RIGA GRADUATE SCHOOL OF LAW

DEVELOPING A LEGAL FRAMEWORK FOR RESILIENT SOCIETIES IN LATVIA AND THE EUROPEAN UNION

RIGA GRADUATE SCHOOL OF LAW

Embassy of the Federal Republic of Germany Riga

NATO OTAN

DEVELOPING A LEGAL FRAMEWORK FOR RESILIENT SOCIETIES IN LATVIA AND THE EUROPEAN UNION

Riga
2024

The project aims to gather key local and international experts from the media, legal community, and NGOs to develop national, European, and transatlantic level recommendations for a legal framework for countering disinformation and enhancing societal resilience against it.

Authors: Adam Czarnota, Dariia Opryshko, Dmitri Teperik, Ēriks Kristiāns Selga, Magdalena Wilczyńska, Mārtiņš Hiršs, Maya Sobchuk, Monika Hanley, Solvita Denisa-Liepniece, Vygantė Milašiūtė.

Editor: Adam Czarnota, Sintija Broka

Project coordinators: Sintija Broka, Krišs Ēlerts

English language editor: Talis Saule Archdeacon

Cover design: Anda Nordena

Layout: Anda Nordena

The project has been developed with the support of the Embassy of the Republic of Germany in Riga and the NATO Public Diplomacy Division.

The opinions presented here belong to the authors and may not necessarily represent the views of the Riga Graduate School of Law, any project partners, or any governmental or other entities.

ISBN 978-9934-8684-3-6

Table of contents

Opening remarks

Viktors MAKAROVS,
Special Representative of the Latvian Ministry of Foreign Affairs
on Digital Matters

Disinformation is in no way a new phenomenon, but the public's and policymakers' preoccupation with it is quite recent. In 2014, in the wake of the Russian invasion of Ukraine, the Baltic states' warnings about the rising tide of Kremlin propaganda were often dismissed as an issue that is specific and limited to those raising the concerns ('we will help you deal with your problem; as for us, we are fine'). Today, less than a decade later, things could hardly look more different.

Disinformation is prominent in public awareness and on political agendas across the world. Not one, but multiple exciting new academic fields have spawned or been energised by the phenomenon. Civil society has carved out a role for itself, and unlike many governments, it never lacks enthusiasm and creativity – even if sometimes it does lack coordination and funding. The independent media have been the first responders as well as leaders in raising awareness about and exposing disinformation. Academic and policymaking thinking on disinformation has evolved so much that even the term itself seems to no longer fit our understanding of the complex reality behind it. We can pride ourselves on the fact that the conceptual framework most widely used in the West today was developed through the efforts of EU institutions. Even four years ago, the idea of 'regulating the Internet' seemed unrealistic and unnecessary to many. Today, the EU's Digital Services Act is a powerful regulatory tool to address disinformation on online platforms without compromising on fundamental rights; it has already become a source of inspiration and ideas for regulation in countries outside the EU.

Despite all these achievements, however, the threats that disinformation poses to societies and to democracy loom larger than ever.

Overall, governments often still tend to respond to these challenges tardily, and sometimes even too late, when it comes to enacting practical, coordinated and sufficiently resourced policies. Even more problematically, there is ample evidence that disinformation is not necessarily something governments act *against* – in autocracies and struggling democracies, disinformation can be something governments and political actors employ to distort and game the political process. Disinformation remains a powerful factor that can tip the scales of elections in democracies – usually towards populist and even authoritarian outcomes. The pervasiveness of terrorist and anti-Semitic disinformation on the Internet in the wake of the savage Hamas slaughter of Israeli civilians shows both its potential to destabilise societies and the persistent failure of online platforms to address the problem.

Information manipulation by authoritarian states and other malicious actors is more of a challenge than it was a decade ago. For all its successes in building resilience, the West has not yet found an effective way to impose costs on the actors behind the most malicious and lethal forms of disinformation. The Russian government's propaganda machinery is still working in overdrive to justify its aggression and to deny its crimes in Ukraine. While restrictive measures have been introduced by the West, they are far from complete and have not stopped the global spread of Russian disinformation efforts. Inside Russia, for the propagandists labouring daily to shore up public support for the war, there no prospect of consequences. The issue of criminal liability for war propaganda remains unaddressed academically and politically. While Russia remains a leader both in terms of investment in disinformation and in terms of the technical quality of its execution, the Chinese government's actions in the information domain have been increasingly assertive, ambitious, and hostile to the West. Other foreign state actors are not far behind.

Lastly, the explosive development of AI is likely to change the disinformation field dramatically and in ways that, at this moment, are hard to predict. AI could power disinformation by making in cheaper, faster, and better; it could the take human confirmation bias to a new level and offer tailormade imagined realities, with disastrous consequences for the democratic process. It could also

empower citizens through better access to education and knowledge and give governments and civil society better tools to detect and expose falsehoods and information manipulation.

Ensuring that effective practical policies are in place to address the many aspects of disinformation will require more – not less – attention and resources in the years to come. Yet hoping that this is enough to build resilience would also be a dangerous mistake. Perhaps the most important lesson to be drawn from the last decade is this: while disinformation is a policy field, it is not an isolated problem. In a way, it is a symptom of a deeper challenge modern societies face. Democratic societies today are going through major social and political transformations. Disaffection with political and economic outcomes, shifting identities and a shifting sense of political communities, an erosion of trust in institutions – these are just some of the risks that accompany this process. Add to this a technological landscape that changes faster than societies can adapt, and a perfect storm of disinformation becomes an existential risk for democracies. If there is a silver lining to the gathering clouds, it is the possibility that addressing this one challenge can focus minds to reflect critically on broader threats to democracy – both internal and external. In the clash between democracy and authoritarianism, disinformation is just one battleground. But it's a battleground we cannot cede.

Looking Beyond Russia: Sources of Disinformation in the Baltic States

Dr. Martins HIRSS,
Political scientist

Disinformation is not a new phenomenon in the Baltic states. Russia has been disseminating propaganda about the Baltic states since the 1990s. However, Russia is not the only source of disinformation in the Baltics. Some local actors, including major political parties and influential local media outlets, have also been disseminating disinformation for decades. This article will start with a historical overview of Russian propaganda about the Baltic states and the key actors pushing Russian narratives. It will continue with an overview of local actors pushing conspiracy theories about George Soros, COVID-19 and the Istanbul Convention. This article will argue that focussing only on Russia neglects the real extent of the problem. Local actors disseminating disinformation often borrow their narratives from Russia. At a minimum, they erode critical thinking within society and open up people's minds to disinformation coming from hostile state actors.

When a complex and nuanced term enters the popular discourse, its original meaning often becomes muddied and vague. This has happened with the term 'disinformation' over the last few years. In its more precise meaning, disinformation is false information that is intended to cause harm. However, 'disinformation' (along with 'fake news') is now commonly used as a catch-all term for all types of manipulated information, starting from factually true but one-sided information up to purposely fabricated false information. In between, there exists a multitude of information manipulation techniques. Furthermore, the narrow definition of disinformation does not capture the whole extent of the problem. False, easy-to-spot and easy-to-debunk content is just the tip of the iceberg in a sea of manipulative information. Hence, this article will focus on a broader understanding of disinformation in the context of the Baltic states.

Disinformation also is not a novel concept of the 21st century – neither globally,[1] nor in the Baltic states. Each of the three countries experienced censorship and state propaganda when democracy was replaced by an authoritarian rule in the interwar period. All three experienced massive Soviet propaganda throughout the decades of Soviet occupation. After the collapse of the Soviet Union, Russia was weak and lost some of its propaganda capabilities. Nonetheless, the information campaigns against the Baltic states did not stop.

Since 1991, the Russian government and Russia's media have been framing the Baltic states as nationalist, fascist and Russophobic, with these terms often used as synonyms. This framing has gone together with the narrative that the Baltic states are violating the human rights of their Russophone minorities. Russian media have been systematically portraying the Baltic states as weak, impoverished 'failed states' that are vassals of the European Union or the US.[2] While these narratives have been present since 1991, Russia has also added new narratives over the last 30 years.

After Vladimir Putin became president in 2000, Russia increasingly started to rewrite history and deny the fact that the Baltic states were occupied by the Soviet Union. Instead, Russia went on a propaganda offensive and accused the Baltic states of the 'falsification of history'. Before the Baltic states joined the NATO alliance in 2004, Russia started framing NATO expansion as a NATO conspiracy to surround and invade Russia through the Baltic states.[3] By 2009, Russia's media predominantly referred to the Baltic states as *Pribaltika*[4] – a derogatory term which implies that the Baltic states are not real, sovereign countries, but just a territory next to the Baltic Sea. False and fabricated information is not the only tool in Russia's propaganda arsenal. Russia's disinformation campaigns rely on a decades-long cultivation of specific frames, narratives and attitudes which sow divisions in the Baltic states and benefit the Kremlin.

1 Turcilo, L., Obrenovic, M. (2020). *A Companion to Democracy #3 Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy.* Heinrich Böll Foundation, p. 5. Retrieved from: https://www.boell.de/sites/default/files/2020-08/200825_ E-Paper3_ENG.pdf.

2 Denisenko, V. (2015). *The basic concepts of the Baltic States image in the Russian periodical press after the collapse of the Soviet Union (1991–2009).* Journalism Research. No. 8, pp. 123-124.

3 Ibid. p. 124.

4 Denisenko, V. (2015). *Basic concepts of the Baltic States image in the Russian press after the collapse of the Soviet Union*. Presentation at Vilnius university, Faculty of Communication.

The main actors pushing these and similar narratives in the Baltic states were Russian media, which became increasingly controlled by the Russian state after Putin became president. The most popular TV channels among Russophones in Estonia and Latvia were local versions of Russia-based TV channels – First Baltic Channel (*Pervіy Baltiskiy Kanal*), NTV Mir Baltic, and RTR Planeta Baltija. All three were either directly or indirectly controlled by the Russian state and disseminated Kremlin-aligned narratives.[5] Latvia banned these three channels in 2021. Lithuania and Estonia did the same in 2022 after the Russian invasion of Ukraine. The closure of these TV channels has limited Russia's ability to easily reach Russophones who predominantly consume traditional media.

The 2022 Russian invasion of Ukraine also had other far-reaching implications on the disinformation landscape in the Baltics. All three governments also banned access to Russian state-controlled online news outlets. A few local Baltic online news outlets that disseminated Russian narratives before the war[6] stopped republishing stories from Russia-based media. Harmony party, which had won multiple elections in Latvia but was never included in a coalition government due to its cooperation agreement with Putin's party United Russia and the Communist Party of China, condemned Russia's invasion of Ukraine and no longer repeats Kremlin-aligned geopolitical narratives in Latvia.

Nonetheless, Kremlin-aligned propaganda still reaches Baltic populations. Kremlin-aligned content is still widely disseminated and freely accessible in the Baltic states on some social networks, especially Telegram[7] and TikTok.[8] Some local politicians, influencers and Kremlin-affiliated activists[9] still keep repeating

5 Winnerstig, M. (ed). (2014). *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*. FOI. pp. 54, 87, 88. Retrieved from: http://appc.lv/wp-content/uploads/2014/12/FOI_Non_military.pdf.

6 Hirss, M. (2021). *Kremlin-aligned "media" in Latvia: Kingdom of Crooked Mirrors*. GLOBSEC. Retrieved from: https://www.globsec.org/what-we-do/publications/kremlin-aligned-media-latvia-kingdom-crooked-mirrors.

7 Tetarenko – Supe, A. (2023). *Kremlin's propaganda in our pockets. How disinformation thrives on Telegram*. LETA, Specially for Re:Baltica. Retrieved from: https://en.rebaltica.lv/2023/07/kremlins-propaganda-in-our-pockets-how-disinformation-thrives-on-telegram/.

8 Spriņģe, I., Meidutė, A., Malts, K. (2023). *Disinformation on TikTok: Latvian police open criminal probes, while the police in Estonia ask to delete*. Re:Baltica. Retrieved from: https://en.rebaltica.lv/2023/02/dealing-with-tiktok-disinformation-latvian-police-opens-criminal-probes-estonian-simply-asks-to-delete/.

9 Liepiņa, I., Jemberga, S. (2023). *A Year of War. The Deniers, the Agitators, the Glorifiers – Who are They?* Re:Baltica. Retrieved from: https://en.rebaltica.lv/2023/02/a-year-of-war-the-deniers-the-agitators-the-glorifiers-who-are-they/.

some Kremlin-aligned narratives. While some streams of Russia's disinformation flows into the Baltic states have been blocked or dried up, it is impossible to block the flow of information completely in the digitalised world.

Looking beyond Russia – local actors using disinformation

While often associated with hostile state actors, such as Russia or China, the dissemination of disinformation is not limited only to them. Hostile state actors might have the most resources at hand to develop and disseminate wide-ranging information operations, but nonetheless, they are hardly the only actors using disinformation. Focusing only on hostile state actors misdirects attention away from the real extent of the problem. The table below shows the multitude of actors that manipulate information for their benefit, as well as some of the reasons they use disinformation.

Hostile states	Extremist groups, radicals, and populists	Non-independent media	Domestic governments	Political parties	Commercial actors	Individuals
• To achieve geopolitical goals • To discredit and weaken opponents	• To advance their agenda • To ferment polarisation To intimidate opponents	• To push agendas which benefit the owner, either directly (e.g. financial interests) or indirectly (e.g. political favours)	• To gain popular support • To discredit the opposition, independent media or political opponents	• To manpulate political discourse • To provide a one-sided, partisan perspective	• For profit (e.g. advertising that is misleading about the benefits of a product to boost sales)	• For financial or personal gains (e.g. an inflated sense of self-importance on social networks)

The goal of disinformation is to influence people's opinions, choices and behaviours. When disinformation is done at scale, the goal is to influence and change public opinion. The intentions behind the dissemination of manipulated information are usually some sort of profit or benefit for the source.[10] Hostile

10 Turcilo, L., Obrenovic, M. (2020). *A Companion to Democracy #3 Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy.* Heinrich Böll Foundation, pp. 5, 19. Retrieved from: https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_ENG.pdf.

state actors use disinformation to achieve their geopolitical goals, but other actors also use it to their benefit. For example, disinformation allows dishonest businesspeople to make a financial profit; politicians can get more votes after using manipulative, one-sided information in election campaigns; and individuals sharing conspiracy theories on their social media accounts can get an inflated sense of self-importance, such as a false perception that they are trying to save the world against a global, evil conspiracy. While this article cannot map out all disinformation actors in the Baltic states, it will focus on three case studies – local Baltic actors disseminating conspiracy theories about COVID-19, George Soros and the Istanbul Convention.

Throughout the COVID-19 pandemic, conspiracies were popular in the Baltic states. According to 2021 survey data, 42% of respondents in Latvia agreed that leading medical and scientific authorities are lying about the number of COVID-19 cases, 32% thought that COVID-19 was a planned operation by hidden forces or elites to control the population, and 9% of respondents thought that COVID-19 is fake and does not exist. There were similar figures in Lithuania, except for the second question (46%, 23%, and 10% for the respective questions) and slightly lower percentages in Estonia, where 22%, 21%, and 6% agreed with these statements.[11] While some COVID-19 conspiracies originated from Russia, they also originated from Western countries, especially the US. Often these were local actors who copied and adapted these conspiracies to the Baltic context.

A multitude of local actors in the Baltic states disseminated COVID-19 conspiracies along with Russian propaganda and occasionally in tandem with it. Estonian MEP Jaak Madison (EKRE), former Lithuanian MEP Viktor Uspaskich (DP), and Latvian member of Saeima Aldis Gobzems (KPV) were some of the most notable politicians disseminating anti-vaccination conspiracies. A few local celebrities, businesspeople and individuals on social media actively pushed COVID-19 conspiracies in the Baltics as well.[12] Often these were local actors without any ties to Russia, and they disseminated disinformation for political, financial or personal benefit. Furthermore, COVID-19 was not the

11 *GLOBSEC Trends 2021 Central & Eastern Europe one year into the pandemic.* (2021). GLOBSEC. pp. 52-54. Retrieved from: https://www.globsec.org/sites/default/files/2021-06/GLOBSEC-Trends-2021_final.pdf.

12 Repečkaite, D., Raudsik, H., Bērziņa. S., Puriņa, E. (2021). *Who spreads the vaccine lies in the Baltics*? Re:Baltica. Retrieved from: https://en.rebaltica.lv/2021/02/who-spreads-the-vaccine-lies-in-the-baltics/.

only case where some local political leaders disseminated disinformation. Some conspiracies have been deeply ingrained in the Baltic political landscape.

Similar to Russian propaganda, belief in conspiracies is also not a new phenomenon in the Baltic states (and elsewhere in the world). In an early-2020 survey (from before the COVID-19 pandemic), a significant number of respondents in the Baltic states believed various classic conspiracy theories. A total of 43% of respondents in Latvia (42% in Lithuania and 37% in Estonia) agreed that world affairs are decided by secret groups aiming to establish a totalitarian world order. Meanwhile, 29% of respondents in Latvia (34% in Lithuania and 16% in Estonia) thought that Jews have too much power and secretly control governments and institutions around the world.[13] These numbers are not surprising taking into account that conspiracies about George Soros have been disseminated in the Baltic states by some political parties and a few major media outlets for decades.

One conspiracy theory that has been used in politics in the Baltic states since the 1990s is about George Soros and his alleged sinister influence. This conspiracy theory, which has strong antisemitic undertones, portrays Soros as the leader or part of an alleged hidden global network of ruthless capitalists, bent on destroying the traditional way of life.[14] In Latvia, the Soros conspiracy has been repeated for decades by the oligarch Aivars Lembergs and his party the Union of Greens and Farmers,[15] as well as by politicians of the National Alliance.[16] 'Sorosites' has become a swearword used to demonise liberals in Latvia. In Estonia, the political party EKRE has pushed conspiracies about Soros's 'evil' intentions and accused him of 'provoking riots and inciting wars'.[17] In Lithuania,

13 *Voices of Central and Eastern Europe Perceptions of democracy & governance in 10 EU countries*. (2020). GLOBSEC. pp. 47-48. Retrieved from: https://www.eesc.lt/wp-content/uploads/2020/12/Voices-of-Central-and-Eastern-Europe_read-version.pdf.

