Summary of

The 3rd E-Democracy / E-Governance Conference of the Eastern Partnership

‘Disinformation in the digital age - Effects on democracy, state and society’

University of Tartu

20 May 2022

Prof Dr Dr Robert Krimmer, Elis Vollmer, Salina Castle, Logan Carmichael, Art Alishani, Stefan Dedovic, Bogdan Romanov

Eastern Partnership eDemocracy Conference 20 May 2022

The 3rd Eastern Partnership e-governance/e-democracy conference took place in Tartu, Estonia on May 20th, 2022. The hybrid conference brought together 241 participants from 19 countries, out of which 61 participated in person and 180 participated online. The conference had simultaneous translation between English and Russian languages.

The conference opening words were given by Prof Dr Dr Robert Krimmer, conference chair, Prof Toomas Asser, rector of the University of Tartu, and Dr Thomas Buchsbaum, former special envoy of Eastern Partnership.

The keynote presentation was given by President Toomas Hendrik Ilves, former President of Estonia and Visiting Professor of University of Tartu and Distinguished Visiting Fellow at Hoover Institution, Stanford University. The keynote presentation was followed by three thematic sessions:

- **Challenges by disinformation in the digital age**, moderated by Rasto Kuzel, MEMO 98, and keynote presentation by Urska Umek, Department of Information Society, Council of Europe
- **Foreign factors in digital disinformation**, moderated by Marta Achler, International Law Expert, EUI PhD in New technologies and Human Rights, and keynote presentation by Armin Rabitsch, independent experts, University of Innsbruck, electionwatch.eu.
- **Opportunities and challenges of internet voting**, moderated by Dr Mihkel Solvak, Associate Professor at University of Tartu, and keynote presentation by Beata Martin-Rozumilowicz, independent expert, advisor at the European Commission.

In addition, the afternoon session was preceded by keynote presentation by Mr Guilherme Canela, Freedom of Expression and Safety of Journalists Section, UNESCO on How to counter disinformation/misinformation to protect democracies and human rights.

The closing of the conference was led by Prof Dr Dr Robert Krimmer and Dr Thomas Buchsbaum.

The recording of the conference (ENG) is available at https://www.uttv.ee/naita?id=33226
The recording of the conference (RUS) is available at https://www.uttv.ee/naita?id=33230

Within the first 30 days, the video recordings were watched more than 1048 times.

Photos and slides from the conference are available here: https://eceps.ut.ee/research/eap-conference

The Eastern Partnership eDemocracy Conference was organised by

Prof. Robert Krimmer, University of Tartu, Estonia

Dr. Thomas Buchsbaum, Ministry of Europe, Integration and Foreign Affairs, Austria

Ms Elis Vollmer, University of Tartu, Estonia

The Eastern Partnership eDemocracy Conference was supported by

European Commission, Eastern Partnership (EaP)

University of Tartu, Faculty of Social Sciences

European Commission, ECePS ERA Chair project (GA no 857622)

Acknowledgments

The conference was supported by European Union's Horizon 2020 research and innovation programme project ECePS ERA Chair (ERA Chair of e-Governance and Digital Public Services; grant agreement No 857622)

Table of Contents

Executive Summary

The 3rd Eastern Partnership e-governance/e-democracy conference "Disinformation in the digital age - Effects on democracy, state and society" took place in Tartu, Estonia on May 20th, 2022. The conference was organised by Johan Skytte Institute of Political Studies, University of Tartu, and supported by the European Commission. The hybrid conference brought together 241 participants from 19 countries, out of which 61 participated in person and 180 participated online.

The conference opening words were given by Prof Dr Dr Robert Krimmer, conference chair, Prof Toomas Asser, rector of the University of Tartu, and Dr Thomas Buchsbaum, former special envoy of Eastern Partnership.

The keynote presentation was given by President Toomas Hendrik Ilves, former President of Estonia and Visiting Professor of University of Tartu and Distinguished Visiting Fellow at Hoover Institution, Stanford University. In his speech he highlighted that disinformation has been around forever, but it has been aggravated and has become an issue where surveillance and disinformation are known phenomena in the past years. Governments started to use platforms and opportunities to spread (dis)information. The real problem is that people believe myths rather than truth and science.

