic participation, weaken trust in institutions and intimidate critical voices. Disinformation was described as often appealing to identity, morality, gender or appearance in order to provoke emotional reactions and deepen divisions. Introducers underlined that one of its effects is to discourage participation in public debate, thereby contributing to the shrinking of civic space.

Recent conflicts and crises were cited as examples of the scale and consequences of disinformation campaigns. Russia's war against Ukraine was repeatedly referenced as an example of how disinformation and propaganda can be used alongside military tactics to shape public perception and distort people's understanding of facts in real time. Introducers also noted that disinformation often intensifies during election periods.

Introducers stressed that disinformation should be understood not only as a cause of societal division, but also as a symptom of wider crises of trust in institutions, media and public debate. A particular concern raised during the session was the impact on young people. As young people spend significant time online, they are especially exposed to misleading content that shapes their trust — or distrust — in democratic institutions. Digital, media and information literacy were therefore identified as essential democratic skills that should be strengthened.

The discussion also addressed the role of large technology platforms and artificial intelligence in the spread of disinformation. Introducers noted that certain business models and algorithmic design choices may incentivise the amplification of polarising or controversial content, as such content can generate high levels of engagement. At the same time, artificial intelligence tools are increasing both the speed and scale at which false or misleading content can be produced and disseminated. Combined with algorithms that personalise information, this development risks reducing pluralism and narrowing the range of perspectives citizens encounter online.

Introducers emphasised that efforts to counter disinformation must fully respect human rights and freedom of expression. Addressing disinformation requires long-term, rights-based and whole-of-society responses that strengthen trust, participation and resilience.

Session 3: Strengthening digital resilience for the protection of civic space

Introducers:

- *Rebecca Vincent, Director of Insights and Innovation, Thomson Reuters Foundation*
- *Maarja Kask, Policy Officer, Ministry of Foreign Affairs of Estonia; Member of the Freedom Online Coalition Steering Committee*
- *Andrew Smith, Head of Case and Policy Team, Meta Oversight Board*

Moderator: *Susan Kerr, Head, Human Rights Department, ODIHR*

Introducers emphasized that digital resilience is increasingly central to democratic resilience, as civic participation, independent media and civil society rely to varying degrees on digital systems and networks. Building resilience requires strong multilateral and multistakeholder cooperation among governments, civil society, journalists, researchers, and technology companies, particularly in response to cyberattacks, surveillance, disinformation, and transnational repression.

The discussion underlined that resilience is not only a matter of technical infrastructure, but also of trusted relationships, coordinated responses and sustainable support systems. Protecting civic space in the digital age requires rights-based policies that safeguard privacy, encryption and freedom of expression, support independent media, and help open societies withstand pressure without compromising democratic principles.

The audience heard about the practices of Meta's Oversight Board, and the measures that the Board is implementing to help safeguard civic space on privately owned platforms. It was noted that effective protection of civic space on digital platforms requires a rights-based approach that combines individual user redress with broader human rights due diligence.

Introducers highlighted cases involving journalists, artists, activists and human rights defenders, underlining that both over-enforcement and under-enforcement of platform rules can restrict civic space, amplify discrimination or enable threats and censorship. By examining individual cases in context, incorporating input from civil society and affected communities, and assessing how platform systems operate in practice, oversight and remedy mechanisms can help identify systemic risks and drive reforms that better protect freedom of expression and other fundamental rights.

The session also addressed what digital resilience means in high-risk and restrictive environments. In such contexts, digital resilience depends on concrete protective measures, including secure communication channels, trusted legal contacts, rapid response mechanisms and access to practical support. Introducers stressed that democracies need stronger collective responses, and that digital policies must be grounded in human rights.

It was further highlighted that OSCE participating States can contribute by addressing threats to information integrity, upholding their wider commitments to protect human rights and democracy, and providing concrete support to independent media and civil society organisations, including access to resources, training and legal assistance.

Recommendations

1. Embed human rights safeguards across digital governance policies and measures, ensuring that efforts to strengthen digital resilience fully respect international human rights standards.
2. Protect privacy, freedom of expression and access to information, and ensure that any measures restricting these rights are lawful, necessary and proportionate.
3. Include civil society structurally in digital governance processes.
4. Strengthen legal safeguards against unlawful surveillance and censorship, establish independent oversight mechanisms, and introduce stronger export controls and sanctions against abusive spyware industries.
5. Establish stronger mechanisms to monitor coordinated disinformation campaigns and strengthen meaningful civil society engagement.
6. Require technology platforms to strengthen transparency and accountability, allow greater public-interest scrutiny of algorithms and content moderation systems, address business models that incentivise the spread of disinformation, and empower users with greater control over the content they consume.
7. Increase media literacy by educating the public from an early age to identify and recognise disinformation.
8. Provide practical support to independent media, exiled outlets, and civil society organisations to help withstand cyber threats, disinformation, and other forms of pressure, including funding, training, digital security assistance, legal aid, and capacity-building.
9. Improve coordination between governments, civil society, international organisations, media, and technology companies, including through rapid-response mechanisms and information-sharing networks.
10. Protect civic space and support the participation of women, youth, journalists, and activists. Long-term strategies should focus on media literacy and address the underlying social conditions that allow disinformation to spread.
11. Provide long-term support for organisations protecting journalists, activists, and survivors of digital abuse.
12. Incorporate local knowledge and input from civil society, experts, and affected communities to better distinguish between legitimate expression and genuine harm.
13. Recognise internet shutdowns, spyware, surveillance, and information manipulation as threats to information integrity and address them through the OSCE's cross-dimensional security framework.
14. Ensure that cybercrime and cybersecurity measures include robust safeguards, judicial oversight, and protections for freedom of expression, and prevent the use of surveillance, spyware, and vague cyber laws to target journalists, lawyers, and civil society actors.
15. The OSCE should establish a formal mechanism to monitor and publicly report on reprisals against human rights defenders engaging with the OSCE.