14 Astapova, A., Colacel, O., Pintilescu, C., Scheibner, T. (eds). (2020). *Conspiracy Theories in Eastern Europe: Tropes and Trends*. Routledge. pp. 192-195, 207-226.

15 Gabre, A. (2011). *Lembergs aktualizē Sorosa ietekmi*. [Lemberg rises up the issue of Soros' influence.] Neatkariga Rita Avize. Retrieved from: https://nra.lv/latvija/politika/49966-lembergs-aktualize-sorosa-ietekmi.htm.

16 Iesalnieks, J. (2007). *Trīs konkurējošās "elites"*. [Three compeating "elites".] Retrieved from: http://www.iesalnieks.lv/2007/10/tris-konkurejosas-elites.html.

17 Koorits, V. (2016). *EKRE portaal avaldas George Sorosi kohta artikli, mis kubiseb tavaliselt Venemaa propagandas kasutatavatest süüdistustest*. [The EKRE portal published an article about George Soros that is full of accusations usually used in Russian propaganda.] Delfi. Retrieved from: https://www.delfi.ee/artikkel/74281153/ekre-portaal-avaldas-george-sorosi-kohta-artikli-mis-kubiseb-tavaliselt-venemaa-propagandas-kasutatavatest-suudistustest.

no political party has embraced Soros conspiracy rhetoric. However, the conservative Lithuanian newspaper *Respublika* has been pushing conspiracies about Soros and writing about his 'network' of 'influence agents' in Lithuania for decades.[18] While conspiracies about Soros currently play a smaller role in the political landscape of the Baltic states than they used to, these conspiracies have been replaced by a new set of conspiracies to discredit liberal ideas. One of them is about the Istanbul Convention.

The Istanbul Convention (The Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence) is a human rights treaty of the Council of Europe aimed at the prevention of domestic violence, improving victim protection and ending the impunity of perpetrators of domestic violence. Six EU member states have not ratified the Convention. Latvia and Lithuania are among these six countries, with mainstream political parties often denouncing the Convention based on conspiracies and false claims.

Various individuals, NGOs and political parties (the National Alliance, the New Conservative Party, United List) in Latvia are against the Convention, often portraying it as an evil global conspiracy. For example, critics in Latvia have claimed that the Convention will 'destroy the traditional family' and operate 'like a global feminist police which has the right to intervene in the international affairs of every state'.[19] Similarly, in Lithuania the Catholic church and some politicians – for example, members of the Union of Lithuanian Peasants and Farmers (LVŽS), have claimed that the Convention 'under the cover of protecting women' actually 'manipulatively' pushes a 'liberal' agenda 'threatening' traditional values. They also claim the Convention could lead to schools encouraging kids to 'experiment with opposite gender clothing, accessories, and their

18 *Sorošo tinklas Lietuvoje: Ka raše "Respublika" apie Džordža Soroša prieš 15 metu*. [Soros network in Lithuania: What "Respublika" wrote about George Soros 15 years ago.] (2021). Respublika. Retrieved from: https://www.respublika.lt/lt/naujienos/lietuva/lietuvos_politika/soroso_tinklas_lietuvoje_ka_rase_respublika_apie_dzordza_sorosa_pries_15_metu/.

19 Veidemane, E. (2023). *Ratificējot Stambulas konvenciju, mērķtiecīgi iesim uz ģimenes iznīcināšanu*. [By ratifying the Istanbul Convention, we will purposefully go towards the destruction of the family.] Neatkariga Rita Avize. Retrieved from: https://neatkariga.nra.lv/komentari/elita-veidemane/414304-ratificejot-stambulas-konvenciju-merktiecigi-iesim-uz-gimenes-iznicinasanu.

gender identity'.[20] While Estonia has passed the Istanbul Convention, EKRE voted against the Convention because of 'hidden abnormal nonsense'. In addition to the destruction of traditional values, EKRE claimed it had found a secret conspiracy in the Convention to open Europe to Muslim immigration.[21] Although the details have been changing over time, conspiracies and disinformation have been a consistent element in domestic Baltic politics and societies.

Local actors disseminating disinformation diminish resilience to Russian disinformation

Conspiracy theories, including the ones covered previously, distort worldviews and erode critical thinking in society, thus making people more susceptible to other types of disinformation. Multiple studies have reconfirmed that the 'single best predictor of belief in one conspiracy theory is belief in a different conspiracy theory'.[22] This means that if someone believes a conspiracy theory about COVID-19, Soros or the Istanbul Convention pushed by local disinformation actors, he or she is more likely to fall for a conspiracy theory pushed by Russian propaganda. This happens because local actors pushing conspiracies erode the critical thinking skills of their followers and help them develop a conspiratorial mindset.[23] People who use conspiratorial thinking see the world through a lens by which most events in the world are the result of the actions of a small, sinister, all-powerful group. This is the opposite of critical thinking, which involves analysing information based on evidence without any bias.

20 Puidokas, M. (2018). *Stambulo Konvencijos siekis apsaugoti moteris priedanga kitiems siekiams*. [The aim of the Istanbul Convention to protect women is a cover for other aims.] Alkas. Retrieved from: https://alkas.lt/2018/04/10/m-puidokas-stambulo-konvencijos-siekis-apsaugoti-moteris-priedanga-kitiems-siekiams/.

21 EKRE. (2017). *EKRE ei toeta istanbuli konventsiooni sinna peidetud anormaalsete jaburuste tõttu*. [EKRE does not support the Istanbul Convention because of the abnormal nonsense hidden there.] EKRE home page. Retrieved from: https://www.ekre.ee/ekre-ei-toeta-istanbuli-konventsiooni-sinna-peidetud-anormaalsete-jaburuste-tottu/.

22 Van Prooijen, J. W, Douglas, K. M. (2018). *Belief in conspiracy theories: Basic principles of an emerging research domain*. European Journal of Social Psychology. 48(7):897-908. https://doi.org/10.1002/ejsp.2530.

23 Lantian, A., Bagneux, V., Delouvée, S., Gauvrit, N. (2021). *Maybe a free thinker but not a critical one: High conspiracy belief is associated with low critical thinking ability*. Applied Cognitive Psychology. Volume 35, Issue 3 May/June 2021. pp. 674-684 Retrieved from: https://doi.org/10.1002/acp.3790.

The fight against hostile state disinformation starts at home. Russia and other hostile state actors often tap into real problems and divisions that exist in society. If local actors push conspiracy theories and disinformation, weakening critical thinking within society, it creates fertile ground for Russian disinformation. Furthermore, Russian propaganda can tap into conspiracy theories already popular in Baltic societies, amplify them, and spin them for Russia's benefit. It is necessary to call out and fact-check not only hostile state actors but also local actors when they use disinformation.

Furthermore, all three of these examples of conspiracy theories pushed by local actors portray liberal values, local governments and the West in a negative light. Some of these local actors copy their ideas from Western populists and conspiracy theorists. Others repeat conspiracies originating from Russia, which are also narratives that Russian propaganda is pushing about the West directly. Russian narratives aim to undermine Western governments by portraying 'Western civilisation as degrading, eroding and falling apart' and discrediting liberal-democratic values by depicting them as morally decadent, leading to the collapse of traditional values, 'bestiality, paedophilia and incest' in the West.[24] Local actors using conspiracies portraying the West and liberal values as evil help Russian information operations or at a minimum make it possible for Russian propaganda to tap into these sentiments.

Fact-checkers should debunk not only manipulated information coming from Russia but also that which is disseminated by local actors. However, fact-checking is only one tool in the countering-disinformation toolbox. Experimental research shows that fact-checking and media literacy interventions can help to reduce agreement with falsehoods, with the best results being when both tools are combined. However, these tools are not silver bullets. They cannot easily change deeply engrained mindsets and beliefs. Furthermore, in a real-life setting, fact-checking is likely to be less effective because it is hard for it to reach the right target audience, and disinformation actors discredit valid fact-checking with

24 Hybrid Warfare Analytical Group. *How Russian media fuels hostility towards the West.* Black Sea Trust of the German Marshall Fund, Ukraine Crisis Media Center. pp. 43 – 45, 72. Retrieved from: https://spravdi.gov.ua/wp-content/uploads/2021/06/final-report-in-text.docx-3.pdf.

conspiracies about fact-checkers and their own 'fake' fact-checking initiatives.[25] Fact-checking alone will not solve the problem of disinformation.

In the Baltic states, over the last few years, there have been numerous campaigns promoting critical thinking and media literacy. However, these have been ad hoc and project-based. There isn't a central institution in any of the Baltic states that is tasked with improving media literacy and critical thinking in society and that receives annual government funding. One of the best examples of decades-long systematic media literacy education is Finland. The Finnish National Audiovisual Institute is tasked with the coordination and implementation of Finnish national media education and media literacy policy, working with other government bodies as well as civil society organisations on national and regional levels.[26] Without a systematic and strategic approach to media literacy, and without brave initiatives that dare to call out disinformation coming from local actors, media literacy interventions will have only a limited impact.

For example, there have been a multitude of media literacy and critical thinking initiatives aimed at schools. Baltic governments have announced that both skills are a priority within the education system. However, much more work needs to be done to bolster the development of these skills in schools. In a school survey carried out in 2021, 63% of 11 to 17-year-old pupils in Lithuania (57% in Latvia and 55% in Estonia) stated that they have not been taught in their schools how to verify the truthfulness of information.[27] Media literacy and critical thinking are skillsets that will be increasingly relevant in the 21st century with an ever-increasing amount of information in a digitalised world. This requires significant, consistent, and strategic investment from the government, not simply disjointed ad hoc projects and sporadic initiatives.

25 Hameleers, M. (2020). *Separating truth from lies: comparing the effects of news media literacy interventions and fact-checkers in response to political misinformation in the US and Netherlands*, Information, Communication & Society, 23 (12). Available at https://doi.org/10.1080/1369118X.2020.1764603.

26 National Audiovisual Institute home page. *Media Education*. Retrieved from: https://kavi.fi/en/media-education/.

27 Telia Company, Drossinternets.lv (2021). *Vai bērni un jaunieši pārbauda informācijas patiesumu internetā?* [Do children and young people check the truth of information on the Internet?] Dross Internets home page. Retrieved from: https://drossinternets.lv/lv/materials/download/infografika-vai-jauniesi-parbauda-informaciju.

Lastly, more focus should be placed on 'prebunking' – pre-emptively debunking disinformation in its bud by countering and dispelling myths and misconceptions to inoculate people against disinformation.[28] For example, an anti-vaccine movement – albeit a smaller one – already existed in Lithuania, Latvia and Estonia before the COVID-19 pandemic. This growing movement was largely ignored before the pandemic. There were very few if any vaccination promotion campaigns in the Baltic states until it was too late. Vaccination support campaigns prebunking misconceptions and calming worries about vaccination could have helped to reduce anti-vaccination sentiments during the global pandemic, making it harder for conspiracy theorists to hijack the debate. Similarly, information campaigns prebunking conspiracies, popular myths and misconceptions would create societies that are more resilient to disinformation.

28 Harjani, T., Roozenbeek, J., Biddlestone, M., van der Linden, S., Stuart, A., Iwahara, M., Piri, B., Xu, R., Goldberg, B., & Graham, M. (2022). A Practical Guide to Prebunking Misinformation. University of Cambridge, BBC Media Action, Jigsaw.
Retrieved from: https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf.

The Mapping of Disinformation and Fake News Phenomena: The EU Perspective

Ēriks Kristiāns SELGA,
Guest Lecturer at the Riga Graduate School of Law

The EU has defined disinformation as 'the creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public'.[1] Disinformation campaigns have been observed for decades, if not centuries, having their roots in state- and non-state-led propaganda campaigns. However, with the rise of social media and other online platforms as the main hubs of information, the ease of access and delivery mechanisms have made disinformation an increasingly utilised tool by adversaries seeking to interfere with or destabilise EU member states and their Western allies.

A myriad of disinformation campaigns have been observed in the last decade. Though not exhaustive, prime examples include attacks against Ukraine, the US and French presidential elections, as well as interference in the Brexit referendum.[2] In early 2020, following the COVID-19 outbreak, the unprecedented wave of health-related disinformation was described by the World Health Organisation as an 'infodemic'.[3] The invasion of Ukraine by Russia in February 2022 is the latest escalation of disinformation orchestrated by the

1 European Court of Auditors. (2020). *EU Action Plan against Disinformation*. Accessed October 2, 2023.

2 Chłoń, T. (2022). *NATO and Countering Disinformation*. EU Agenda, Retrieved from: https://www.globsec.org/sites/default/files/2022-05/NATO-and-Countering-Disinformation-ver1-spreads.pdf.

3 World Health Organization. (2020). *Let's Flatten the Infodemic Curve*. Gavi, the Vaccine Alliance. Retrieved from: https://www.gavi.org/vaccineswork/lets-flatten-infodemic-curve?gclid=Cj0KCQjwy4KqBhD0ARIsAEbCt6hq47kxdlLBwAmYdYiuR4CYPwHXsHu3M2eVLMXziKfA8hPX_CtzZ.

Russian government and aligned actors.[4] Investigations of Russian-orchestrated disinformation campaigns have revealed that they employ diverse strategies to introduce, amplify, and spread false and distorted narratives, mixing fake and artificial accounts, anonymous websites, official state media, online social media platforms, and street-level campaigns.[5] These disinformation activities are produced in large volumes, and they are produced and disseminated by specialised paid 'trolls' to spread inflammatory content.[6]

Fake news remains one of the most important types of campaign. Because social media is increasingly the source of news for children and adults – a Reuters study found that at least a third of people receive their news from social media – and because news cycles are rapid, news-related posts remain an effective channel to initiate and 'hook' audiences into different disinformation funnels.[7] The impact of disinformation has ranged from short-term destabilisation to a diminishing of the quality of democracy in the medium to long term by distorting electoral processes and fostering incivility and polarisation online.[8]

Until recently, there was no discrete legal framework governing disinformation in the EU apart from Article 11 of the Charter on the Fundamental Rights on the Freedom of Expression and Information. To confront the growing disinformation challenges, in 2018 the EU adopted the Action Plan Against Disinformation, which is composed of four pillars. The first pillar aims to improve the capabilities of Union institutions to detect, analyse and expose disinformation – these actions include, for example, strengthening the StratCom task forces. The second pillar regards strengthening a coordinated and joint response, including setting up a Rapid Alert System (RAS), which is a dedicated digital platform where EU member states and EU institutions can share insights on disinformation through a network of 28 national contact points, alongside

4 European External Action Service. (2022). *2022 Report on EEAS Activities to Counter FIMI*. STRAT.2, Retrieved from: https://euhybnet.eu/wp-content/uploads/2022/11/EEAS-AnnualReport-WEB_v3.4.pdf.

5 OECD. (2022). *Disinformation and Russia's war of aggression against Ukraine*. OECD Policy Responses. Retrieved from: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

6 Ibid.

7 Newman, N. (2023). *Digital News Report 2023*. Reuters Institute. Retrieved from: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023.

8 Colomina, C., and Sanchez, H., Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world*. European Parliament. Retrieved from: https://europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

the European Parliament (EP), NATO, and the G7.[9] The third pillar entails mobilising the private sector to tackle disinformation via a non-binding Code of Practice on Disinformation for online platforms. The fourth pillar regards raising awareness and improving societal awareness through a variety of resilience campaigns, supporting quality journalism, fact-checking, promoting medial literacy, and enacting the Elections Package.

The plan was followed by the Commission's European Democracy Action Plan of 2020, part of which is dedicated to strengthening the fight against disinformation, which led to setting up an overhaul of the Code of Practice on Disinformation into a co-regulatory framework of obligations and accountability for online platforms.[10]

Lastly, and most importantly, was the implementation and coming into force of the Digital Services Act (DSA) in 2022, which introduced legally binding tools requiring companies with at least 45 million monthly users to put in place systems to control the spread of misinformation, hate speech, and terrorist propaganda, among other things, or risk penalties of up to 6% of global annual revenue or even a ban in EU countries.[11] The Directorate-General for Communications Networks, Content and Technology has published an independent study highlighting that some of the main subjects of the DSA – X (formally known as twitter), Meta, TikTok and Alphabet/YouTube – have enabled the Kremlin to run large-scale disinformation campaigns targeting the EU and its allies, with an aggregate audience of at least 165 million individuals, generating at least 16 billion views.[12]

In 2022, all major platforms except Telegram signed a strengthened Code of Practice on Disinformation based on the Commission's guidance, and this was applied during the second half of 2022. The companies published the results

9 EEAS. (2019). *Rapid Alert System Factsheet*. Retrieved from: https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf.

10 European Commission. (2023). *European Democracy Action Plan*. Retrieved from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en#countering-disinformation.

11 Platforms with less than 45 million users also have to comply with the DSA rules, though with smaller compliance burdens.

12 Directorate-General for Communications Networks. (2023). *Content and Technology, "Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns"*. Retrieved from: https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1.

of compliance efforts in early 2023, noting that the Code was not designed to address systemic information warfare perpetrated by state-backed actors across platforms, including hybrid tactics that go far beyond the spread of disinformation.[13]

In June 2023, the Special Committee of the European Parliament on foreign interferences in democratic processes (ING2) endorsed a report on countering foreign interference and information manipulation, calling for a 'whole-of-society' (WOS) approach to tackling the issue. The report consolidates several strains of thought that have emerged over the last decade, such as ensuring independence and the security of critical independence, a critique of large online platforms' failure to respond to disinformation, and the need to strengthen European- and national-level capacities for identifying and debunking malignant information campaigns.[14]

These findings also inform the development of further counter-disinformation developments, like the European Digital Services Board, which will be set up in 2024 to assist in supervising the implementation of the DSA, and the upcoming Regulation on Transparency and Targeting of Political Advertising, which introduces harmonised rules on the use of targeting and amplification techniques for political advertising involving the use of personal data. Together with the GDPR and transparency rules, this will affect how the targeting and amplification of political advertising can take place using personal data.[15]

Main challenges

As noted by the EP, the disinformation threat is both complex and multidimensional.[16] Several fundamental challenges remain in the mapping of disinformation, especially regarding fake news: (1) identifying their scope, (2) tracing their impact, and (3) gauging the effectiveness of resiliency measures.

13 Ibid.

14 European Parliament. (2023). *Foreign interference in all democratic processes in the European Union, including disinformation*. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.pdf.