The keynote presentation was followed by three thematic sessions:

1. **Challenges by disinformation in the digital age**, moderated by Rasto Kuzel, MEMO 98, and keynote presentation by Urska Umek, Department of Information Society, Council of Europe

   Key takeaways: The large processing of personal data for advertising with use of psychological profiling are really the big problem. To address this the digital literacy, transparency, guidelines for those providing information (eg media) online, having guidelines is very important. The truth is the first victim in the war. Displaced people remain in the (dis-)information sphere influence of their own country and the disinformation leads them in the wrong direction. Disinformation affects life and death situation when it comes to COVID virus.

2. **Foreign factors in digital disinformation**, moderated by Marta Achler, International Law Expert, EUI PhD in New technologies and Human Rights, and keynote presentation by Armin Rabitsch, independent experts, University of Innsbruck, electionwatch.eu.

   Key takeaways: Disinformation dissemination is travelling faster than truth. Especially in the case of coordination of inauthentic behaviour, amplification of disinformation, manipulation of search ranking, hacking and sharing damaged info, mutual admiration societies, microtargeting, impersonalisation, voter suppression, and deepfakes. And the problem when the richest man is controlling the social media.

   Businesses should not be run by their own self impacted regulations but rather be guided by non-governmental international organisation-based approach. Digital rights, tracing where the money comes for disinformation. It is very important that the journalists are educated and regularly trained on countering disinformation and not misunderstand that providing balanced news by providing misinformation is not appropriate. The role and capacity of regulators needs to be upgraded.

3. **Opportunities and challenges of internet voting**, moderated by Dr Mihkel Solvak, Associate Professor at University of Tartu, and keynote presentation by Beata Martin-Rozumilowicz, independent expert, advisor at the European Commission.

   Key takeaways: Capacity and CSO capacity needs to be updated, same for international guidelines, including cyber security issues. Needs-based approach information, the broad input from society. COVID has pushed the digitalisation, in information, campaigning, financing, and even in securing our health.

In addition, the afternoon was opened by presentation by Guilherme Canela, Freedom of Expression and Safety of Journalists Section, UNESCO on How to counter disinformation/misinformation to protect democracies and human rights. He explained how UNESCO is addressing the disinformation. Most important of all, he announced upcoming publishing of handbook ´Elections in Digital Times´, authored by Prof Krimmer and colleagues, which is a guide to electoral practitioners and will soon be published in several languages.

The closing of the conference was led by Prof Dr Dr Robert Krimmer and Dr Thomas Buchsbaum.

Keynotes

Armin Rabitsch, University of Innsbruck, electionwatch.eu

Beata Martin-Rozumilowicz, independent expert, advisor at the European Commission

Toomas Hendrik Ilves, former President of Estonia

Urška Umek, Department of Information Society, Council of Europe

Panel Speakers

1. Anna Romandash, journalist, Ukraine
2. Armen Grigoryan, Centre for Policy Studies, Armenia
3. Armen Smbatyan, Secretary of the Central Electoral Commission of Armenia
4. Daniel VODĂ, Head of the Public Diplomacy, Strategic Communication and Press Relations Division, Ministry of Foreign Affairs and European Integration, Moldova
5. Denys Verteletskyi, EU4Youth Alumni, Ukraine
6. Dmytro Khutkyy, Research Fellow in Digital Governance, JSIPS, ECePS ERA Chair, University of Tartu, Ukraine
7. Giorgi Iashvili, Georgian Information Security Association (GISA), Georgia
8. Marcin Walecki, former head of Democratization Department at the OSCE/ODIHR
9. Salome Tordia, Strategic Communications Division of the Administration of Government of Georgia, Georgia
10. Subhan Hasanli, Atlantic Council DFRL (Digital Forensic Research Lab), Open Platform initiative, Azerbaijan
11. Victor Guzun, International negotiations lecturer, former public servant and Ambassador of the Republic of Moldova to Estonia (2010-2015)
12. Zaur Akbar, Eastern Partnership Civil Society Forum member, Azerbaijan

Opening of the 3rd Eastern Partnership e-governance/e-democracy conference 2022

Speakers:

Prof Dr Dr Robert Krimmer, conference chair, University of Tartu

Rector Toomas Asser, University of Tartu

Mr Thomas Buchsbaum, former Special Envoy of Eastern Partnership

As part of opening the conference, Professor Robert Krimmer indicated that technology and democracy were the core ideas the conference was brought to life five years ago. Technology and democracy have been challenged by the onset of data driven democracy. We can now analyse in more ways the data collected by the governments, corporations and by expansion of social media, and this has led to perils of democracy. Dealing with these topics in developing democracies is a challenge and an opportunity. While the conference was postponed last fall due to COVID crisis, the topic of disinformation is even more relevant now, in spring 2022.