15 European Commission. (2023). *Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising.* Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0731.

16 European Parliament. (2023). *Foreign interference in all democratic processes in the European Union, including disinformation*. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.pdf.

Though 83% of Europeans think fake news is a threat to democracy, and over 70% are concerned about disinformation online (especially in the pre-election period), the scope of disinformation is unclear.[17] Identifying the scope of disinformation entails understanding and properly identifying when disinformation is taking place. There is a consistent and careful balance that must be struck in identifying the difference between purposeful and malignant disinformation, misinformed views, and contrary or inflammatory opinions. Disinformation is capable of morphing between the three as it multiplies and amplifies existing positions. Identifying the amplification effect of a certain strain of disinformation remains highly difficult and requires an in-depth understanding of the context of the perpetrator of certain information, its recipients, and the subtext or connotation of certain information within different groupings.

Similarly, tracing the impact of disinformation remains a quantitively difficult task. It is still unclear whether the EU measures deployed to combat disinformation are truly impactful and what the temporal impact of such activities is. General measurements of impact may be too conservative, as exemplified by the fact that the RAS has not yet issued alerts, nor has it been used to coordinate common action. The threshold for triggering the alert system has been defined in qualitative terms as a disinformation campaign that has a 'transnational significant impact', implying that a significant impact at a transnational level has not been reached yet. Though the RAS may address a short-term disinformation incident, it is even more difficult to measure the long-term impact of disinformation campaigns on democracies, information spheres, polarisation, or other societal health and cohesiveness determinants.

Lastly, it is difficult to measure the impact of resiliency-building or counter-disinformation measures. The Commission has used opinion polling as one way to assess the effectiveness of strategic communications to influence perceptions about the EU, but it is difficult to attribute such results to EU or member-state actions. The StratCom task forces have not comprehensively measured the impact of their work, nor have they had an evaluation to assess their effectiveness. This has been a notable issue with EU v. Disinfo, the flagship of the EU's efforts to combat disinformation, which has faced criticism in the past for the erroneous attribution of Russian disinformation to domestic

17 EEAS. (2019). *Rapid Alert System Factsheet*. Retrieved from: https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf.

publications and for publishing cases that do not represent a threat to EU democracies. Thus, the findings that core online platforms like Meta, Google, YouTube, TikTok and X have not sufficiently increased their capacity to combat disinformation may be moving the needle too little – or, in certain cases, too far.[18]

The European Court of Auditors' audit of the EU Action Plan Against Disinformation also highlights that while the broader approach of the EU against disinformation has been a structurally significant step, the practical implementation of its action plans was inhibited by a lack of clear coordination arrangements in implementing the plans. As reacting or building resilience to disinformation is a subsidiary, grassroots activity, many different piecemeal initiatives have been developed to tackle them. However, the audit highlights the lack of coordinating communication workflows in partnership with local actors and civil society.[19] Commission DGs or the EEAS and other European initiatives often work in silos, without parallel streams of cooperation.[20] The three StratCom task forces also have different objectives, covering different agents of disinformation, without clear policy objectives or legal foundations and without a clear source of continued funding.[21]

Policy recommendations

The pervasiveness of the disinformation threat does not have a silver bullet solution. As disinformation continues to evolve, it is important that the EU community and its Western allies evolve alongside it and tackle it proactively. Several policy shifts are vital to getting ahead of disinformation and combatting the vulnerabilities it presents, especially in terms of fake news campaigns.

First, it is important to move to a risk-based approach to give the flexibility to react to threats and to form a united European standard for disinformation

18 EEAS. (2019). *Rapid Alert System Factsheet*. Retrieved from: https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf.

19 European Court of Auditors. (2020). *EU Action Plan against Disinformation*. Accessed October 2, 2023.

20 Ibid.

21 EEAS. (2019). *Rapid Alert System Factsheet*. Retrieved from: https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf.

risk assessment and risk mitigation. The DSA establishes categorical objectives for public protection through mitigating risks to fundamental rights, public safety, electoral processes, and more. It is imperative to continue developing risk standards that account for threats, vulnerabilities, and consequences to allow for the prioritisation of counter-disinformation activity and resource allotment. The Commission and member states should work together to develop a harmonised understanding of these kinds of risks to prevent a transnational spillover of disinformation, or even regulatory arbitrage due to a lack of enforcement capacity or will. It is also important to ensure that disinformation trends are reviewed annually.

Risk mitigation must also be evaluated post-implementation for its proportionality and the effectiveness of measures to address specific risks. The DSA provides 11 separate measures or processes to do so, broadly categorizable as policies or standards, content moderation, and algorithmic recommender systems. The mitigation metrics as proposed by researchers could entail the speed and consistency of disinformation removal, the de-amplification of disinformation travelling through the platform, non-follower engagement prevention, labelling consistency, the responsiveness rate to user notifications, redress of denial services, restrictions on inauthentic behaviour or algorithmic exploitation, denylisting URLs, and others.[22]

It is important that the EU utilise the anti-disinformation foundations it has created to rapidly disseminate threat and vulnerability data, as well as perpetrator information. This can entail, depending on the context, evidence of direct links with a malignant state or non-state actor, proximity to such actors, or ideological alignment with them. It is important to ensure that there are also consequences for the perpetrators where possible. The identification of these individuals or affiliated parties should be provided when criminal or civil proceedings are necessary, as should the tools to rapidly freeze assets and the functioning of any disinformation-enabling nexus in the EU. The criminalisation of disinformation is also imperative.

22 Directorate-General for Communications Networks, Content and Technology. (2023). *Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns*. Retrieved from: https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1.

A risk-based approach would also align with the EP's proposed creation of 'mirror clauses', which would ensure that the openness of the European information space to third countries would be proportionate to the access European media outlets have in these countries.[23] Similarly, the EP has recommended the Commission develop an EU-wide regulatory system to prevent media companies under the editorial control of foreign governments from acquiring European media companies. This involves further definition through observation of the main nodes of information travel, as well as the format and channel of disinformation campaign inputs – including the ability to create profiles, post, post as others, purchase accounts, advertise, or other ways to access digital and traditional media. When such input paths are discovered, it is critical that the perpetrators are found and prevented from performing other campaigns to the greatest extent possible. This may lead to more identity controls for platforms in regards to their users, as traditionally creating and using a profile has been relatively frictionless, requiring only an email address.

Lastly, it is important to continue providing adequate resources to the various journalistic, anti-disinformation, and resiliency-building measures being enacted at a grassroots level. However, such initiatives should be measurable via a national risk assessment.

In monitoring the implementation of the Code, the Commission envisaged collecting information on the scrutiny of ad placements, political advertising and issue-based advertising, the integrity of services, the empowerment of consumers, and the empowerment of the research community.[24]

23 European Parliament. (2023). *Report on foreign interference in all democratic processes in the European Union, including disinformation*. Retrieved from: https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html.

24 European Commission. (2018). *European Commission contribution to the European Council. Action Plan against Disinformation*. Retrieved from: https://commission.europa.eu/system/files/2018-12/eu-communication-disinformation-euco-05122018_en.pdf.

Fake News Phenomena and Law: The Baltic States' Perspective

Dr. Vygantė MILAŠIŪTĖ,
Associate Professor at the Vilnius University

Historical developments and the current situation

The issue of fake news, and most acutely disinformation (information that is false and deliberately created to harm a person, social group, organisation or country[1]), especially online disinformation campaigns (when false or misleading content that may cause public harm is spread online with an intention to deceive or secure economic or political gain[2]), acquired particular importance in the Baltic states in the context of election campaigns, the COVID-19 pandemic-related 'infodemic', and news related to Russia's war against Ukraine.

In 2013, right before the election process, the Estonian e-voting system was reported to be vulnerable to attack from foreign powers. Pro-Kremlin media also falsely claimed that e-votes were not secret and benefited right-wing parties.[3] Estonia's State Electoral Office in 2016 created an interagency task force to combat the influence of false messaging in its democratic processes. To guide its work, the small staff of the State Electoral Office adopted a network approach by engaging partners from other government agencies, intergovernmental organisations, civil society, social media companies, and the press to identify and monitor disinformation and to work with the press to correct false statements.

1 UNESCO definition of disinformation. Retrieved from: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2021/ASP%20Regional%20Dialogue%20on%20Digital%20Transformation/Session%20Pages/RD-Session-5.aspx.

2 EU definition of online disinformation. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

3 EUvsDisinfo. (2020). DISINFO: *Estonia's e-voting can be hacked*. Retrieved from: https://euvsdisinfo.eu/report/estonias-e-voting-can-be-hacked.

It also developed a curriculum that would help secondary school students improve their ability to separate fact from fiction. The collaboration largely succeeded in checking foreign interference. However, considerations involving free speech and censorship hobbled the task force's efforts to restrain the spread of disinformation by domestic political parties and their supporters.[4]

Foreign influence is suspected in relation to Latvia's municipal elections in 2021. From 13 May to 8 June 2021, DebunkEU.org analysed 564 articles related to the 2021 Latvian municipal elections. As a result, 45 articles (7.8%) were identified as disinformation. False and misleading information was most often published in Russian (57.8%). False and misleading information in digital media and social media tended to focus more on the elections as a political process, seeking to discredit and diminish the reputation of political parties and candidates (71.1% of all publications). Nevertheless, the activity of disinformation sources was relatively low. Like other democracies, Latvia has been a target of infrequent interferences within its cyberspace. However, there were no cases of external intervention before or after the 2021 municipal elections. No monitored credible local media sources discussed this matter, and Latvia's Security Service reported no direct or systematic attempts by external actors to influence the municipal elections.[5]

Disinformation related to elections was also reported in Lithuania by the Central Electoral Commission in 2019 in relation to the presidential elections (voting bulletins were misleadingly reported to contain errors)[6] and by the disinformation analysis centre 'Debunk' regarding the parliamentary election in 2020 (negative posts on Facebook sought to discredit democratic processes in Lithuania; 97.3% of posts that included negative communication about the Lithuanian parliamentary election and its participants were in Lithuanian, and

4 Innovations for Successful Societies. (2020). *Innovations for Successful Societies. Defending the vote: Estonia creates a network to combat disinformation, 2016–2020.* Global Challenges Election Disinformation. Retrieved from: https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/TM_Estonia_Election_FINAL%20edited_JG.pdf

5 Disinformation analysis center - Debunk. *Analysis of foreign influence and cyber incidents during the Latvian municipal elections 2021.* Retrieved from: https://www.debunk.org/analysis-of-foreign-influence-and-cyber-incidents-during-the-latvian-municipal-elections-2021 .

6 The Central Election Commission of the Republic of Lithuania. (2019). *Socialiniuose tinkluose buvo paskelbta dezinformacija apie rinkimų biuletenius.* Retrieved from: https://www.vrk.lt/naujienos/-/content/10180/1/socialiniuose-tinkluose-buvo-paskelbta-dezinformacija-apie-rinkimu-biuletenius.

only a minority [2.7%] were posted in Russian)[7] and municipal elections in 2023 (potential attempts to artificially boost the content posted by certain candidates were noticed on Facebook; an official complaint was filed by NGOs with the Central Electoral Commission regarding the possible use of bots, urging it to begin an investigation in conjunction with Meta).[8]

Regarding COVID-19 pandemic-related fake news, Latvia used its criminal law provisions to punish the perpetrators. On 30 July 2020, the Criminal Court approved an agreement between the prosecutor and the accused regarding the criminal offence described in Section 231, Paragraph 1 of the Criminal Law. The criminal act – the disturbance of public order, manifested in an apparent disrespect for society, ignoring generally accepted norms of behaviour and disrupting the work of human beings and institutions (hooliganism) – was carried out by posting fake news, among other things, regarding COVID-19 on a specifically created webpage. As a reaction to this news, several members of parliament (Saeima) proposed enacting new criminal law norms that would envision criminal liability for distributing fake news with financial intent.[9] An influencer who posted lies regarding the first case of COVID-19 in Latvia (while there were still none) was detained the next day and then found guilty of hooliganism and incitement to hatred on social media, and they were sentenced to seven months in prison. Latvia is the only one of the Baltic states that has used the Criminal Code in combatting misinformation and that has had state institutions detain people for spreading fake news. Although in Lithuania and Estonia there has also been talk of the state exercising the Criminal Code against spreaders of disinformation, the concern that it will restrict freedom of speech has proven to be stronger. Latvia's neighbouring states are currently relying on media literacy programmes to educate society. In Estonia, there is a

7 Disinformation analysis center - Debunk. *Negative posts on Facebook sought to discredit democratic processes in Lithuania*. Retrieved from: https://www.debunk.org/negative-posts-on-facebook-sought-to-discredit-democratic-processes-in-lithuania.

8 Disinformation analysis center - Debunk. *NGOs recorded cases of potential social media manipulation during municipal election campaign*. Retrieved from: https://www.debunk.org/ngos-recorded-cases-of-potential-social-media-manipulation-during-municipal-election-campaign.

9 Fertmann, M. and Kettemann, M.C. (eds.). (2021). *Viral Information. How States and Platforms Deal with Covid-19-Related Disinformation: an Exploratory Study of 20 Countries*. Gdhrnet working paper No. 1. Retrieved from: https://graphite.page/GDHRNet-WP1/assets/documents/GDHRNet-Working_Paper-1.pdf.

special team at the State Chancellery working on the issue, while Lithuania has involved military analysts.[10] Disinformation analysts established that in May 2020, Latvia had the widest spread of COVID-19-related disinformation in the Baltic states – more than a half of this kind of news was published in Latvia (59%), almost one third of it (28%) was recorded in Lithuania, and less than 13% appeared in Estonia[11] – which could explain the harshness of its response to the problem. In 2022, the Ministry of Justice of Latvia reached the conclusion that it is necessary to separate from general hooliganism criminal liability in relation to the deliberate distribution of false information; this will facilitate proving a criminal offence, as well as ensure that the special provision deters individuals from disseminating false information that creates a gross disturbance of public order. It emphasised that the amendments to the criminal law are not designed to limit the free expression of views and beliefs but are instead aimed at preventing a gross disturbance of public order by publicly and consciously disseminating false information. The ministry noted that we are currently living in an era where deliberate and targeted disinformation is being disseminated in order to influence the geopolitical situation, as well as the mood and divisions in society, including in order to achieve certain objectives related to the creation of instability and panic in the country.[12] The President of the Constitutional Court of Latvia in her speech at the opening sitting of the Constitutional Court Judicial Year on 4 February 2021 noted that 'in a technological age permeated by targeted disinformation meant to influence public opinion, the judiciary needs to proactively reach out to the public and to the other branches of government. It is important for us that the public sees, hears and understands the judiciary – not only through our rulings, but also through a high-quality exchange of ideas on important

10 Springe I., et. al. (2021). *Who calls the shots on fake news? The minefield of countering lies in the Baltics*. LRT.lt. Retrieved from: https://www.lrt.lt/en/news-in-english/19/1418424/who-calls-the-shots-on-fake-news-the-minefield-of-countering-lies-in-the-baltics.

11 Delfi.lt. (2020). *Debunk EU: Latvia had the widest spread of COVID-19 related disinformation in May*. Retrieved from: https://www.delfi.lt/en/politics/debunk-eu-latvia-had-the-widest-spread-of-covid-19-related-disinformation-in-may-84505739.

12 Ministry of Justice of The Republic of Latvia. (2022). *Ministry of Justice of The Republic of Latvia's clarification of the amendments to Criminal Law concerning deliberate dissemination of false information both in the public sphere and in the digital environment*. Retrieved from: https://www.tm.gov.lv/en/article/ministry-justice-republic-latvias-clarification-amendments-criminal-law-concerning-deliberate-dissemination-false-information-both-public-sphere-and-digital-environment?utm_source=https%3A%2F%2Fwww.google.com%2F.

national issues which affect us all, the values and principles of a democratic state governed by the rule of law'.[13]

In the context of Russia's war against Ukraine, which started in 2014 and entered the phase of a wide-scale Russian invasion in 2022, measures aimed at reducing disinformation included the suspension of broadcasting services from Russia, as well as additional measures aimed at deterrence. In Estonia, Latvia and Lithuania, the national authorities issued instructions to suspend Russian media outlets shortly after the invasion of 24 February 2022 – prior to the Council Regulation (EU) 2022/350 of 1 March 2022 (which is directly applicable in its entirety and suspended broadcasts from and access to certain Russian media outlets) and even before the President of the European Commission announced the intention to implement this measure across the EU.[14] The suspension of broadcasting services started in Lithuania and Latvia even earlier. Since 2014, the Radio and Television Commission of Lithuania has on a number of occasions decided to temporarily suspend the broadcasts of some Russian TV stations, as investigations concluded that the content being broadcast violated the European Union Audiovisual Media Services Directive and the Republic of Lithuania Law on the Provision of Information to the Public because the content repeatedly incited hatred among nations and instigated war.[15] In Latvia, several operators had already stopped the distribution of some Russian channels on 1 February 2022, before the beginning of the wide-scale war. The intention behind these actions is unknown – presumably it was due to a lack of consumer interest. The chairman of the National Electronic Mass Media Council (NEPLP) noted that this decision would reduce the amount of propaganda. Sixty programmes – half of which were Russian – were banned from broadcasting in Latvia during the three years prior to 2022.[16] In Lithuania, Russian TV bans after the start

13 Constitutional Court of the Republic of Latvia. (2022). *Report on the work of the Constitutional Court in 2021*. p.113. Retrieved from: https://www.satv.tiesa.gov.lv/wp-content/uploads/2022/06/WEB_PRINT_ST_gada_parskats_ENG_pa_lapam_V2.pdf.

14 Susi, M. et. al. (eds). (2022). *Governing information flows during war. A comparative study of content governance and media policy responses after Russia's attack on Ukraine*. Retrieved from: https://graphite.page/gdhrnet-wp4/#read-full-article.

15 Keršanskas, V. (2021). *Deterring disinformation? Lessons from Lithuania's countermeasures since 2014*, Hybrid CoE Paper No. 6. p.14. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf.

16 Susi, M. et. al. (eds). (2022). *Governing information flows during war. A comparative study of content governance and media policy responses after Russia's attack on Ukraine*. Retrieved from: https://graphite.page/gdhrnet-wp4/#read-full-article.

of war in Ukraine in 2014 were met by critical remarks from human rights defenders, who stressed the importance of educating the public and offering alternative information channels.[17]

In proceedings concerning the decision of the Lithuanian Radio and Television Commission that required media service providers active in Lithuanian territory and other persons providing Lithuanian consumers with services related to the distribution of television channels or broadcasts via the Internet to only broadcast or retransmit the Russian channel NTV Mir Lithuania in pay-to-view packages (for 12 months from the date on which the decision became effective), the Court of Justice of the EU found that the EU law does not apply, as this public policy measure does not restrict the retransmission of television programmes from one member state in the territory of the receiving member state.[18] Restrictions ordered by the Lithuanian Radio and Television Commission in this case were thus not against EU law.

The strategy adopted by Lithuania to deter further disinformation related to combines governmental, civil and private initiatives, and it includes measures to build resilience, deter by denial, and impose costs across different domains. Importantly, this meant moving from responsive 'crisis communication' to preventive 'strategic communication' as well as trying to better understand disinformation threats and looking for hybrid threats, as a number of information operations against the Lithuanian authorities have been conducted in coordination with cyberattacks.[19] In the initial years extremely high Russian disinformation flows, short-term mitigation (including the suspension of Russian TV channel broadcasting) was prioritised; however, longer-term initiatives were undertaken simultaneously to gradually boost societal and institutional resilience, to build an institutional capacity for the quick and effective mitigation of disinformation campaigns, to review the legal basis, and to develop targeted

17 Leonavičiūtė, I. (2015). *Transliacijų draudimų oponentai: lengviau skleisti propagandos baimę nei šviesti visuomenę.* MANO TEISES. Retrieved from: https://manoteises.lt/straipsnis/transliaciju-draudimu-oponentai-lengviau-skleisti-propagandos-baime-nei-sviesti-visuomene/#.

18 CJEU, C-622/17, Judgment of 4 July 2019, ECLI:EU:C:2019:566.

19 Keršanskas, V. (2021). *Deterring disinformation? Lessons from Lithuania's countermeasures since 2014*, Hybrid CoE Paper No. 6. pp.15-16. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf.

measures that could deal with the identified vulnerable elements (e.g. national minorities, regional media and similar).[20]

Analysis of the main challenges

One of the main challenges related to addressing the problem of disinformation is the need to preserve respect for the freedom of expression, i.e. the right to impart and receive information, which is not limited to correct information.[21] The obligation of states to protect freedom of expression is a constitutional norm and an international obligation. At the level of constitutional law, states may differentiate between types of information and define their statuses. Thus, under the Lithuanian constitution (Article 25), disinformation is specifically mentioned as a criminal action incompatible with freedom of expression, whereas mere fake (untrue) news would not fall under this category. Criminal law sanctions for spreading fake news might be problematic in cases where a person who is spreading fake news would be punished for merely spreading information that is not true. The monopolisation of truth by the state would be a problem in this case.[22] One possible way of justifying criminal responsibility for disseminating incorrect information is by referring to the harm such a spreading of information can cause. Such an approach is at the basis of, for example, the EU Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (in particular, states are required under Article 1 Paragraph 1(c) to make punishable publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity, and war crimes directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to

20 Ibid. p. 10.

21 Organization for Security and Co-operation in Europe. (2017). *Joint declaration on freedom of expression and "fake news"*, disinformation and propaganda. Retrieved from: https://www.osce.org/fom/302796.

22 Yale Law School. (2021). *Introducing: Tackling the "Fake" Without Harming the "News"*. Information Society Project. Retrieved from: https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/introducing-tackling-fake-without-harming-news.

violence or hatred against such a group or a member of such a group). Another way of circumventing the 'monopoly of truth' problem is to regulate the methods of spreading the information rather than the content of the information. The regulation of bots that amplify news on the Internet is one possible example of this kind of activity.[23] A recent Lithuanian draft law on the manipulation of online platforms, which is essentially aimed at criminalising so-called 'troll farms' (or 'bot farms'), seems to be taking both paths at the same time.

In February 2023, the media reported that Conservative MP Laurynas Kasčiūnas, who chairs the parliamentary National Security and Defence Committee, drafted amendments to the Law on the Provision of Information to the Public and to the Criminal Code. He proposes that the dissemination of disinformation by 'manipulating an Internet platform' should be punishable by up to three years in prison. Viktoras Daukšas, head of the Debunk.org disinformation analysis centre, told the committee that 'bots are a significant problem both in Lithuania and in the EU, but they [are] not being properly dealt with'. According to Daukšas, when social networks are informed about fake malicious accounts, they are usually not removed and continue to spread disinformation.[24] The abovementioned draft laws were registered at the parliament of Lithuania on 2 March 2023.[25]

> The proposed new provision of the Criminal Code reads as follows:
>
> 'Article 118. Illegal amplification of content dissemination via manipulation of online platforms.

23 Kurtz, L. (2020). *For misinformation not to be law: proposals against fake news*. Institute for Research on Internet and Society. Retrieved from: https://irisbh.com.br/en/for-misinformation-not-to-be-law-proposals-against-fake-news-2/. Yale Law School. *Fighting Fake News. Workshop report, 2017.* Information Society Project.
Retrieved from: https://law.yale.edu/isp/initiatives/floyd-abrams-institute-freedom-expression/practitioner-scholar-conferences-first-amendment-topics/fighting-fake-news-workshop.

24 BNS. (2023). *Lithuania moves to criminalise 'troll farms'*. Retrieved from: https://www.lrt.lt/en/news-in-english/19/1887143/lithuania-moves-to-criminalise-troll-farms.

25 Parliament of the Republic of Lithuania. *Visuomenės informavimo įstatymo Nr. I-1418 2 straipsnio, priedo pakeitimo ir Įstatymo papildymo 52(1) straipsniu įstatymo projektas Nr. XIVP-2468*.
Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/2d0290b0b8ce11ed924fd817f8fa798e?positionInSearchResults=0&searchModelUUID=249a6965-f4f6-4931-964d-730524145195.
Parliament of the Republic of Lithuania. *Baudžiamojo kodekso papildymo 1181 straipsniu projektas Nr. XIVP-2469.* Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/0a937391b8cf11ed924fd817f8fa798e?jfwid=14jc7oel2v.

1. A person who by manipulating an online platform amplifies dissemination of content directed at carrying out activities hostile to the Republic of Lithuania – its constitutional order, sovereignty, territorial integrity, defence or economic power shall be punished by a fine or by arrest or by imprisonment for a term of up to three years.
2. A legal entity shall also be held liable for an act provided for in this Article.'

The explanatory report[26] to this draft indicates that the aim of this provision is not to criminalise disinformation and its dissemination *per se*. Rather, the aim is to criminalise only the amplification of content visibility by manipulating an online platform and only when it is directed against (is hostile to) the state of Lithuania. The authors of the draft also note that activities hostile to the state of Lithuania are already defined in Article 118 of the Criminal Code, which envisages criminal responsibility for assisting another state in carrying out such activities. The amplification of content visibility is not going to be punished if it is done for the purpose of advertising, business, or training artificial intelligence. Criminal responsibility is foreseen for both natural and legal persons because both a private natural person and an employee of a legal person can manipulate an online platform.

On 20 March 2023, Debunk.eu published an article analysing the use of bots during the election campaign for municipal councils and mayors to artificially boost the content posted by certain candidates on Facebook. In the article, it referred to plans to include the concept of the manipulation of an online platform – including the prohibition thereof and related sanctions in legislation – saying this would be an important step in the run-up to the 2024 presidential, Seimas, and European Parliament elections.[27]

In November 2023, the abovementioned draft laws are still being examined at the parliament. The Ministry of Justice of Lithuania concluded that the

26 Parliament of the Republic of Lithuania. *AIŠKINAMASIS RAŠTAS dėl įstatymų projektų Reg. Nr. XIVP-2468, XIVP-2469*. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/f95d0f40b8cf11ed924fd817f8fa798e?jfwid=14jc7oel2v.

27 Disinformation analysis center - Debunk. *NGOs recorded cases of potential social media manipulation during municipal election campaign*. Retrieved from: https://www.debunk.org/ngos-recorded-cases-of-potential-social-media-manipulation-during-municipal-election-campaign.

amendment to the Law on the Provision of Information to the Public has to be seen in the context of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), and thus the government has to give its opinion on the draft.[28] Regarding the proposed amendment to the Criminal Code, the Ministry of Justice did not have any remarks in relation to the EU law (and it did not identify any need for the government's opinion).[29] On 6 September, the government adopted its opinion on the draft amendment to the Law on the Provision of Information to the Public.[30] Importantly, the government noted the need to elaborate on and clarify the notion of the manipulation of Internet platforms and proposed that the parliament should modify the draft. In particular, the government, following the opinion previously expressed by the law department of the parliament itself,[31] proposed using the phrase 'manipulation of accounts on an online platform'. In addition to that, the government proposed introducing the additional notion of 'manipulating the dissemination of content via accounts on online search engines', referring to the Regulation 2022/2065 definition of an online search engine. As regards the proposed amendment to the Criminal Code, the law department of the parliament in its opinion on the draft[32] suggested that the wording of the concept of 'manipulation' should be aligned with that in the Law on the Provision of Information of the Public. The debate on the notions to be used in the Law on the Provision of Information of the Public is thus of direct relevance to the examination of the draft amendment to the Criminal Code.

28 Parliament of the Republic of Lithuania. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/f7e1e570c87c11ed9b3c9397e1236c2a?jfwid=14jc7oel2v.

29 Parliament of the Republic of Lithuania. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/7dd56f50c7ae11ed9b3c9397e1236c2a?jfwid=14jc7oel2v.

30 Parliament of the Republic of Lithuania. *Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 6 d. nutarimas Nr. 715*. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/7509c1f44e0911ee8e3cc6ee348ebf6d?jfwid=14jc7oev04.

31 Parliament of the Republic of Lithuania. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/8d33e350bdbd11ed924fd817f8fa798e?jfwid=14jc7oel2v.

32 Parliament of the Republic of Lithuania. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/8d33e350bdbd11ed924fd817f8fa798e?jfwid=14jc7oel2v.

Policy recommendations

A rights-based approach is required to ensure the necessary respect for a constitutionally and internationally recognised right to freedom of expression and to keep restrictions on that right limited to what is necessary in a democratic society. Differentiating between various types of fake news (or the ways in which they are used) is necessary to ensure that freedom of expression extends beyond one version of the truth favoured by the state or an online content moderator in a particular situation.

The public should know where and how to find accurate information. It also has to be informed of the existing dangers of information campaigns and be educated to reach an adequate level of media literacy. Building the resilience of the society is essential. Quality journalism that delivers reliable news should be promoted. Fact-checking initiatives by public and private actors should be encouraged and supported in order to identify and debunk disinformation. State authorities should take the task of communicating with the public seriously, taking into account the fact that in a technological age permeated with disinformation possibilities, the practice of reaching out to the public and providing authentic information is vitally important.

The choice of soft measures aimed at identifying disinformation campaign-related threats should be left to the state itself, as the state is best-placed to assess its capacities to organise its response to such threats. For example, for small countries that have small administrations, coordination and a reliance on an inter-agency network approach to identifying disinformation in the context of elections may be a good solution, whereas transposing this approach to larger states may be problematic because of different patterns of inter-agency cooperation.

Without underestimating the importance of soft measures aimed at building resilience, identifying disinformation, debunking it and enabling access to reliable channels of information, a sanctions approach may be required to address the most acute threats related to disinformation, and a criminal law response to disinformation cannot be fully ruled out. Sanctions may well be limited to an online content take down, a cancellation of user accounts, or a suspension of the broadcasting of TV channels. However, to address incitement to hatred, violence, or war propaganda, a criminal law response may be required.

As criminal law is determined by legal traditions, societal needs and other particularities of specific states, the need for criminal law measures can best be identified by the state itself. Examples from the Baltic states show how one state may choose a criminal sanction method in the context of the pandemic, while another may experiment with using this response for addressing threats stemming from largely unregulated technological possibilities (enabling the use of troll farms), and yet another state may choose not to use the criminal law method at all in the context of fake news or disinformation.

One generally applicable recommendation would be to take a more strategic approach to disinformation and employ a variety of short-term and long-term measures to tackle this issue. Moving from a 'reaction to crisis approach' to a 'proactive strategic communication with the public approach' is necessary. Engaging in analytical activities aimed at better understanding existing threats is required to be able to adapt to the rapidly changing situation in terms of technologies available for organising information campaigns. Moreover, the hybrid nature of threats related to disinformation campaigns has to be given sufficient attention, as disinformation campaigns tend to be linked to other hostile activities such as cyberattacks, which makes it necessary to ensure the efficient coordination of relevant government agencies to respond to such hybrid threats.

The Fake News Phenomenon and Law: An EU Perspective

Dr. Dariia OPRYSHKO,
Senior Fellow in the Institute for Information,
Telecommunications and Media Law of the University of Münster

Problems connected with the definition of disinformation and its dissemination began to arise at the European Union level in 2014, namely after Russia's illegal annexation of the Autonomous Republic of Crimea and its active participation in the hostilities in eastern Ukraine. The issue of the 'fake news' phenomenon was and remains challenging, complex and multidimensional, especially for democratic states. This is due to many factors, including disinformation or manipulative information being disguised as value judgments, the use of the right to freedom of expression for the dissemination of such information, the rapid development of Internet technologies and the use of all the opportunities they provide (the fast dissemination of content, the use of 'bot farms' and 'trolls' to promote disinformation, war propaganda, incitement to hatred and/or violence, etc.), the rapid development of artificial intelligence (AI), the lack of a unified approach to the legal regulation of issues connected with countering the dissemination of disinformation and manipulative information, etc.

In this article, the author aims to make a brief overview of historical developments and the current situation regarding the 'fake news' phenomenon in the EU, to analyse the main challenges that arise in connection with this, and to provide recommendations on strengthening the existing EU legal framework.

Overview of historical developments and the current situation

The first steps related to combatting disinformation at the level of the European Union included the establishment of the East StratCom Task Force as part of the Strategic Communications and Information Analysis Division of the European External Action Service in 2015. In 2016, this was followed by the adoption of the Joint Communication 'Joint framework on countering hybrid threats – a European Union response', in which actions aimed at countering hybrid threats and fostering resilience at the EU and national levels were outlined. These included improving awareness, building resilience, preventing and responding to crises, and recovering from crises. It became a driving force for the establishment of the European Centre of Excellence for Countering Hybrid Threats (in 2017), which is focused on developing resilience and countering hybrid threats through research and practical trainings.

During the same time-period, the European Parliament called on the Commission 'to analyse in depth the current situation and legal framework with regard to fake news, and to verify the possibility of legislative intervention to limit the dissemination and spreading of fake content'[1]. These steps were followed by the adoption of the European Commission Communication 'Tackling online disinformation: a European approach', the European Commission Communication on 'Securing free and fair European elections', and the 'Action Plan against Disinformation' (all in 2018), as well as the launching of the Rapid Alert System (in 2019). Both communications as well as the action plan assigned a great role to improving the media literacy level as a tool that would empower citizens to better identify and cope with disinformation. In 2020, another two remarkable events connected with tackling disinformation happened. These were the establishment of the European Digital Media Observatory (EDMO) and the adoption of the European Commission Communication on the 'European Democracy Action Plan'. The latter set out a reinforced EU policy framework and specific measures for three spheres, including countering disinformation (Section 4 of the communication).

It is necessary to note that an important event aimed at combatting disinformation online happened in 2018. For the first time, representatives of

1 European Parliament resolution of 15 June 2017 *on online platforms and the digital single market* (2016/2276(INI), par. 36.

a number of online platforms, leading tech companies, and the advertising industry agreed on a set of self-regulatory standards and signed the 'Code of Practice on Disinformation'. During 2019 and 2020, the application of these standards and approaches was assessed by its signatories as well as by the European Commission with the help of the European Regulators Group for Audio-visual Media Services (ERGA). The results showed that the Code made an important impact on online platforms' policies for dealing with disinformation, including by encouraging them to become more transparent. However, the intensive flow of disinformation online during the COVID-19 pandemic[2] exposed a number of shortcomings of the Code[3] that had to be addressed. As a result, a wider range of stakeholders – which included a number of online platforms, fact-checking organisations, civil society and research organisations, and representatives of the advertising industry and technology spheres – signed the 'Strengthened Code of Practice on Disinformation' in 2022. At the same time, the need to establish additional strong and comprehensive mechanisms aimed at countering disinformation became more and more obvious.

Such a necessity became one of the main grounds for the adoption of the Digital Services Act (DSA) in 2022. In particular, the DSA strengthened the obligations of all providers of intermediary services that offer services to recipients in EU territory, considering factors such as the type of provider (*inter alia*, the introduction of obligations for providers to produce annual transparency reports that would allow the tracing of issues connected with disinformation; the obligation of hosting providers to introduce notice and action mechanisms; the duty of online platforms to introduce effective internal complaint-handling systems and to prioritise notices submitted by trusted flaggers; and the obligation of the providers of very large online platforms and of very large online search engines to maintain risk-assessment and mitigation mechanisms and to be subject to an annual independent audit). It also included a strengthening of the role of the EU Commission, the introduction of digital

2 Commission Staff Working Document. (2020). *Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*. SWD, 180 final of 10.09.2020, pp. 5,6.

3 European Regulators Group for Audiovisual Media Services (ERGA). (2020). *Report on disinformation: Assessment of the implementation of the Code of Practice*. Retrieved from: https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf ; Commission Staff Working Document. (2020). Section 3.2.

service coordinators and the establishment of the European Board for Digital Services, and a reinforcement of the role of civil society and researchers. If providers of intermediary services fail to comply with their obligations as laid down in the DSA, they might face sanctions (which shall be defined in the national legislation of EU member-states and shall not exceed 6% of their annual worldwide turnover, and which in some cases could include a temporary restriction of access to the service or to the online interface of the provider in the EU single market) (Articles 51(3)b, 52, 74). All this contributes to increasing the transparency and accountability of providers of intermediary services, especially of online platforms, as well as to providing a balanced mechanism for combatting disinformation online.