In his opening speech, rector Toomas Asser pointed out that conference is held fittingly in Estonia, the digital country excelling in e-governance, e-ID, e-elections, e-government. Estonia as a small country and young age enables agile development and rapid innovation, he said. We are all soldiers in global digital battleground and what happens there affects every aspect of life. Just only in March University of Tartu was under digital attack because of our decision to not support Russia. This conference is worthwhile step in raising awareness on digital literacy and democracy.

In the opening words by Dr Thomas Buchsbaum, one of the initiators of the conference series, he said that the COVID situation would not have been manageable by the administrations unless e-solutions were available or quickly introduced – e-signature, e-voting, e-health, e-justice, e-governance. It also brought to our attention the negative issues with digitalisation and rapid spread of disinformation – disinformation, information manipulation and fake news became global and can affect democratic governance and institutions and jeopardise political decision-making, even on war and peace. Why more people are not drawn toward independent media, he asked. The future and development of Eastern Partnership is at hand. Concluding, he stressed that the international relations are held in un-civil ways, we need civil and law-based international relations to be quickly restored.

Keynote presentation by Toomas Hendrik Ilves, former President of Estonia

Mr Toomas Hendrik Ilves, the former President of Estonia, gave a keynote presentation where he talked about the history of disinformation as a concept, technology, and liberal democracy. Here he provided an overview of the historical developments rooted in the 17th and 18th centuries that led western societies to develop modern science to the degree that we see it today and connected **the growth of science to the rise of the liberal democracy**. However, he pointed out that the fundamental values that liberal democracy has cultivated and grown into are largely under threat in the last 20 years, mainly due to the recent scientific and technological developments. **What is currently happening with disinformation has fundamentally changed how our society approaches the truth.**

He pointed out the **role of technological developments in enabling new forms and means of surveillance and provides a historical account of the recent events that shaped disinformation and surveillance**. He started by referring to the Moonlight Maze attacks, which is an investigation that took place in 1999 in the US and is also known as one of the first public cases of state hacking. He then pointed out the developments around smartphones, which are now pervasive technology with a remarkable impact on our society. Smartphones have enabled billions of people around the world to access the internet. President Ilves next referred to technological developments around digital platforms, especially Facebook, as a key technological development that changed how information is disseminated and what people read on the internet. The Arab Spring is an example where smartphones and digital platforms were actively used in an attempt to build democratic institutions. During that period, President Ilves highlighted the optimistic discussion on the role of technology and the dissemination of democratic values through digital platforms. However, this debate changed once governments started using the same technological developments as a channel to spread disinformation. This was evident on many occasions, especially in 2014, when Russia invaded Crimea. Since then, he pointed out that, there have been many efforts to use technological developments and different digital platforms to spread disinformation, while questioning science and scientific results. President Ilves further referred to the Dutch Referendum in 2013, the 2016 Presidential election in the US, and especially the anti-vax movement during the Covid-19 pandemic. This keynote concluded that **technological developments, which are a product of science, are leading to massive amounts of people not believing to science and scientific results**.

Keynote presentation "How to counter disinformation/misinformation to protect democracies and human rights", Guilherme Canela, Chief, Freedom of Expression and Safety of Journalists Section, UNESCO

Mr Canela stressed that disinformation is important in the context of every aspect that is relevant for the United Nations – democracy, human rights, sustainable development etc. There is no definite solution, but from the multilateral perspective it is important how we see this problem and how to tackle it in the coming months and years.

He reminded that in his speech more than 4 years ago, Barack Obama put forward the idea that the way **social media networks create the echo chambers, facilitates waves of disinformation/misinformation, but also conspiracy theories and hate speech**. This was and is one of the relevant tracks for our democracies. President Obama was right, and afterwards the situation has become even more complex and dangerous.

There are three aspects that Mr Canela emphasised:

1. **Using disinformation purposefully is an old phenomenon**. On the day we invented truth, we also invented lies. When this is not a new phenomenon, what could we do about it?
2. Word of caution – **we need to maintain an open mind to digital environment, since it also provides many opportunities (freedom of expression) in addition to risks**. We have to be careful not to throw the baby out with the bathwater. It is the biggest change after Gutenberg, but it is important to create resilience against the risks.
3. **Digital ecosystem is complex**, resembling a card house. Whatever we decide to do by law, regulatory system, enforcement, it risks the danger of pulling a card out of the house and disrupting the whole system. **In our response we have to know that this is a multi-layer eco system and we should not create more harm than good**.

There are new aspects related to the old phenomenon of disinformation – AI, algorithms – which are new in comparison with the age before the internet. But also, **the volume and velocity of information flows**. **The capacity of micro targeting is a game changer**. The logic of technological advances poses an extra complication – **disinformation strategies look very real and are difficult to ban**. E.g. the deep fakes are becoming easier to make, which plays an important role in the political context of democracies.

From the UNESCO perspective several things can be done:

1. The rights stipulated in the 1948 Universal Declaration of **Human Rights should be protected both offline and online**, but how can we do it in a changed world?
2. UNESCO promotes the idea on the conceptual framework of information being a public good. Citizens need to be empowered, **media and information literacy are absolutely crucial** to offer the tools to increase the resilience of citizens of all ages to the phenomenon of disinformation.
3. **The supply of accurate information is vital, as well as supporting free and pluralistic media, and scientists to be able to do their job properly.** Social media contents are a vital variable in this equation, it is a problem but also a part of the solution.
4. **Transparency is important**. Policy can only be based on information, and we need to know about misinformation in a structured way. In climate change, health policies, migration

etc. we can give more general recommendations, but here, with disinformation, we need to be much more specific.

I am happy to announce that there are some serious tools already on the way in the form of a handbook ´Elections in Digital Times´ by Prof Robert Krimmer and colleagues, which is a guide to electoral practitioners and will be published in many languages.

What can UNESCO do to mitigate the issues around disinformation?

The key challenge is how to move from a self-regulating *laissez-faire* to a regulatory environment. The latter is full of risks, since there are demands to regulate, but it also needs to correspond to the international human rights law. **We need data to create better policies**, since it is difficult to give recommendations without an evidence-based knowledge on the size and difficulty of the problem.

Panel 1: Challenges by Disinformation in the Digital Age

Keynote presentation: Urška Umek, Department of Information Society, Council of Europe

During this session, important global trends affecting election integrity were explored. This included the spread of disinformation and misinformation, the increase in threats and violence against journalists and media actors, and disruptions in electoral campaigning and communications. Misinformation and disinformation campaigns, the amplification and weaponization of hate speech, micro-targeting of voters, AI-driven campaigning and the use of automated messaging such as social bots and chatbots have been flagged as major challenges to electoral integrity and trust in democratic institutions. The onset of war in Europe and the COVID-19 pandemic has brought new challenges to the management of elections worldwide, has highlighted the importance of responsible media and of access to verified information, and increased support for fact-checking initiatives. It has also led to calls for social media platforms to take faster action in dealing with political disinformation and hate speech.

This session began with an introduction from Rasto Kuzel, outlining the shift toward the more sizable reach of modern technologies, vis-a-vis their predecessors, via platforms such as YouTube, among others, used to reach vast numbers of people. The biggest difference, he said, is **the ability of these platforms to amplify information** more than ever before, but also to disseminate disinformation.

Next, there was a keynote address from Urška Umek (Department of Information Society, Council of Europe), providing an overview of the disinformation landscape and the use of online campaigning utilising large amounts of data. She firstly emphasised Brexit as a key event for disinformation and its impact on democracies: it also signalled a major instance in online campaigning, going on to examine and coverage around elections (or in the Brexit case, among others, referenda) campaigns. While Umek said that o**nline campaigning can democratise this overall process, it also has a negative side**, which we see through **microtargeting, manipulation, and psychological profiling done with clear agendas.** Campaigning online uses opaque techniques (indeed, it is difficult or, often, impossible to know about the underlying algorithms), **capitalises on polarising issues to increase socio-cultural divides, generates mistrust, and can even undermine free and fair elections**.

However, Umek then offered a number of potential antidotes to the many downsides of online campaigning that she has described. First and foremost, she explains the **importance of media literacy** to critically evaluate the online campaigning we see before us. **Transparency** is crucial to ensure reliable online campaigning. If a voter is shown a political message or campaign online, they should be explicitly aware that it is such. Online platforms also have a responsibility, she said, to provide information about the algorithms that they are using, to keep archives of the campaigns held over their platforms, and to allow their users to opt out of their targeted campaigning. Finally, Umek added that **online campaigning must be coupled with free, fair, and accurate media reporting**.