However, it is worth noting that the outlined measures apply only to the online sphere and do not concern traditional media. At the same time, other legal instruments are also used to limit the dissemination of disinformation in the EU – in particular, sanctions. This was due to the Russian aggression towards Ukraine, which was accompanied by massive disinformation campaigns. It resulted, *inter alia*, in a ban of Russian state-connected news media, in particular *RT* and *Sputnik*[4]. In addition, if the dissemination of disinformation includes spreading hate speech and/or incitement to violence or hatred, the distribution of such content may be forbidden by the national authorities under their national legislation and the Audiovisual Media Services Directive. In such cases, the European Commission decides whether the measures taken by the national authorities are compatible with EU law. For instance, in May 2019, the Latvian regulator suspended the retransmission of a Russian-language channel *Rossiya RTR* for three months. In this case, the Commission decided that the decision of the Latvian regulator was proportionate and justified[5].

In addition, attention is often paid to the fact that the wide use of AI, with its ample opportunities in many areas, contributes to increasing the flow of

4 Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

5 European Commission. (2019). *Latvia's decision to suspend broadcast of the Russian language channel "Rossiya RTR" complies with EU law.* Retrieved from: https://digital-strategy.ec.europa.eu/en/news/latvias-decision-suspend-broadcast-russian-language-channel-rossiya-rtr-complies-eu-law.

disinformation and manipulative content[6]. Currently, the European Union is preparing a legislative framework[7] aimed at regulating issues connected with AI, in particular in regard to the transparency obligations for certain AI systems.

Issues related to countering disinformation were briefly considered by the European Court of Justice and the European Court on Human Rights (ECHR). Although the terms 'disinformation' or 'fake news' are not used in their case-law, the courts evaluated the measures taken by the authorities to counter the dissemination of disinformation and propaganda[8]. The ECHR draws attention, in particular, to the fact that the dissemination of unreliable information is not illegal itself. However, if such content incites hatred and/or violence, or if it supports and justifies it, it is not protected by international law. In addition, balancing the right to freedom of expression and the need to take measures to protect national security, public order, territorial integrity, and the rights of others is considered through the prism of compliance with journalistic standards. The socio-political context, which is considered by the courts, is also of high importance[9].

Thus, during the last decade, there has been a tendency to strengthen legal regulations on issues related to countering disinformation – from self-regulation and media literacy campaigns to the development of a relevant legal framework.

Analysis of the main challenges

Currently, it is possible to identify the following main challenges that are connected with combatting disinformation in the EU: the lack of unified approaches to the legal definition of disinformation; the application of a

6 Shane, G. (2023). *A Campaign Aide Didn't Write That Email. A.I. Did*, New York Times. Retrieved from: https://www.nytimes.com/2023/03/28/us/politics/artificial-intelligence-2024-campaigns.html.

7 Proposal for a Regulation of the European Parliament and of the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

8 *Inter alia*, case T-262/15, *Dmitrii Konstantinovich Kiselev v. Council* [2017] ECLI:EU:T:2017:392; case C-622/17, *Baltic Media Alliance Ltd. v. Lietuvos radijo ir televizijos komisija* [2019] ECLI:EU:C:2019:566; case T125/22, RT France v. Council [2022] ECLI:EU:T:2022:483.

9 Decision of the European Court of Human Rights of 15.06.2023, case *Gaponenko v. Latvia*, application no. 30237/18.

sanctioning mechanism to counter the dissemination of disinformation; an insufficient level of media ownership transparency; and an increase in the flow of disinformation in connection with the development of information technologies, in particular AI systems.

The legal definition of disinformation

There are difficulties with defining the term 'disinformation'. A definition is provided only in Lithuanian legislation[10]. A political definition provided by the European Commission[11] has been criticised for being too broad and vague to function as a legal definition[12]. All this complicates the identification of this phenomenon and the introduction of legal mechanisms to combat disinformation.

A sanction mechanism

The use of economic sanctions to counter the dissemination of disinformation remains problematic. Such measures are widely criticised because of their possible arbitrariness and disproportionality[13]. And while the DSA is expected to become an effective legal tool for countering the spread of disinformation in the online environment, the question of mechanisms for combatting the dissemination of such content through traditional media remains open. In this regard, it is worth mentioning the European Media Freedom Act (EMFA)[14],

10 Įstatymo Lietuvos Respublikos visuomenės informavimo. (1996). Nr. I-1418. Retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29884/asr , point 15 of Article 1.

11 Disinformation is understood by the European Commission as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm', where public harm is considered as 'threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security' (European Commission. *Tackling Online Disinformation: A European Approach*. (2018). COM/2018/236 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236, s. 2.1).

12 Ronan, O.F., Helberger, N., Appelman, N. (2021). *The perils of legally defining disinformation*. Internet Policy Review, 10(4). DOI: 10.14763/2021.4.1584. Retrieved from: https://policyreview.info/articles/analysis/perils-legally-defining-disinformation.

13 *Inter alia*, Dirk, V. (2022). *EU silences Russian state media: a step in the wrong direction*, International Forum for Responsible Media Blog. Retrieved from: https://inforrm.org/2022/05/08/eu-silences-russian-state-media-a-step-in-the-wrong-direction-dirk-voorhoof/. Baade, B. (2022) *The EU's "Ban" of RT and Sputnik*. Verfassungsblog. Retrieved from: https://verfassungsblog.de/the-eus-ban-of-rt-and-sputnik/.

14 Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU, COM(2022) 457 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0457.

published by the European Commission in September 2022. The EMFA proposes the introduction of unified standards for all types of media (audiovisual, online, and print). Despite criticism regarding the inclusion of the press in the scope of the EMFA[15], this approach has its advantages. In particular, the establishment of common basic standards for all types of media (aimed at ensuring editorial independence, the transparency of media ownership, media pluralism, etc.) may contribute to more effective countermeasures against the dissemination of disinformation. In this context, the author agrees with Frederik Ferreau that the prevention of propaganda's dissemination within the EU shall be covered by the media law (based on the principle of the media being remote from the state), but not by the sanction law[16]. The EMFA is a step forward in this direction and may strengthen efforts to combat disinformation in the EU. However, the mechanisms proposed in the draft are currently insufficient to counter coordinated disinformation campaigns.

Transparency of media ownership

Transparency of media ownership plays an important role in countering the dissemination of disinformation, although this issue is usually considered in the context of ensuring media pluralism and fair economic competition in the media sphere. This is due to the fact that a complex analysis of a media ownership structure provides the possibility to trace the existence or absence of connections with certain states or persons related to those states. In case such a connection exists, questions as to the editorial independence of such media arise. This becomes especially important in times of an armed aggression of one state against another, as the connection of a particular media outlet to the state-aggressor or persons connected with that state are evidenced by the ownership structure, and this may become grounds for providing media regulators with tools to reduce the aggressor's information influence on the society.

15 *Inter alia*, Grünwald (2022). *Der European Media Freedom Act*. MMR 2022, 919. European Newspaper Publishers' Association. (2022). *European press publishers call on the European Commission not to adopt "Media Unfreedom Act"*. Retrieved from: https://www.enpa.eu/press-releases/european-press-publishers-call-european-commission-not-adopt-media-unfreedom-act.

16 Frederik, F. (2022). *"Sendeverbot durch Sanktionen: Das EU-Verbot russischer Staatsmedien aus der Perspektive des Medienrechts"*. VerfBlog. Retrieved from: https://verfassungsblog.de/sendeverbot-durch-sanktionen/. DOI: 10.17176/20220311-001240-0.

Artificial intelligence

The use of AI systems has become one of the biggest challenges in the context of combatting disinformation. They are widely used both for creating manipulative content and deepfakes (and for the identification thereof), as well as for 'detecting social bots, screening content for potential disinformation, performing deeper analysis that can detect modified versions of already debunked articles, modelling discussed topics, following hostile narratives, identifying AI-generated content (e.g., text, images, audio), and other activities'[17]. Currently, the legal regulation of AI systems is only now being developed, and stakeholders are facing many problems. For example, it is proposed that AI systems mark their generated content with watermarks[18]. However, scientists from the University of Maryland proved that the removal of such markings is 'a challenging, but not necessarily impossible task'[19].

Policy recommendations

Taking into account the challenges outlined above, it is recommended to consider the following actions.

- Continuing work on the development of a legal definition of the concept of 'disinformation', as well as legal mechanisms for countering its dissemination. Until such a legal mechanism is created, other measures should be taken by the EU and its member states to combat this phenomenon. They should include, in particular, further work on the improvement of the media literacy level, the creation of a favourable environment for the activities of an independent media working in compliance with journalistic standards to ensure public access to reliable information, as well as the creation of favourable conditions for the functioning of a pluralistic media environment.

17 Juršėnas, A. *et. al*. (2022). *The Role of AI in the Battle Against Disinformation*. NATO Strategic Communications Centre of Excellence. p. 34. Retrieved from: https://stratcomcoe.org/publications/download/The-Role-of-AI-DIGITAL.pdf , p. 7.

18 Philipp, H. *et. al.* (2023). *Regulating ChatGPT and other Large Generative AI Models*. pp. 1112–1123, Retrieved from: https://doi.org/10.1145/3593013.3594067. p. 1119.

19 Mehrdad, S. *et al.* (2023). *Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks*. pp.24, Retrieved from: https://doi.org/10.48550/arXiv.2310.00076. p. 10.

- Continuing work on the establishment of mechanisms to counter the dissemination of disinformation content. It is advisable to ensure this by adopting a separate media law at the EU level, which would regulate this issue for all types of media. The EMFA may become such a legal act – however, it is necessary to continue improving its provisions that are aimed at tackling this issue.
- Paying more attention to the issue of media ownership transparency in the context of countering disinformation. For this purpose, it is advisable to conduct relevant studies and hold public discussions of their results with the involvement of all stakeholders, as well as to assess the possibility of strengthening EMFA provisions in this regard.
- Continuing to work on finding the most effective ways to combat the dissemination of disinformation and manipulative content created with the help of AI systems – in particular, to analyse periodically the effectiveness of legal mechanisms introduced by the DSA for combatting disinformation, including manipulative content and deepfakes, generated by AI systems.

Fake News Regulation in the United States or Legal Perspectives on the Phenomenon of False Information in the United States?

Monika HANLEY,
Journalist at *The Baltic Times*

With a rise in social media usage and a decline in trust in traditional news media, the United States has grappled with the pervasive influence of misinformation and disinformation across various digital platforms. A 2022 Gallup poll found that just 7% of Americans had 'a great deal' of trust and confidence in the media, and 27% have 'a fair amount'.[1] A record 38% reported having no confidence in newspapers, radio, or TV news media, a rising rate which began in the mid- to late-1990s, coinciding with the advent of mainstream computer and Internet usage. The level of trust in media seems to be highly politically divisive, with 70% of those who identify as Democrats having a 'great' or 'fair' amount of confidence in media, while just 14% of Republican-leaning respondents report the same levels of confidence. Trust in the federal government is also at low levels in the judicial, executive, and legislative branches. Platforms that have enabled the wide sharing of information and news have faced much scrutiny over allowing the dissemination of false information and manipulative content to become pervasive in the US media environment.[2] While the proliferation of fake news, disinformation, and the dissemination of false content is not unprecedented, the current era is marked by an unparalleled

1 Brenan, M. (2023). *Americans' Trust In Media Remains Near Record Low.* Gallup. Retrieved from: https://news.gallup.com/poll/403166/americans-trust-media-remains-near-record-low.aspx.

2 The Center for Information, Technology, and Public Life (CITAP). (2023). *Addressing the Decline of Local News, Rise of Platforms, and Spread of Mis- and Disinformation Online.* Retrieved from: https://citap.unc.edu/news/local-news-platforms-mis-disinformation/.

level of accessibility and speed at which misinformation can propagate, creating challenges in maintaining information integrity and fostering a well-informed society.[3] Efforts to minimise the effects and stop the spread of false content have been met with opposition from legal entities and the civilian population, citing the defence of free speech at all costs.[4]

The perceived impact of the phenomenon on US society underscores the urgent need for comprehensive strategies to address the challenges posed by misinformation and disinformation, while balancing the fundamental principles of free speech and democratic values. This has led to the introduction of many measures aimed at attempting to either stop the dissemination of false information or to punish individuals or platforms for allowing false or harmful content, or aimed at providing broader education in society to arm citizens with critical thinking and media literacy skills to minimise the effects of harmful content. However, very few of these attempts have become law, and most have been met with criticism.

This chapter will provide an overview of legal measures that exist or have been taken against disinformation and false content, a review of notable cases, recommendations for strengthening the current framework in the United States, and takeaways for the European Union.

Overview

In the United States, the regulation of false speech is a complex matter governed by a framework that balances constitutional protections with the urgent need to address the harm caused by disinformation. While content-based laws typically trigger strict scrutiny, the Supreme Court has historically permitted the regulation of specific categories of false speech, such as defamation and fraud. Additionally, federal statutes prohibit certain forms of false speech, including perjury and providing materially false information to government

3 Hanley, M. and Munoriyarwa, A. (2021). *Fake News: Tracing the Genesis of a New Term and Old Practices*. Digital Roots: Historicizing Media and Communication Concepts of the Digital Age. pp.157-176. De Gruyter Oldenbourg. https://doi.org/10.1515/9783110740202-009.

4 Nielsen, R.K. (2021). *How to Respond to Disinformation While Protecting Free Speech*. Reuters Institute for the Study of Journalism. Retrieved from: https://reutersinstitute.politics.ox.ac.uk/news/how-respond-disinformation-while-protecting-free-speech.

officials.[5] Existing regulations extend to areas such as political advertising and broadcast media – these aim to curtail the spread of misinformation, but they can also safeguard misinformation in political advertising.[6] The United States is an exceptional case, however, as it not only strongly protects free speech but also includes hate speech in this definition, in stark contrast to many nations in the European Union.[7] While bills amending previous legislation have been put forward, thus far, none have passed at a federal level. The laws currently in force have been used to some extent for counter-disinformation efforts, but they are often deemed insufficient in addressing the multifaceted challenges posed by the rapid proliferation of false or misleading information in the digital sphere.

Current regulations and laws

The First Amendment

The foundational document that is the First Amendment of the Constitution serves as a cornerstone in safeguarding the right to free expression. It explicitly states: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.'

The First Amendment prohibits or limits government interference with free speech, however, the extent to which this protection extends to false or misleading speech remains a subject of ongoing legal and societal debate. However, the First Amendment does not prevent restrictions on speech put in place by private entities or businesses, including social media platforms.[8] These entities are free to regulate, or not regulate, as they see fit.

5 Congressional Research Service. (2022). *False Speech and the First Amendment: Constitutional Limits on Regulating Misinformation*. Retrieved from: https://crsreports.congress.gov/product/pdf/IF/IF12180.

6 CBS News. (2022). *Why Broadcasters Must Air Political Ads Even If They Contain Misinformation*. Retrieved from: https://www.cbsnews.com/news/broadcasters-air-political-ads-even-if-they-contain-misinformation/.

7 American Library Association. (2023). *Hate Speech and Hate Crime*. Advocacy, Legislation & Issues. Retrieved from: https://www.ala.org/advocacy/intfreedom/hate.

8 American Library Association. (2021). *First Amendment and Censorship*. Advocacy, Legislation & Issues. Retrieved from: https://www.ala.org/advocacy/intfreedom/censorship.

The Supreme Court has also upheld the idea that, as one of the rights guaranteed by the First Amendment, the right to receive information is also to be enforced and unimpeded by government intervention.[9] Supreme Court Justice William Brennan in 1965 stated:

> 'The protection of the Bill of Rights goes beyond the specific guarantees to protect from Congressional abridgment those equally fundamental personal rights necessary to make the express guarantees fully meaningful. I think the right to receive publications is such a fundamental right. The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.'
> *Lamont v. Postmaster General*, 381 U.S. 301 (1965).

In the landmark case *New York Times Co. v. Sullivan* (1964), Justice Brennan also established that public officials cannot sue news media for slander or libel unless the statement is made with actual malice or reckless disregard for the truth.This decision invalidated an Alabama law that enabled a city commissioner to sue the *New York Times* for libel over an advertisement alleging the mistreatment of civil rights demonstrators.[10] Brennan emphasised the necessity of enduring sharp criticism in public discourse and upheld the right to criticise those in positions of power.

Still today, the primary legal avenue to confront false information is through a defamation claim, whereby individuals can pursue litigation if a false statement has been disseminated about them leading to demonstrable harm, including job loss, financial setbacks, or reputational harm.[11] For private individuals, establishing a news outlet's negligence in publishing the false information is also a requisite component of the claim.

9 The Free Speech Center. (2023). *Right to Receive Information and Ideas - The Free Speech Center.* Retrieved from: https://firstamendment.mtsu.edu/article/right-to-receive-information-and-ideas/.

10 The Free Speech Center. (2023). *New York Times Co. v. Sullivan (1964) - The Free Speech Center.* Retrieved from: https://firstamendment.mtsu.edu/article/new-york-times-co-v-sullivan-1964.

11 Legal Information Institute. *Defamation.* Retrieved from: https://www.law.cornell.edu/wex/defamation.

Hate speech protections

Uniquely, under United States jurisprudence, hate speech, while controversial and widely condemned, is generally considered a form of protected speech. This constitutional protection has been upheld in multiple rulings by the United States Supreme Court as protected under the First Amendment. However, there are specific limitations to this protection, notably when hate speech directly incites violence against a particular group or individual or when it incites criminal activity (*Snyder vs. Phelps*). In the case of *Snyder v. Phelps*, it was ruled that the controversial and offensive speech of the Westboro Baptist Church, deemed to be hate speech by many, was protected under the First Amendment due to its lack of direct incitement to violence.[12] The decision underscored the principle that the United States upholds the right to freedom of expression even in cases where the speech is deemed offensive or hateful by the broader public.

Section 230 of the Communications Act of 1934

The Communications Act of 1934 was the first of its kind to bring together regulations for telephone, telegraph, and radio communications; it also created the Federal Communications Commission. Section 230 of the Communications Decency Act (CDA) is a critical piece of Internet legislation in the United States – enacted in 1996, it provides legal protections for online platforms and service providers (such as social media, search engines, and other computer-based services) to prevent them from being held liable for the content generated by third-party users, as such platforms are not considered the publisher of content posted by their users.[13] In essence, this means that platforms are not legally held responsible for the content of their users. However, despite offering broad liability protection, Section 230 does not protect platforms from liability related to federal criminal law, intellectual property law, or electronic communications privacy law. Platforms can still be held accountable for illegal activities that occur on their platforms, such as copyright infringement, human trafficking, and other criminal offenses.

12 United States Courts. *Facts and Case Summary - Snyder v. Phelps.* Retrieved from: https://www.uscourts.gov/educational-resources/educational-activities/facts-and-case-summary-snyder-v-phelps.

13 United States Department of Justice (2021). *Department of Justice's Review of Section 230 of the Communications Decency Act of 1996*. Retrieved from: https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

Section 230 has been the pivotal regulatory element in promoting and protecting free speech in the digital era. Despite this, critics argue that some platforms have misused the protections granted under Section 230, allowing harmful or misleading content to proliferate.[14] There have been ongoing discussions about potential reforms to address concerns related to online content moderation, misinformation, and user safety. While this law has been instrumental in the growth of the Internet, it has also been a subject of debate, with some advocating for reforming it to hold platforms more accountable for disinformation spread on their networks.

Federal Trade Commission (FTC) regulations

The FTC upholds truth-in-advertising laws, a set of rules that regulate nationwide ad content, applied uniformly across all media platforms, including newspapers, magazines, online spaces, mail, and outdoor advertising.[15] It scrutinises claims that have potential impacts on consumers' well-being and financial matters, particularly those concerning food, non-prescription drugs, dietary supplements, alcohol, tobacco, and technology-related products and services. Additionally, the FTC monitors and issues reports on advertising practices within the alcohol and tobacco industries. Amid the recent COVID-19 pandemic, the FTC issued cautionary notices to companies, warning them of potential violations of the FTC Act and the ensuing legal consequences, including federal lawsuits, should they fail to cease such practices immediately.[16]

In 2023, the FTC proposed a new regulation to curb deceptive marketing practices – including the use of fabricated reviews, the suppression of genuine negative feedback, and payment for positive reviews – as these practices mislead consumers seeking authentic product or service evaluations and undermine the credibility of honest businesses.[17]

14 Ashley, J. and Castro, D. (2023). *Fact-Checking The Critiques of Section 230: What Are the Real Problems?* ITIF, Retrieved from: https://itif.org/publications/2021/02/22/fact-checking-critiques-section-230-what-are-real-problems/.

15 Federal Trade Commission. (2021). *Truth In Advertising.* Retrieved from: https://www.ftc.gov/news-events/topics/truth-advertising.

16 Federal Trade Commission. (2022). *FTC Coronavirus Warning Letters to Companies*. Retrieved from: https://www.ftc.gov/news-events/features/coronavirus/enforcement/warning-letters.

17 Federal Trade Commission. (2023). *Federal Trade Commission Announces Proposed Rule Banning Fake Reviews and Testimonials*. Retrieved from: https://www.ftc.gov/news-events/news/press-releases/2023/06/federal-trade-commission-announces-proposed-rule-banning-fake-reviews-testimonials.

Federal Communications Commission (FCC) regulations

The FCC prohibits broadcasting false information that causes substantial 'public harm', such as about a catastrophe or crime, wherein the broadcaster is aware the information is false and will cause 'public harm' if disseminated.[18] According to FCC rules, the 'public harm must begin immediately, and cause direct and actual damage to property or to the health or safety of the general public, or diversion of law enforcement or other public health and safety authorities from their duties'.[19] Broadcasters may circumvent this rule by placing disclaimers before the information. While the FCC is prohibited by US law from censorship or suppressing free speech, it is illegal for broadcasters to broadcast false or distorted news intentionally. The FCC is authorised to take action if there are complaints, and violators may face USD 500 fines per day that the violation takes place.[20]

Proposed legislation and amendments

Proposed bills have largely focused on formulating amendments to Section 230 of the Communications Act. As of October 2023, none of the following acts have been passed.

The Health Misinformation Act: In response to a study claiming that social media platforms failed to act in 95% of COVID-19 disinformation cases, this act was proposed by US Senators Amy Klobuchar and Ben Ray Luján in 2021, and it creates an exception to Section 230 to make social media platforms liable for health misinformation.[21]

The Safe Tech Act: The Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act was first introduced in 2021 by US

18 FCC. (2021). *Consumer Guide - Broadcasting False Information*. Press release. Retrieved from: https://www.fcc.gov/sites/default/files/broadcasting_false_information.pdf.

19 Legal Information Institute. 47 CFR § 73.1217 - *Broadcast Hoaxes*. Retrieved from: https://www.law.cornell.edu/cfr/text/47/73.1217.

20 United States Department of Justice. (2020). *1068. Violation of FCC Regulations—47 U.S.C. § 502*. Retrieved from: https://www.justice.gov/archives/jm/criminal-resource-manual-1068-violation-fcc-regulations-47-usc-502.

21 U.S. Senator Amy Klobuchar. (2021) *Klobuchar, Luján Introduce Legislation to Hold Digital Platforms Accountable for Vaccine and Other Health-Related Misinformation*. Retrieved from: https://www.klobuchar.senate.gov/public/index.cfm/2021/7/klobuchar-luj-n-introduce-legislation-to-hold-digital-platforms-accountable-for-vaccine-and-other-health-related-misinformation.

Senators Mark Warner, Mazie Hirono, and Amy Klobuchar. It seeks to hold online platforms accountable for facilitating illegal activity, including the spread of misinformation, by making modifications to Section 230 immunity protections.[22]

The Honest Ads Act: This bill extends regulations on political advertising from traditional media to the digital sphere. It mandates disclosure statements for certain Internet ads and prohibits foreign nationals from purchasing political advertising. Online platforms would be required to maintain records of political ads exceeding USD 500 and display sponsor identification notices with online political ads. The goal is to prevent the spread of misleading or deceptive political content, particularly during election cycles.[23]

The Journalism Competition and Preservation Act: Introduced to address concerns related to the dominance of tech platforms in the digital advertising market, this proposed legislation aims to enable news publishers to negotiate collectively with online platforms, potentially providing a more sustainable economic model for the news industry.[24]

The Digital Citizenship and Media Literacy Act: This proposed legislation emphasises the importance of promoting media literacy and digital citizenship education in schools and communities. By integrating media literacy into educational curricula, these bills aim to equip individuals with the critical thinking skills necessary to discern and evaluate information sources, including identifying and combatting disinformation and fake news. While this legislation has not passed the Senate or the House, 18 states have passed media literacy education legislation on their own as of August 2023.[25]

22 Warner, M. (2021). *The SAFE TECH Act (Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms Act)*. Press release. Retrieved from: https://lawyerscommittee.org/wp-content/uploads/2021/02/SAFE-TECH-Act.pdf.

23 Lou, T. (2020). *The Honest Ads Act Explained*. Brennan Center for Justice. Retrieved from: https://www.brennancenter.org/our-work/research-reports/honest-ads-act-explained.

24 Congressional Budget Office. (2023). *S. 1094, Journalism Competition and Preservation Act of 2023*. Retrieved from: https://www.cbo.gov/publication/59467.

25 Furlong, J.A. (2023). *More States Are Now Mandating Media Literacy Education in Public Schools*. Ad Fontes Media. Retrieved from: https://adfontesmedia.com/states-mandating-media-literacy-education/.

Recommendations

While the United States has not reached a firm legal conclusion on the regulation of false information, it has upheld a strong free speech approach, in contrast to many other countries that have recently passed laws regulating the transmission or dissemination of false information. The European Union as a whole has taken a more proactive stance than the US in regulating disinformation since its launch of the Disinformation Action Plan in 2018 and Framework Decision 2008/913/JHA on racism and xenophobia, emphasising the importance of safeguarding democratic processes and maintaining public trust in information sources. The Charter of Fundamental Rights of the European Union guarantees everyone 'the right to freedom of expression […] to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.[26] However, restrictions are permitted if they are 'necessary in a democratic society', which can include justifications regarding national security, public safety, territorial integrity, or the prevention of disorder – disinformation could be placed in all of these categories in certain circumstances.[27] Additionally, the EU has advocated for the development of media literacy programmes and initiatives aimed at promoting digital resilience among its citizens.

However, such restrictive measures have come up against scrutiny in individual EU nations, and the measures stand in contrast to the more nuanced approach of the US, which, until present, has taken a primarily case-by-case approach as opposed to blanket legislation.

It is challenging to recommend policy approaches from the United States that may benefit the European Union, as very little has been enacted. However, the absence of these amendments or new laws, along with the strong opposition faced by those putting forth new bills to amend previous legislation or laws, speaks to a greater emphasis on preserving the foundational principles of free speech and avoiding potential restrictions that could encroach upon constitutional rights and democratic values.

26 Charter of Fundamental Rights of the European Union. Article 11.

27 ECHR. Article 10. 2.

As such, the following are selected recommendations for policymakers who are working to mitigate the effects of disinformation and decrease the flow of false information.

- Balance free speech with regulation: Emphasise the significance of upholding free speech rights while simultaneously developing targeted regulations to address specific categories of harmful content. Encourage the establishment of a framework that carefully delineates the boundaries of permissible speech, ensuring that regulatory measures do not unduly inhibit the open exchange of ideas.
- Promote media literacy education: Implementing comprehensive media literacy programmes that equip citizens with the critical thinking skills necessary to discern and evaluate the credibility of information sources is vital in all democratic societies. Prioritising educational initiatives that empower individuals to identify and counteract the influence of disinformation in the digital landscape has been developing as a priority in the United States and around the world, and it has been repeatedly shown to be more effective at mitigating the effects of false information than platform controls or censorship.[28]
- Increase collaborative cross-border efforts: It is also important to continue to foster international collaboration and information-sharing between the United States and the European Union to develop coordinated strategies for combatting cross-border disinformation campaigns.[29] Additionally, encourage joint research projects, exchange programmes, and collaborative initiatives aimed at enhancing the resilience of both societies against the spread of false information. This has been shown to strengthen societal resiliency in larger regions, and collaborative projects between UNESCO, the UN, and other organisations such as the International Center for Journalists (ICFJ) can be taken as proof of concept that coordinated efforts do, in fact, support efforts to build digital resilience and combat the global spread of false information.

28 Panakam, A. (2022). *Combating Misinformation through Media Literacy Education.* Defense360. Retrieved from: https://defense360.csis.org/combating-misinformation-through-media-literacy-education/.

29 White House. (2023). *U.S.-EU Joint Statement of the Trade and Technology Council.* Retrieved from: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/.

- Enhance digital transparency and accountability: In order to make informed decisions on mitigating false information, one must also advocate for increased transparency and accountability measures within digital platforms, including the disclosure of algorithms, data collection practices, and targeted advertising methods.[30] The implementation of clear and accessible mechanisms that allow users to understand how their data is utilised and how content is curated and disseminated across online platforms should also be supported. While federal platform regulation may not be fully the answer, total platform self-governance is also not an ideal solution, as it has not been shown to produce any meaningful changes in the flow of false information to date, and Section 230 largely shields them from broader regulatory actions.[31] There should be continued efforts for the industry to self-regulate, as has been espoused by industry analysts and experts, as such changes may come faster than any federally instituted regulations.[32] Historical examples from the film and video game industries show that self-regulation can have an effect and be successful on some level – and, as some argue, this may be the best way to begin enacting change, especially with the increased use of AI and AI-generated content. As there is often a regulatory vacuum of sorts in the early periods of newer technology, self-regulation by businesses and platforms may, in fact, be the only way forward.[33]

30 Krass, P. (2022). Transparency: *The First Step to Fixing Social Media - MIT Initiative on the Digital Economy*. MIT Initiative on the Digital Economy. Retrieved from: https://ide.mit.edu/insights/transparency-the-first-step-to-fixing-social-media/.

31 Samples, J. (2019). *Why the Government Should Not Regulate Content Moderation of Social Media*. Policy Analysis No. 865. Retrieved from: https://www.cato.org/sites/cato.org/files/pubs/pdf/pa_865.pdf.

32 Cusumano, M.A. (2021). *Social Media Companies Should Self-Regulate. Now.* Harvard Business Review. Retrieved from: https://hbr.org/2021/01/social-media-companies-should-self-regulate-now

33 Penava, E. (2023). *New Technology Will Raise New Legal Questions.* The Regulatory Review. Retrieved from: https://www.theregreview.org/2023/01/31/penava-new-technology-will-raise-new-legal-questions/.

The Role of NGOs in Building Informationally Resilient Societies in the Baltics

Dr. Solvita DENISA-LIEPNIECE,
Disinformation resilience advisor at the Baltic Centre for Media Excellence (BCME)

Dmitri TEPERIK,
Senior Policy Expert, Societal Resilience, Disinformation, Crisis Communication and Civil Security

Historically, the Baltic nations have been on the frontier of troublesome environments for several continuous decades, resulting in the formation of quite unique societal and individual cognitive patterns that combine varied feelings of anxiety, insecurity and injustice, along with vigilance, adaptability, resourcefulness and mindful consciousness.

Preserved and cultivated collective memories supported the survival of the Baltic nations through difficult times of oppression and taught valuable lessons on how to strengthen awareness of their self-identities and resist malicious interventions into their cognitive space.[1] The restoration of independence in the Baltics was also made possible because of strong civic movements and non-violent actions by organised citizens.[2] By conceptualising their survival experiences into policies and practices of nation-building and development, the Baltics have sustained the mindset of trauma-sensitive societies, which has led to security-focused thinking among the elites for the decades since the 1990s. However, the mentality of being in the 'borderlands' has not hampered transformative

1 Teperik, D. (2020). *The Challenge of Distinguishing Own From Alien. ICDS commentary.* Retrieved from: https://icds.ee/the-challenge-of-distinguishing-own-from-alien.

2 Karatnycky, A., and Ackerman, P. (2004). *How freedom is won: From civic resistance to durable democracy. Int'l J. Not-for-Profit L. 7* (2004): 47.

processes in the Baltic countries – on the contrary, the socioeconomic development of Estonia, Latvia and Lithuania has significantly accelerated,[3] and many aspects of civil society life have evolved and undergone thorough qualitative changes.[4]

The background of recent history has provided the Baltic nations a solid basis to reconsider their sociopsychological interactions as 'disruptive innovations' that strengthen societal resilience, which has become more in-demand since 2014, when the level of international hostility and violence began to grow in the region of Eastern Europe. As the Russian regime has deliberately chosen to weaponize almost every process in its domestic and international policies, the only normal predictable reaction was the securitisation of various strands of civic life, including the roles of civic society and NGOs in the national resilience of the Baltics. Any alternative would have meant surrender.

As resilience requires cross-sectoral cooperation and coordination, civil society, including NGOs, is the backbone of a whole-of-society approach. Additionally, the level of well-being of a civil society can indicate shifting interactions between democratic, populist and autocratic movements that might influence public safety and internal security.[5] In everything from official strategic documents to the rhetoric of politicians, opinion leaders and policy experts, Estonia, Lithuania and Latvia often refer to a whole-of-society approach at different levels and in different formats (including defence, security, social care, emergency planning, etc.). Moreover, resilience practices in the Baltic states share many similarities,[6] which might also indicate a very synchronised understanding of resilience and its instrumentalization, including a focus on crisis preparedness and the roles of civic society organisations in crisis responses.

3 Mole, R. (2012). *The Baltic States from the Soviet Union to the European Union: Identity, Discourse and Power in the Post-Communist Transition of Estonia, Latvia and Lithuania (1st ed.). Routledge*. https://doi.org/10.4324/9780203121498.

4 Götz, N. (2003). *Civil Society in the Baltic Sea Region (J. Hackmann, Ed.) (1st ed.). Routledge*. https://doi.org/10.4324/9781315199610.
Ruutsoo, R. (2000). *Civil Society and Nation Building in Estonia and the Baltic States: Traditions on Mobilization and Transition 1986-2000 - Historical and Social Study*. Rovaniemi, Finland: Lapin Yliopisto.

5 Hummel, S. and Graf Strachwitz, R. (2023). *Contested Civic Spaces: A European Perspective. Berlin, Boston: De Gruyter Oldenbourg*. https://doi.org/10.1515/9783111070469.

6 Kalnins, O.E. (2019). *Resilience of Necessity in the Baltics, RUSI*, Retrieved from: https://rusi.org/explore-our-research/publications/commentary/resilience-necessity-baltics.

There is a broad scope of potential functions that NGOs can have in pre-crisis and crisis environments, where a whole-of-society approach could be in high demand. Given the limitations of this chapter, it will narrow its exploration of the information environment to a general focus on communications and the cognitive dimension, thereby taking a human-centric perspective.[7]

Keeping historical developments in mind, in parallel with the constant contemporary re-building of capacities to face already existing and emerging threats, this chapter also highlights some potential challenges based on the observations of NGOs working in crisis environments. The chapter is based on an analysis of activities, interviews, reports and public events related to the non-governmental sector.

While the key role of NGOs in increasing societal resilience is to build enduring advantages against current threats, the main challenge remains being able to both forecast evolving trends and predict what is necessary for (self-) transformation. The authors acknowledge that discussing some specific activities, as well as an explicit mentioning of some actors, could make them a target for adversaries – with that in mind, the authors decided to use generalisations for sensitive projects in order to protect the initiatives and active citizens behind them, as direct references in the current hostile situation could be harmful. Nevertheless, the authors also understand that truly lasting societal resilience is enmeshed with the ability to self-repair and recover from fears of vulnerability.

Bridging recent history and current affairs

The past several months of Russia's brutal full-scale invasion against Ukraine have sped up the transformation of the role, the purpose, and the capacities of the information environment related to NGOs in the three Baltic states. Although initial changes in the information and communication space started well before the invasion, the scale of threatening new developments in the wider region has shifted the ongoing processes significantly.

In the informational and cognitive domains, the Baltic countries have been learning both individual and collective – as well as internal and external –

7 GAO U.S. Government Accountability Office. (2022), *Information Environment. Opportunities and Threats to DOD's National Security Mission*, US Air Force. Retrieved from: https://www.gao.gov/assets/gao-22-104714.pdf.

lessons from Georgia, Belarus, Moldova, and Ukraine (even before the annexation of Crimea). The post-2014 situation has heightened threat awareness, while the intensification of Russia's aggression in February 2022 has re-actualised challenges and gaps, forcing civic actors to revise their actions and to rethink their needs.[8] Some Baltic NGOs that have been actively engaging with Ukrainian partners were literally 'trying on the shoes of Ukrainian NGOs'. The war has echoes in the Baltics not just politically and socioeconomically,[9] but also in the domains of security, information and societal cohesion.[10] Moreover, civil society organisations from all over Europe, including the Baltic states, have begun a rapid adaptation to address the growing challenges on the informational frontline.[11]

With different scales of participation in terms of strengthening and supporting the development of the Eastern Partnership counties and some democratic media in Russia of that time, Baltic NGOs have made a significant contribution to the international and domestic communities of various professional fields. To illustrate this engagement: in June 2022, a few months after the full-scale invasion by Russia, the Baltic Centre for Media Excellence (BCME) supported training events for media literacy practitioners in Ukraine and beyond, and some of the Ukrainian participants indicated that they had learned the word 'resilience' from their Estonian peers several years ago.