Following Umek's keynote address was the first panel session. Firstly, Daniel Voda (Moldova – Ministry of Foreign Affairs and European Integration) outlined the disinformation challenges faced by Moldova, especially as Ukraine's neighbour, as realities have shifted since 24th February. With large numbers of Ukrainian refugees arriving in Moldova (450,000 have transited, 90,000 have stayed on Moldovan territory), reliable information for these refugees is crucial. Moldovan authorities deemed that a great deal of disinformation was coming through Telegram, so, Voda explained, the subsequent response was alternative Telegram **channels aimed at debunking**

disinformation, alongside artistic and civil society campaigns. All this, he said, showed that Moldova is a "small country with a big heart" to the international community.

Between panellists, moderator Kuzel pointed out that **in war, the truth is always the first victim**. Next, panellist Zaur Akbar (Azerbaijan – Eastern Partnership Civil Society Forum Steering Committee) spoke of **disinformation being a "blight" on democratic systems**. He cited examples from post-Soviet countries: firstly, Pegasus Spyware and its use to surveil media and commentators by governments, and secondly, Russian weaponisation of ethnic communities to stir dissent and tension in another country.

The third panellist, Denys Verteletskyi (Ukraine – Ukrainian National Youth Council) spoke about the war in Ukraine, outlining the immense difficulties faced by Ukrainians inside the country, but also for those trying to remain involved from outside the country. He emphasised the **importance of sharing information about what is happening in Ukraine**, and encouraged Europeans to use the Ukrainian language as a show of solidarity.

Armen Grigoryan (Armenia – Centre for Policy Studies), the final panellist, spoke about difficulties surrounding the media and disinformation. He noted that a **lot of media outlets are lacking contact information, so it is difficult to attribute information or to contact them**, which is problematic in the post-Soviet space, where many **media outlets are funded by oligarchs or corrupt politicians**. He also noted that disinformation about Ukraine long pre-dated the Russian invasion in February 2022, citing an example from the 2020 Nagorno-Karabakh War of disinformation about Ukraine supplying weapons to belligerents in that conflict.

The moderator, Kuzel, closed the panel by summarising some of the impacts of disinformation. He explained that disinformation can have varying degrees of impact: for example, in an election, if you make a decision based on incorrect information, you must deal with the political impact. However, with something like a vaccine, if you make a decision based on disinformation, it can have an impact on your health and your life.

Panel 2: Foreign factors in digital disinformation

Keynote presentation: Armin Rabitsch, University of Innsbruck, electionwatch.eu

Information manipulation has become a global phenomenon and even more so in war situations, serving as a prominent instrument in the strategic foreign policy toolkit of many governments around the world. Foreign influence operations are by no means a new phenomenon. However, the global retreat of democracy, decline of political parties, the presence of financial scandals and recent technological developments have made it easier for authoritarian countries to quickly and maliciously interfere with democratic institutions and processes. Disinformation exploits existing divisions and leads to further polarisation. Understanding the reasons behind disinformation campaigns helps us to stop them. In this session we discussed mitigation measures and how disinformation in different forms of media, including social platforms, can be monitored and countered.

Marta Achler the moderator of this panel addressed the importance of the disinformation in the current times. In addition, she pointed out that the in the current case of war the sources of misinformation present are also a source of trouble.

In line with Marta Achler, the keynote speaker Armin Rabitsch addressed the **role of the social media platforms and networks, upcoming framework on disinformation and regulation**. Mr Rabitsch presented that the research that shows that disinformation spread faster than truth. The techniques for disinformation that are used by various sources from Russia, MyanMar, Iran and USA. These **techniques include coordinated inauthentic behaviour (troll farms…), amplification of disinformation, manipulation of search rankings, hacking and sharing damaging information, mutual admiration societies, micro targeting, impersonation, voter suppression and deep fakes.** He also pointed out in the case of Austrian elections that the main disinformation came from abroad and foreign factors.

Mr Rabitsch mentioned upcoming Digital Service Act of the EU and pointed out that there is still lack of access of researchers to information and algorithms. In line with these challenges, **recommendations to overcome disinformation and unethical behaviour of the AI and mass media** are following:

1) Private sector should be responsible to respect human rights as per UN guiding principles;
2) common standards for accessible and transparent content moderation;
3) need of independent third-party oversight;
4) enlargement with EU institutions to shape upcoming regulations, advocate for human rights-based approach in addressing disinformation, learn how to better co-op with disinformation through education.

After the keynote presentation, the moderator introduced the panellists. The discussion started by presenting interesting fact by Mr Walecki, a visiting fellow at St Antony Oxford College, who pointed out that **funding is a key issue that should be discussed**. The issue of funding raises the question whether the receivers of foreign money should be considered as disseminators of disinformation, bearing in mind that Russia and China spent millions of dollars to disseminate disinformation in foreign countries. The current state of disseminating disinformation includes new techniques, he addressed, and that also the political financing regulations are quite old.

Similar to Mr Walecki, Ms Romandash, journalist from Ukraine, addressed that the disinformation campaigns are different and depended on the local context. That is why it is quite **important to compare the local contexts in order to address disinformation campaigns**. Ana also addressed the **new approach of authoritarian regimes towards fake balance of the opinions**, in which the different opinions are presented to public, which leads to confusion.

Likewise, Mr Hasanli, from Digital Forensic Research Lab in Azerbaijan, said that nowadays it is quite **hard for citizens to realize what is the right truth**. To achieve that, Suhani mentioned that there should be **strong collaborations among the CSOs and the government**. In addition to the collaboration, the education from young age is crucial to develop critical society.

Finally, panellists addressed the **importance of transparency and accountability mechanisms**. The **importance of regulating the disinformation is crucial, however very challenging endeavour for regulators**, panellists concluded.

Panel 3: Challenges and opportunities of Internet voting

Keynote presentation: Beata Martin-Rozumilowicz, independent expert, advisor at the European Commission

The negative effects of disinformation are felt in all aspects of the electoral process, from online political discussions to campaign strategy. War, internally displaced persons (IDP), refugees and COVID-19 pandemic – the ability to govern during crisis situations has strongly highlighted the need for digital governance, including internet voting. The need to be able to make decisions from a distance in a transparent and secure way has been rapidly accelerated. Furthermore, various convenience voting methods (such as advance voting and postal voting) have become topics of intense debate. The trials and pilots of this voting method that have been and are currently conducted in various countries focus on how to ensure election integrity with technological applications in a potentially hostile cyber environment while offering the most user convenience and low participation barriers to ensure uptake and usage. Therefore, it is crucial to combat disinformation and develop trustworthy internet voting technology and ensure trust among a heterogeneous voting population. This session discussed the increased use of remote voting methods and interest in internet voting as the ultimate form of remote and convenience voting.

Trust in technology should be cultivated and developed with further deployment of the technology in question. However, there might be a paradox, which was addressed by Mihkel Solvak (University of Tartu) in his online voting (i-voting) in Estonia illustration – **people do trust the electoral technology of online voting, but the same people do not trust the EMB representatives, who do the vote tallying**. These aspects should be somehow mitigated.

The same idea was continued by keynote presenter Beata Martin-Rozumilowicz (advisor at the European Commission). In the speech she provided an overview of advantages of i-voting (e.g., lower cost, higher turnout, involvement of young people in democratic processes, etc.). Also, there are **international standards in regard to i-voting**, which make it so popular: **absence of connection between voter and a vote, no coercion due to the vote re-casting, accountability and transparency** despite relatively complicated technical nature.

Keynote speaker also referred to Estonia as a case, where share of i-voters has been steadily growing but has not increased the number of participants overall. Can this situation be explained by the absence of trust or computer literacy, this is still to be found out, she said. One way to understand peculiarities of i-voting is to test it in different environments, and this is a modern trend since new countries involved with i-voting and pilots such as New South Wales, Australia; Swiss Post e-voting system; Utah, West Virginia, Denver in the US, parts of Canada.

Nevertheless, i-voting might be perceived as a 'silver bullet', as it was demonstrated by the success story of Estonia, it still has its flaws: **malware**, especially from personal laptops, **state-sponsored interference into elections**, although there has been a slight easing of this threat in recent years, and **dynamic nature of trust**. The latter is perfectly captured by the quote from Stephane Nappo: "*it takes 20 years to build a reputation and few minutes of cyber-incident to ruin it*". With the citation, Beata Martin-Rozumilowicz emphasised once again the necessity to be able to **protect population from the dis- and misinformation damaging impact**, because one could

invest all resources in the technology, but the effort could be undermined by couple of posts on Facebook.

After keynote presentation representative of Eastern Partnership member-states shared their perspectives on the development of i-voting in their countries.

The first speaker Victor Guzun (Moldova) raised extremely salient issue, which became even more relevant in the light of Russian-Ukraine war – in Moldova, EMB or agency responsible for compiling a list of eligible voters, does not know how many people are outside of their country, despite having 46 external polling stations at diplomatic missions. In Guzun's opinion, smart ID and i-voting can mitigate this issue to some extent. The former has recently been approved, while the latter might be implemented around year 2024 or 2025.