8 Zarembo, K. (2022). *Civic Activism Against Geopolitics: The Case of Ukraine*, Retrieved from: https://carnegieeurope.eu/2022/11/30/civic-activism-against-geopolitics-case-of-ukraine-pub-88485.
Zarembo K. and Martin E. (2023). *Civil society and sense of community in Ukraine: from dormancy to action, European Societies*, DOI: 10.1080/14616696.2023.2185652.
Amdal, A.S.D. (2022). *Civilian and Private Actors' Support of Ukrainian National Resistance*, Retrieved from: https://publications.ffi.no/en/item/civilian-and-private-actors-support-of-ukrainian-national-resistance.

9 Hartwell, L. et al. (2022). *Winter is Coming: The Baltics and The Russia-Ukraine War: Implications and Policy Recommendation*, Retrieved from: https://www.lse.ac.uk/ideas/publications/reports/Baltics

10 Kuczyńska-Zonik, A. and Tomasz Stępniewski, T. (2023). *The Baltic states and new security challenges in flux*, Retrieved from: https://ies.lublin.pl/wp-content/uploads/2023/05/ies_policy_papers_no_2023-003.pdf.

11 Fivenson, A. (2023). *Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine*, Retrieved from: https://www.ned.org/shielding-democracy-civil-society-adaptations-kremlin-disinformation-ukraine.

Assessing and improving the health of NGOs

The overall sustainability of Baltic NGOs is regularly assessed using an international measurement which includes the following criteria (with multiple sub-indicators): the legal environment, organisational capacity, financial viability, advocacy, service provision, sectoral infrastructure, and public image. As of 2022, the sustainability of civil society organisations in the Baltic countries was categorised as 'enhanced'.[12] According to data from the global civil society alliance CIVICUS, Estonian, Latvian and Lithuanian civic spaces are fully open,[13] which creates favourable possibilities to exercise various freedoms and increase NGOs' engagement in strengthening societal resilience in the Baltics. Notably, the level of active citizenship (i.e. involvement in formal or informal voluntary activities) among the youth in the Baltics is comparable to the EU average (22.7%) – in Estonia it is 27.7%, in Latvia 25.9% and in Lithuania 20.4%.[14]

A total of 40% of Estonians, 40% of Lithuanians and 32% of Latvians are well-informed by civil society organisations about important issues (the EU27 average is 49%). Among the most popular types of civic engagement in the Baltics are financial donations (22% of Estonians, 22% of Lithuanians and 20% of Latvians have donated) and volunteering in various NGO activities (10% of Latvians, 9% of Lithuanians and 7% of Estonians have volunteered), and 34% of Latvians, 33% of Estonians and 27% of Lithuanians are convinced that their civic engagement has a real impact.[15]

(Re)learning some important lessons

The Baltic NGOs that have been working in and with the Eastern Partnership countries have learned a lot from Georgian, Moldovan, Belarusian, Ukrainian and Russian experiences of protecting civil society and making it more resilient

12 Family Health International, (2022). *CSO Sustainability Index for Central and Eastern Europe and Eurasia*. Retrieved from: https://www.fhi360.org/resource/civil-society-organization-sustainability-index-reports.

13 CIVICUS Monitor. (2023). *National Civic Space Ratings*. Retrieved from: https://monitor.civicus.org (last accessed 1.11.2023).

14 Eurostat online database, https://ec.europa.eu/eurostat/databrowser/view/ilc_scp19$dv_1042 (last accessed 1.11.2023).

15 European Parliament. (2020) *Civic Engagement. Flash Eurobarometer (FL4023)*. Retrieved from: https://www.europarl.europa.eu/at-your-service/files/be-heard/eurobarometer/2020/civic_engagement/report/en-report.pdf.

to various threats in the information environment. Multiple crises, including the COVID-19 pandemic, fuelled further cooperation, although in limited capacities.

When applicable, imported practical knowledge, including SWOT analysis results of the work of NGOs, has been transformed into projects to sustain societal resilience when under increasing pressure. The evidence-based overview of designing and implementing regional, local and hyper-local projects helped significantly to justify the needed costs for the donor community. Civic society actors are therefore not just making an important contribution to protecting and strengthening the information environment, but are also serving as self-motivated enlighteners for the local and state authorities and for other resilience stakeholders. There are a number of cases where Baltic NGOs served as first responders in identifying harmful content and malign actors, drawing attention to worrisome tendencies, flagging problems, and suggesting or even providing effective solutions to various governmental agencies and other interested parties.

Examples from Estonia

In Estonia, there is a shared societal agreement to contribute to the achievement of long-term national priorities – ensuring and developing a support system for citizens' initiatives, introducing a culture of cooperation based on the partnership between public authorities and citizens' initiatives, introducing good cooperation practices and ensuring their wide-scale use in practice, and actively promoting lifelong civil education.[16] A good example of a cooperative platform is a communication reserve that operates on a voluntary basis and includes specialists from across various sectors (media, strategic communications, public relations, advertising, etc.) to support the Estonian authorities in their crisis communications, including counteractions against disinformation and propaganda.[17] Strategic communication is seen in Estonia as a tool to strengthen

16 Network of Estonian Nonprofit Organizations. (2002). *Estonian Civil Society Development Concept*. Retrieved from: https://heakodanik.ee/en/estonian-civil-society-development-concept-2.

17 Sazonov, V. *et al.* (2021). *Sisekaitse personalireservid ja nende vajadus. Tallinn: Estonian Academy of Security Sciences.* Retrieved from: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2699/2021%2001%20personalireserv-WEB.PDF.

the cohesion of society, with the goal of resolving security issues using a community-based approach that involves civil society networks and volunteers, which improves the resilience of society and strengthens deterrence.[18]

Moreover, significant support is provided by Estonian governmental agencies and public foundations to several non-profit organisations that deal with the development of information resilience. For instance, the trilingual (Estonian, Russian and English) blog Propastop is aimed at contributing to Estonia's information space security. The blog is run by a group of volunteers, many belonging to the Estonian Defence League. Propastop brings to public attention deliberately disseminated lies, biased or distorted information in the media, and other cases of manipulated information. The blog was also instrumental in debunking COVID-19-related mis- and disinformation throughout 2020-21.[19] In 2023, Propastop was awarded with the European Citizen's Prize.[20]

As some shortcomings of Estonia's system have been previously criticised,[21] currently, more efforts are being invested in enhancing media and information literacy (MIL) programmes in Estonia, as there is a clear need to (re)educate various societal groups and disadvantaged audiences, with special attention paid to communication as well as training and capacity-building within the non-governmental sector.[22]

18 Spruds, A. et al. (2018). *Societal Security in the Baltic Sea region: Expertise Mapping and Raising Policy Relevance, Riga: Latvian Institute of International Affairs*. Retrieved from: https://liia.lv/en/publications/societal-security-in-the-baltic-sea-region-expertise-mapping-and-raising-policy-relevance-716.

19 ERR News. (2021). *Anti-propaganda portal: COVID-19 Facebook misinformation on the rise*. Retrieved from: https://news.err.ee/1232575/anti-propaganda-portal-covid-19-facebook-misinformation-on-the-rise.

20 BNS. (2023). *Propastop awarded European Citizen's Prize*. Retrieved from: https://news.postimees.ee/7805189/propastop-awarded-european-citizen-s-prize.

21 *Teperik, D. (2019). What Is Wrong With Our Strategic Communications? ICDS commentary*. Retrieved from: https://icds.ee/what-is-wrong-with-our-strategic-communications.

22 Mangus, A. (2021). *Kriitiline mõtlemine ja meediapädevus noorsootöös. MIHUS*. Retrieved from: https://mihus.mitteformaalne.ee/kriitiline-motlemine-ja-meediapadevus-noorsootoos/.
Sõmersalu, L. (2022). *Civic Cultures in Eastern Europe: Communication spaces and media practices of Estonian civil society organizations* (Licentiate dissertation, Södertörns högskola). Retrieved from: https://urn.kb.se/resolve?urn=urn:nbn:se:sh:diva-49483.
Blaubrük, A.-L. (2023). *Eesti õpetajate meediapädevus nende enda hinnangul ja vahend selle mõõtmiseks*. Master thesis, University of Tartu. Retrieved from: https://hdl.handle.net/10062/90382.

Examples from Lithuania

A good case from Lithuania is the Civic Resilience Initiative – a significant actor that is implementing increasingly relevant projects.[23] Founded in 2018, it has been implementing various initiatives aimed at increasing societal resilience to disinformation though educational projects in Lithuania. Another organisation frequently mentioned by Lithuanian leaders and experts in the field is 'Demaskuok' (which is mainly a fact-checking organisation) – a local success story that got international attention[24] alongside the Lithuanian 'elves' fighting Russian disinformation.[25]

The civil society sector in Lithuania, as described by communication expert Dalia Bankauskaitė, has the following main areas of activities (in terms of NGOs acting individually or in associations). 'i) their own media literacy capacity building; ii) media literacy education of their target audiences; iii) engagement in media literacy policy design, research, and resource creation'. Some entities named by the expert are the Knowledge Economy Foundation,[26] The National Network of Education NGOs,[27] and 'the NGO umbrella organization'.[28] According to Bankauskaitė, the National NGOs Coalition 'has engaged in the Strategy for Preparing Citizens for Civil Resistance' – this is an important document that shapes the consistent and comprehensive education of the public on civil resistance.[29]

In 2022, Lithuanian experts created the Baltic Research Foundation for Digital Resilience. This started as a common initiative between academia, media organisations and independent journalists with the overarching goal to detect,

23 CRI – Civic Resilience Initiative, https://cri.lt/ (last accessed 1.11.2023).

24 The Economist. (2019). *Lithuanians are using software to fight back against fake news*. Retrieved from: https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news.

25 Abend, L. (2022). *Meet the Lithuanian 'Elves' Fighting Russian Disinformation. The Time*. Retrieved from: https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/.

26 Knowledge Economy Foundation, https://www.zef.lt/ (last accessed 1.11.2023).

27 National Network of Education NGOs, https://svietimotinklas.lt/apie-mus/ (last accessed 1.11.2023).

28 National NGOs Coalition, http://3sektorius.lt/nisc/nacionaline-nvo-koalicija/ (last accessed 1.11.2023).

29 Ministry of National Defence of the Republic of Lithuania. (2022). *Seimas approves civil resistance readiness strategy*. Retrieved from: https://kam.lt/en/seimas-approves-civil-resistance-readiness-strategy/.

analyse, prevent and curb disinformation activities in Lithuania and beyond.[30] In a recent report, Lithuanian experts explore resilience as a co-production process, with new forms of collaborative actions among potential stakeholders – namely state institutions, media and culture organisations, and citizens.[31] As society's engagement in the country's security has significant potential, Lithuanian NGOs are expected to contribute to the country's total defence, including through non-violent resistance.[32]

Examples from Latvia

The Latvian civil society sector that operates in the information environment could be described as being based more on stand-alone actors rather than communities.[33] Different consortiums have been formed; however, historically, the creation of these networks was driven by the complexity of requests from donors (for example, a grant application that foresaw engagement with several local organisations). In Latvia, the Ministry of Culture initiated a networking of the NGOs related to the information environment and other relevant stakeholders, including representatives of academia and the donor community.[34] In addition to coordinating meetings, the Ministry of Culture provides updates and initiates news exchange.

Recently, attempts to make more efficient contributions by engaging with NGOs were made by the National Electronic Mass Media Council of Latvia (NEPLP). They also provided networking activities – for example, strengthening the journalistic community. Moreover, they launched a database that collects media-literacy-related content and makes it widely available.[35]

30 Baltic Research Foundation for Digital Resilience DIGIRES, https://digires.lt/en/ (last accessed 1.11.2023).

31 Balčytienė, A. *et al*. (2022). *DIGIRES: Multisectoral and Multistakeholder Foresights Towards Resilient Digital Citizenship in Lithuania*. Retrieved from: https://digires.lt/wp-content/uploads/2023/01/Digires-report-final_n.pdf.

32 Bankauskaite, D. and Šlekys, D. (2023). *Lithuania's Total Defense Review. PRISM 10, no. 2 (2023)*: 54–77. https://www.jstor.org/stable/48718173.

33 Denisa-Liepniece, S. (2016). *The case of Latvia, an EU member state at the border with Russia*. In: Resisting States Propaganda in The New Informational Environment: The Case of the EU, Russia, and the Eastern Partership Countires. Brīvības Solidaritātes Fonds. pp. 223–294.

34 Media literacy database, https://datubaze.neplp.lv/datubaze/ (last accessed 1.11.2023).

35 The National Electronic Mass Media Council, https://www.neplp.lv/lv (last accessed 1.11.2023).

A significant newcomer is the strategic communication department within the State Chancellery, whose presence in the field is growing.[36] This entity has also facilitated the adoption of the first National Concept on Strategic Communication and Security of the Information Space 2023–2027. According to the document, 'partnership with the organised civil society and private and academic sectors is one of six key action-lines to strengthen the security of the national informational space'.[37]

Within the general NGO–state cooperation platform (the annual forum of parliament and NGOs), only few sections have been dedicated to the information environment, including one on media literacy in 2017. As of 2023, during the 15th forum entitled 'Safe in our Latvia' (*Droši savā Latvijā*),[38] when discussing how to support Ukraine, participants drew attention to the removal of a Russia-related organisation from the lists of recipients that can be financed from Latvia's state budget.

The procedure suggested by the head of the commission was to request any information to prove a link. Changes in legal norms were mentioned as one of the concerns and challenges, which may result in more sophisticated bureaucracy. Notably, one of the suggestions to fund initiatives fighting disinformation was to include them under the category of 'development cooperation projects'. While setting priorities, the participants also mentioned the representation of Latvian NGOs in the international arena.

Baltic NGOs in building partnerships

In the report on media literacy initiatives in the Baltic countries that was recently published by the BCME,[39] the significant role of NGOs was mentioned

36 Strategic Communication and Security of the Information Space, https://www.mk.gov.lv/en/stratcom (last accessed 1.11.2023).

37 Cabinet of Ministers. (2023). *The National Concept on Strategic Communication and Security of the Information Space 2023–2027.* Retrieved from: https://www.mk.gov.lv/en/media/15446/download?attachment.

38 The Parliament of Latvia. (2023). *Saeimas un nevalstisko organizāciju sadarbība*. Retrieved from: https://www.saeima.lv/lv/sabiedribas-lidzdaliba/sadarbiba-ar-nvo/.

39 Baltic Centre for Media Excellence. (2022). *Media Literacy Sector Mapping in Estonia and Lithuania. With Media Literacy Towards Cognitive Resilience*. Retrieved from: https://bcme.eu/en/our-work/media-literacy/report-media-literacy-sector-mapping-in-estonia-and-lithuania-and-the-policy-brief-with-media-literacy-towards-cognitive-resilience-2.

in terms of their promoting and raising awareness, carrying out activities, creating communities, and providing spaces for networking. In states where trust in the government and state institutions remains unstable or critically low, such reliable partners are highly needed.

Despite the inevitable differences between national structures of and approaches to the engagement of the governmental sector and civil society in the Baltic states, the limited resources of all parties motivates stakeholders to seek and exercise various forms of cooperation domestically as well as internationally. For many Baltic NGOs, foreign donors remain one of the leading agenda-setters in the information environment by suggesting roadmaps for grants, supporting short-term and long-term cooperative projects, and underlining the need for monitoring and evaluation. As presumably the exit strategies of some foreign donors might inhibit pan-Baltic cooperation between NGOs, special support measures should be introduced in a timely manner. Long-term European funds are required to empower civil society in Estonia, Latvia and Lithuania for collaborative innovations.[40]

The recent tendency among donors is to see the region as a whole by creating a hub or several hubs to work with resilience stakeholders through the formation of local partnerships. To mention just a few, these include the multi-year media literacy project by IREX,[41] Internews,[42] and recently launched Google initiatives across the region.[43] Another new Baltic entity is the Baltic Engagement Centre for Combatting Information Disorders (BECID), which is a pan-Baltic network of experts working to combat information disorders and promote media literacy.[44] Nevertheless, there are still some minor obstacles to

40 Interreg Baltic Sea Region Programme. (2023). *We make transition! Towards sustainable and resilient societies through empowered civil society and collaborative innovation*. Retrieved from: https://interreg-baltic.eu/project/we-make-transition-interreg-baltic-sea-region/. (last accessed 1.11.2023).

41 IREX. Media Literacy in the Baltics, https://www.irex.org/project/media-literacy-baltics (last accessed 1.11.2023).

42 Baltic Centre for Media Excellence. (2022). Retrieved from: https://bcme.eu/en/our-work/research/open-tender-for-external-evaluation (last accessed 1.11.2023).

43 Baltic Centre for Media Excellence. (2023). *Baltic Centre of Media Excellence signed a long-term partnership and cooperation agreement with Google*. Retrieved from: https://bcme.eu/en/our-work/media-literacy/baltic-centre-of-media-excellence-signed-a-long-term-partnership-and-cooperation-agreement-with-google.

44 Baltic Engagement Centre for Combating Information Disorders (BECID), https://becid.eu/ (last accessed 1.11.2023).

be overcome in terms of reducing the competing, non-cooperative attitudes of some governmental and non-governmental organisations in the Baltics that do not share the understanding of all three countries being actually in the same boat, not just geographically but also in terms of common security, socio-economic, and sociopsychological challenges.