Then the floor was passed to Armen Smbatyan (Armenia – Central Electoral Commission of Armenia) who opened his speech by listing milestones in Armenian i-voting evolution – i-voting was enabled in parliamentary elections in 2012, 2017, 2018, 2021; presidential elections in 2013, but only for particular cohorts of people. Also, he mentioned that Estonia was and still is a great role model in a sense of gradual i-voting deployment. Finally, Smbatyan indicated that Armenian **i-voting does nourish vote secrecy and security, transparency, and trust principles**.

Third speaker, Dmytro Khutkyy (Ukraine – University of Tartu), began by explaining that Ukraine has already used i-voting for 6 years for several development projects and on Open Government Partnership projects. I-voting was used in places like Lviv, where participation was up to 14%, which is a great starting point. Additionally, Khutkyy added that **Ukraine has roots for representative, participatory, and direct digital democracy**, the country just needs more time for them to flourish, especially since **people feel more empowered because they can influence policy and politics**.

The last panellist, Giorgi Iashvili (Georgia – Georgian Information Security Association), concluded the discussion by outlining **cybersecurity concerns, surrounding both electronic and online voting**. Both technologies should revolve around cybersecurity triad: **confidentiality, availability, integrity**. Moreover, Mr Iashvili pinpointed almost unique cybersecurity features for online voting, like, securing devices, securing data in transit as the ballot travels, security of internet connection and long-term storage of data vs. short term storage. Taking all these nuances into account, Iashvili appeals to audience and insist that states should look at doing i-voting over 10 or 15 years to take the time to adequately secure the process and mitigate risks, rather than implementing i-voting in a rush.

EaP Country Experiences

This section represents a summary of personal views and comments made by the participants during the discussions. It does not represent an official statement or assessment of the readiness or status of eDemocracy in the EaP countries.

Armenia

Armenia highlights the spread of disinformation at the beginning of the pandemic. Information was increasingly shared aiming to answer questions on the origin of the virus and whether it had been created artificially. Tracking down false information is a key challenge as media sources often miss contact information, making it difficult to trace who is behind. Moreover, many media outlets are owned by oligarch or corrupt politicians who may support a media narrative that goes along with their interests. In regards to i-voting, Armenia draws its eyes on Estonia as a best practice example. Five critical principals Armenia follows are: vote secrecy, transparency (software is open source), vote security (protection from hacking), opportunity to analogue vote, trust.

Azerbaijan

The closure of the RFE/RL (Radio Free Europe/Radio Liberty) in 2014 and further bans on TV channels as well as websites marked a major setback for the democratic system of Azerbaijan. As encountered in other post-Soviet countries, governments make use of spyware to surveil media and commentators, restricting free media. Russia is suspected of fuelling dissent and tension within the country by spreading misinformation about ethnic communities. This was observed in Georgia, where Russia aimed to destabilize the society and influence politics. Furthermore, the aspect of misinterpretation from western journalists was raised, resulting in media disinformation.

Georgia

Georgia has been the subject of external misinformation strategies and threats from Russia, aimed at destabilising the Georgian society. In doing so, Russia attempted to influence Georgian politics in its own interest. In regards to internet voting, cybersecurity concerns are highlighted such as securing devices, securing data in transit, and securing the internet connection. Time should be taken to adequately secure the process and mitigate risks. In order to better secure i-voting procedures, international election and i-voting standards should be merged with cybersecurity standards.

Moldova

The invasion of Ukraine and surrounding concerns (including movement of refugees) has shifted the conversation around disinformation and elections significantly. Moldova, as recipient country of Ukrainian refugees, is involved with collaborative project to provide reliable information to refugees. This is a response to the increased amount of disinformation generated on social media networks since the start of the war. Telegram channels were observed as a predominant source

of disinformation. In order to debunk disinformation, the Telegram channel (Prima Sursa "First Source") was created, and quickly grew to 75,000 subscribers. Western media framed Moldova as Russia's next target; thus, Moldova created a narrative in response to this. Regarding i-voting, Moldova is working on enabling i-voting systems, but it is still unclear when this will be achieved. The smart-ID has recently been approved which marks an important step towards realizing i-voting. However, a key issue remains that Moldova does not know how many citizens live outside of their country, even with 46 external polling stations at diplomatic missions.

Ukraine

Russia's invasion of Ukraine and surrounding concerns are central to the conversation around disinformation. With the start of the war, it increasingly became difficult to access reliable information inside but also outside of the country. Ukraine empathizes the importance of sharing trusted sources in order to further raise attention about the situation, and to combat misinformation coming from Russian media outlets. Russia has a history of spreading disinformation in Ukraine, such as in 2014 when Russia invaded Crimea and aimed to convey a media narrative supporting their actions. Compared to the past, there has been a significant shift in amplifying information but also disinformation on a large scale through platforms like YouTube, reaching millions of people with a single video. The usage of i-voting for the past six years for several elections, such as in Lviv (participation of up to 14%), reflects Ukraine's participatory and digital democracy. This digital enthusiasm is expected to help rebuilding process beyond the war leading to a breakthrough in their digital transformation.

Conclusion

The key ideas presented at the conference:

- President Ilves stressed that disinformation has been around forever, but it has been aggravated and has become an issue where surveillance and disinformation are known phenomena in the past years. Governments started to use platforms and opportunities to spread (dis)information. **The real problem is that people believe myths rather than truth and science**.
- With Youtube and other Social Media platforms the ability amplify dis/misinformation has changed. Urska Umek: BREXIT was turning point where the political decision was largely influenced from abroad, the methods were not new but the scale has changed. The large processing of personal data for advertising with use of psychological profiling are really the big problem. To address this the digital literacy, transparency, guidelines for those providing information (eg media) online, having guidelines is very important.
- Mr Voda from Moldova highlighted that Ukraine is suffering from disinformation in the war. Mr Kuzel pointed out that **truth is the first victim in the war**. Displaced people remain in the (dis-)information sphere influence of their own country and the disinformation leads them in the wrong direction.
- Disinformation affects life and death situation when it comes to COVID virus.
- The handbook on AI, social media, internet, and elections will be published soon by UNESCO.
- Foreign influence – there is a need for kill switch for shutting down internet.
- Armin Rabitsch stressed that disinformation dissemination is travelling faster than truth. Especially in the case of coordination inauthentic behaviour, amplification of disinformation, manipulation of search ranking, hacking and sharing damaged info, mutual admiration societies, microtargeting, impersonalisation, voter suppression, and deepfakes, which are key issues. And the problem when the richest man is controlling the social media.
- These issues are present all around the world, not just EAP countries. Digital Service Act will not solve all issues. Businesses should not be run by their own self impacted regulations but rather be guided by non-governmental international organisation-based approach. Digital rights, tracing where the money comes for disinformation. Where intelligence agencies are smarter in complicated network of proxies.
- It is very important that the journalists are educated and regularly trained on countering disinformation and not misunderstand that providing balanced news by providing misinformation is not appropriate. The role and capacity of regulators needs to be upgraded.
- Capacity and CSO capacity needs to be updated, same for international guidelines, including cyber security issues. Needs-based approach information, the broad input from society. COVID has pushed the digitalisation, in information, campaigning, financing, and even in securing our health.
- Pieces of information can reach millions in matter of seconds.
- Media cannot be trusted as professional and balanced any more as in greed of information at times.
- Some governments are misusing the technical optimism of 2011 that social media can enhance and bring democracy
- Human rights have to be protected online the same way as in offline circumstances
- False info is not illegal per se.

- We cannot defeat disinformation but can prepare people and institutions for it
- Countermeasures are necessary; otherwise, the fake story is repeated. Countermeasures have to be taken by government and civil society
- Appeal to explain in member states what is happening in Ukraine and explain to Russians as well.

Recommendations and solutions as a takeaway from the conference:

- ✓ Undertake proactive actions in lieu of disinformation.
- ✓ Update laws in general to digital era and develop regulatory frameworks in particular media which are in relation to human rights instruments. Focus on structure and organisation and not on content
- ✓ To institutionalise independent third-party oversight on AI use in elections
- ✓ To massively enhance media literacy in particular digital media literacy both among young and older parts of society.
- ✓ Focus on microtargeting which can often be close to manipulation
- ✓ Look on media ownership and insist on the transparency of sources of information
- ✓ When discussing media issue, do not forget situation freedom and independence of journalists.
- ✓ Consider drafting universal convention for digital rights, starting with stakeholders
- ✓ Remaining key issues of i-voting are integrity, secrecy, verifiability, transparency, accountability, recount, auditing, and autocratic states. These are existing serious risks, that need to be mitigated otherwise the public confidence in elections in general, including democracy can be undermined. Develop ISO standards for i-voting.
- ✓ The internet and social media should not be seen only in negative perspective.

Contact

Robert Krimmer
University of Tartu
Johan Skytte Institute of Political Studies
Lossi 36
51003 Tartu
Estonia
Phone: +372 737 5583
E-mail: eceps@ut.ee
www.eceps.ut.ee/en