Major challenges

Baltic NGOs that operate in the information domain face an increasingly complex and competitive environment. Among other main challenges, the *Disinformation and Civil Society Mapping Report* listed the gaps in and needs for financial stability and effective communication skills.[45] The intensification of hostile activities in various conflict zones increases the risk of weakening financial flows from abroad, which makes it important to attract state-related funding, including in the Baltics. At the same time, a review of the necessary capacities highlights the importance of communication.[46] The media literacy environment should adapt accordingly by creating a collective immune system.[47]

Furthermore, some challenges still need to be addressed through cross-sectoral synchronisation and operational improvements in the planning and implementation of MIL-related curricula in formal and informal education (the latter of which is provided mostly by civil society organisations). As the so-called 'traditionalistic' branch of the media community does not particularly welcome the fact of MIL securitisation; there are still some issues to be discussed, clarified and commonly agreed upon in order to properly set the instrumental objectives of MIL education and conduct respective trainings in the Baltics, both in terms of youth education and ongoing lifelong learning and upskilling.[48]

45 Baltic Region. Disinformation and Civil Society Mapping Report. (2023). Retrieved from: https://www.techsoupeurope.org/wp-content/uploads/2023/09/TechSoup_Disinformation-and-Civil-Society-Regional-Mapping-Report_Baltic_Region.pdf.

46 Swedish Civil Contingencies Agency (MSB). (2023). *Building resilience for the future. Lessons from Ukraine*. Retrieved from: https://rib.msb.se/filer/pdf/30449.pdf.

47 Denisa-Liepniece, S. (2023). *From media literacy to cognitive resilience*. Centrum Balticum. Retrieved from: https://www.centrumbalticum.org/en/publications/baltic_rim_economies/baltic_rim_economies_2_2023/solvita_denisa-liepniece_from_media_literacy_to_cognitive_resilience.

48 Maarit Jaakkola, M. (2020). *Editor's introduction: Media and information literacy research in countries around the Baltic Sea. Central European Journal of Communication. Volume 13 No 2 (26) Special Issue 2020. DOI: 10.19195/1899-5101.13.2(26).1.* Retrieved from: https://cejc.ptks.pl/attachments/cejoc132-1-4-19_2020-06-24_09-10-52.pdf.

Additionally, there is a lack of a general strategy for dealing with complex threats and an evidently less-predictable future. Such a strategy should ideally be a multi-stakeholder endeavour by nature and could be implemented vertically (top-bottom or bottom-up) as well as horizontally. For a bottom-up approach, there are inconsistencies in political will, complexities related to giving foreign actors agenda-setting priority, and, most importantly, the need to be up-to-date about plausible risks and incoming threats. A 360-degree situational awareness is possible only if civil society organisations contribute to it.

As there are no trustable signs about a reduction of authoritarian hostilities in Europe's neighbourhood and in the Baltic region, ill-intentioned proxies must be considered as malicious actors who weaken societal resilience domestically and internationally. Since they can use any sociopolitical disagreement or ideological difference as a vulnerability against the self-identities of various groups of free citizens, the motivations, flexibility and creativity of civil society organisations can be features for the further strengthening of national cohesion and of the capacity to resist malign influences and preserve the democratic order in the Baltics.

Moreover, unhealed sociopsychological traumas can last generations. They can create 'civil casualties' that are often overlooked by history. Since group (self) victimisation does not help in the longer-term, transparency, thoughtfulness and prudence are required to advocate and advance societal reconciliation. Civil society organisations can play a vital role in promoting an actual sense of belonging and making it stronger than any perceived fear of rejection.

Embedding a security culture

To move forward with such a combination of multiple threats, the further development of a security culture is needed. A security culture should be implemented on every organisational level, keeping in mind the risks, problems and consequences if a network is compromised by its the weakest link. NGO leadership is the first layer to be addressed, trained and prepared. Yet without a whole-organisational approach, situational awareness cannot be achieved. This is why it is essential not only to train the leaders, but also to endorse and enable the transmission of knowledge within an organisation. Furthermore, if

not properly informed and trained – and/or if simply overwhelmed by day-to-day challenges – some NGO members might move security-related issues out of the agenda, thereby creating additional vulnerabilities in their blind spots.

Implementing the BEACON model of societal resilience can potentially accelerate the embedment of a security culture in Baltic NGOs. The model emphasises systematic and timely actions and preparations, including in the areas of conducting emergency trainings, recognising patterns of targeted communications, creating procedures of crisis management, enacting mechanisms of civic mobilisation, analysing actors with multiple identities, providing rationales for work with disadvantaged audiences, reinforcing weak socio-psychological connections, establishing new cooperation networks, etc.[49] The model is a useful tool to regularly evaluate the current state of affairs and to foresee weaknesses that might be exploited by an adversary and/or its proxy, including within civil society sphere.

Uncertain threat landscape

While it is natural to focus on identifying and learning lessons, as well as gathering any relevant experiences from crises, the necessary mindset for resilience is not solely retrospective but rather future-oriented. Even if some patterns of influence remain the same, new tools and techniques could be used to weaken or harm societies. In other words, some actions, goals and targets of adversaries can (and most probably will) mutate from one episode to another.

By all means, NGOs that operate in the information environment should be better-equipped to make projections about dangerous actors and threats in the information space and in the cognitive dimension. Moreover, the leadership of NGOs should accept and embrace the complexity of these processes and must acquire flexibility in their actions.

For instance, flexibility and creativity allow non-governmental actors to use more innovative tools to combat disinformation – for example, using humour in communications helps to build the resilience of one's own audience, impose

49 Teperik, D. (2023). *The BEACON model for resilience building in the Baltics: key lessons to learn from Ukraine. The Riga Conference Policy Brief.* Retrieved from: https://rigaconference.lv/wp-content/uploads/2023/10/LATO_Broshura_5_2023_Teperik-WEB.pdf.

more costs on the aggressor, and spread important messages across various audiences.[50]

Looking into society – early warning

An overly excessive focus on external threats in information domains could damage the balance of situation awareness if some dangerous domestic processes are deliberately ignored or remain overlooked by accident or ill-designed procedures. Foreign soft power has the danger to mutate into sharp malicious influence in countries where resilience is significantly weakened by societal diseases like corruption, populism, nationalism, polarisation, discrimination, disinformation, etc. Given all the differences between societies, no universal prescription exists, but some behavioural attitudes and a forward-looking mindset can help to improve the overall health of a society. The Baltic countries can become trendsetters in cultivating and implementing this mindset across various sectors, including in civil society organisations.

Resilience relies on ensuring the harmonious coexistence of personal, group, community and national identities. Therefore, proper crisis preparedness (and later recovery) requires early warning about and the early de-conflicting of major socio-political and socio-psychological issues. To avoid unpredictable consequences of the butterfly effect in the future, every move matters now.

By their nature, NGOs form a unique opportunity for having a deeper look at local and hyper-local issues through establishing more trusted access to communities that can be frequently overlooked when relying on general qualitative data. Having access to various unspotlighted communities can be used to verify data gathered solely with technological solutions (such as monitoring tools and surveys). It can be especially important in regards to data about disadvantaged audiences as a way to add another layer of quality for more accurate interpretation. Proper audience analysis with the regular re-evaluation of NGO activities would be helpful to coordinate financial and informational support for the targeted regions and communities.

50 Giles, K. (2023). *Humour in online information warfare: Case study on Russia's war on Ukraine. The European Centre of Excellence for Countering Hybrid Threats*. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231106-Hybrid-CoE-Working-Paper-26-Humor-to-combat-disinformation-WEB.pdf.

Information security as a part of national defence should be co-owned by a range of players – state institutions, government agencies, local authorities, media organisations and civil society organisations. Civil society organisations can be reliable partners in designing policies to address the issues that disadvantaged audiences can face, and they should be better utilised in shielding those groups from foreign malignant influence activities.[51]

Awareness of blind spots

Based on interviews with the implementers of a project aimed at strengthening societies, a massive challenge donors can be formulated. Extending and engaging in all possible activities is hardly imaginable. One of the most critical tasks is to explore and reach disadvantaged audiences. The profiling of groups and evaluations of activities seem to be difficult to prioritise over other duties.

At the same time, by zooming in and out, blind spots can be noticed and then thoroughly studied in order to motivate NGOs to include new audiences in their programme of work and to find a suitable format for these engagements. The same applies to profiling any specific audience. While using digital-media focused monitoring tools, there should also be an awareness about citizens who are getting new knowledge in different forms. Additionally, the issue of data governance and management within and between NGOs should be professionally addressed in cooperation with experts from the fields of cyber and information security, human rights, and applied ethics.

Policy recommendations

Given its natural features, civil society is an indispensable actor and a vitally important stakeholder in the resilience landscape in any democratic society that desires to protect human rights and ensure sustainable development for its citizens. Therefore, NGOs are an integral part of any resilience ecosystem that can be characterised by the following keywords: flexibility, networking, complementarity, consciousness and professional dedication.

51 Teperik, D. *et al.* (2022). *Resilience Against Disinformation: A New Baltic Way to Follow? Research report. Tallinn, Estonia: International Centre for Defence and Security.* ISBN 978-9916-709-03-0 (pdf). Retrieved from: https://icds.ee/en/resilience-against-disinformation-a-new-baltic-way-to-follow.

Nevertheless, trust-based engagement policies for non-governmental stakeholders are still an important growth area to enhance mutually beneficial competencies by co-sharing the infrastructure of various sectors, thereby contributing to public safety and the information security of national matters in the Baltics.

Forward-thinking culture

Future-oriented agility and forward-thinking requires creating a prognostic culture. The goal of strengthening the NGO community involves building trust with their main client and the source of their energy and inspiration – society itself. Trustworthy interactions should demonstrate flexibility and agility while serving society and understanding its complexity. In addition to flexibility, the rapidity of decision-making within top-bottom and bottom-up approaches will remain a necessity in order to provide timely and accurate information on how everyone can contribute and prepare, or on how not to interfere for those who are unprepared or unwilling to assist. Local key organisations should be considered as potential focal points for protecting the information environment. Operational training for relevant NGOs should be implemented to connect the key actors and synchronise their vocabulary, plans and recourses.

Securing the multifunctionality of facilities

Although the focus of discussions around the NGOs lays in the prospect of management, additional consideration should be given to supporting the cross-usage of multiple facilities used as physical spaces. If necessary, these venues could serve the needs of community resilience, providing access to generators, first aid kits, and other important supplies for emergency and trauma care (also known as 'WASH facilities'). An additional task for such venues could also be the preservation of local critical data and cultural heritage to ensure the safety of such information, both in analogue and digital formats, as well as other valuable artifacts.

Resilient staff who are willing to protect and defend

Experts and practitioners who deal with information analysis and communication risks can experience various threats, including hate speech. Coordinated efforts to increase (and not to diminish) their will to protect and defend the information environment are crucial. NGO staff work occasionally with some traumatised audiences, including, for example, journalists and refugees. Moreover, NGOs that operate in the information environment can become the target of dis- or malinformation campaigns or other types of influence operations. Psychosocial support is needed at different levels within NGOs, as well as across cooperation networks. Frequent first responders and their partners must be aware of the consequences of unhealed socio-psychological traumas.

Resilient networks

A growing sense of uncertainty among people damages the social fabric, which can be repaired only by more intergroup connections based on mutual trust and shared values. Instead of emphasising disagreements and distancing people from each other, opinion leaders within civil society should maintain hope for and grow confidence in a better future.

While the importance of building in-country or regional cooperation formats is being addressed, supporting inter-regional (e.g. Baltic–Balkan) as well as EU-wide and transatlantic cooperation for NGOs should also be considered as a priority with long-term goals. Moreover, the Baltic countries have a good potential to initiate and lead the transatlantic debate on fostering a practical understanding of civil society under conditions of digital mediatisation.[52] Additionally, the experiences of Baltic NGOs can be instrumental for discussing innovative approaches to conceptualising MIL within the strategic defence posture.[53]

52 Bakardjieva, M. *et al.* (2021). *Digital Media and the Dynamics of Civil Society: Retooling Citizenship in New EU Democracies*. Rowman & Littlefield International.

53 Jolls, T. (2022). *Building Resiliency: Media Literacy as a Strategic Defense Strategy for the Transatlantic A State of the Art and State of the Field Report*. Center for Media Literacy. ISBN: 978-1-879419-12-4. Retrieved from: http://www.medialit.com/sites/default/files/announcements/FinBuilding%20Resiliency-Media%20Literacy%20as%20a%20Strategic%20Defense%20Strategy%20for%20the%20Transatlantic%20%28Final-10-5-2022%29%20copy.pdf.

The role of this mixed-format approach in crisis situations could be to amplify information. Therefore, NGOs should be equipped to deliver verified messages to international audiences and to support informational efforts to appeal for necessary aid. For this purpose, NGO staff should be trained on how to create audiovisual content during a crisis, as well as how to share that content with news agencies and other important stakeholders domestically and internationally.

Since the cognitive domain includes the human mind (ideas, ideologies, functions, reasons, will, spirit, morale, etc.), winning the great battle of narratives and perceptions requires building an investment roadmap in cognitive capacity, capabilities, and expertise.[54] The future of truth depends on the success of resilience-oriented efficient cooperation between the key stakeholders: state and local authorities, private businesses, and civil society. The latter must foster empathy and hope for a better future, which are indispensable for the sustainable maintenance of societal resilience in the Baltics.

54 Haugland, E.L. (2023). *The Cognitive War: Why We Are Losing and How We can Win*. United States of America. ISBN 979-8856908731.

The Role of CSOs in Building a Resilient Society: The EU Perspective

Magdalena WILCZYŃSKA,
Subject Matter Expert on Countering Disinformation,
TechSoup Europe

Disinformation is a custom-made approach to polarising society by instilling a fear of others and undermining values, democracy, and human rights, as well as the structures that support them. In the European Union, a crisis of values has been apparent for years, with countries like Poland and Hungary departing from the so-called liberal democracy model. Civil society has been actively working for years to counter these phenomena. However, the problems that society faces remain almost unchanged, while the social need to take action is growing.

A brief overview of historical developments and the current situation

Over the last decade, issues related to the information sphere have undergone very significant and quite unprecedented changes. In 2015, during the so-called refugee crisis, the main problem was hate speech, and the idea of fighting disinformation was only starting to enter people's consciousness. However, the war on hate was already ongoing in 2015 – we had a legal framework set out in criminal law, and although the scale of hate speech on the Internet wasimmense, countermeasures had been available and used for years. These included: anti-discrimination education, training for judges and prosecutors, and the implementation of effective mechanisms for identifying the perpetrators of hate crimes, and access for prosecutors to private indictments. And even despite all the countermeasures already in place, the problem still persists today, and one might argue it is bigger than ever before.

Less than 10 years ago, problems with the flow of information on the Internet began to be researched differently – as a problem of (initially) fake news, and then of misinformation and disinformation. The issue was posed in a way that led to the categorisation of different threats.

The first threat identified was disinformation originating from foreign sources, also known recently as Foreign Information Manipulation Interference (FIMI).[1] These attacks were initially contained within the realm of cyber-security, special services, and international alliances such as NATO. FIMI was recognised as an act of hybrid war, and as an early response by NATO, in 2014 (the year Russia invaded Crimea), NATO Strategic Communications Centres were established.[2] Disinformation spread by foreign actors was later used by local actors such as politicians, leaders of anti-vaccine groups, and nationalist movements. Local actors have started using this type of disinformation, particularly narratives that target minorities and vulnerable groups, which led to the localisation of disinformation. This kind of content is then taken directly from the depths of the Internet and spread to the mainstream media. Local disinformation used for profit, political gains or social gains is extremely dangerous because it can be spread by people the public knows and trusts.

There is also a third category to be aware of: misinformation, which involves the spread of manipulative or false content by 'ordinary' people who have come to believe untruths. It is crucial to understand that various forms of disinformation and misinformation require distinct approaches when it comes to tackling them. Nevertheless, all of them share a similar underlying issue: people are struggling to distinguish between facts and fiction. This is causing polarisation on important matters and creating divisions within societies.

In recent years, disinformation research has played a small role in the growth of civil society. Several organisations have been established to conduct research and educational activities aimed at combating the spread of 'fake news'. Initially, these organisations focused on publishing articles to verify the accuracy of information. However, this approach was inadequate in the fight against disinformation. As a result, educational initiatives were launched to promote

1 EEAS. (2023). *Beyond Disinformation - What is FIMI?* Retrieved from: https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en.

2 NATO StratCom. *About Strategic Communications.* Retrieved from: https://stratcomcoe.org/about_us/about-strategic-communications/1#:~:text=NATO%20Strategic%20Communications%20is%20the,order%20to%20advance%20NATO's%20aims.

media literacy, critical thinking, fact-checking, and the countering of false narratives. These efforts are crucial, but they only offer a partial solution.

In order to strengthen their position, fact-checking organisations have established networks, such as the International Fact-Checking Network[3] or the European Digital Media Observatory,[4] and research and publication standards, such as the European Fact-Checking Standards Network.[5] These measures have significantly improved the credibility of these organisations among wider audiences. Nonetheless, fact-checking still only reaches a small part of the public. Only a few years after the civil society response, the EU started to work with platforms on self-regulation, starting with the EU Code of Practice on Disinformation in 2018.[6] The Code's signatories committed *inter alia* to partner with civil society organisations to support efforts aimed at improving critical thinking and digital media literacy, as well as to support the efforts of Chief Security Officers (CSOs) to track and understand disinformation, including by sharing privacy protected datasets and undertaking joint research. However, accessing data from platforms remains a problem even now.

Parallel to the development of the fact-checker community, organisations dealing with so-called OSINT (open-source intelligence) began to emerge, such as the Bellingcat, which was founded in 2014, or the DFRLab, which has been incubated by the Atlantic Council since 2016. As the problem spread around the world, the 2018 Global Disinformation Index was created in an attempt to address the scale of the phenomenon. Moreover, in 2018, researchers at MIT published results[7] showcasing that false information spreads online six times faster than true information. Moreover, it was pointed out that those responsible for this are not, as was previously thought, bots and troll farms, but rather ordinary users. This meant that the problem of misinformation is responsible for much of the problems on the Internet. Therefore, many organisations at the

3 International Fact-Checking Network. Empowering fact-checkers worldwide. Retrieved from: https://www.poynter.org/ifcn/.

4 European Digital Media Observatory. Retrieved from: https://edmo.eu/.

5 European Fact-Checking Standards Network. Retrieved from: https://eufactcheckingproject.com/.

6 European Commission. (2022). *2018 Code of Practice on Disinformation*. Retrieved from: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

7 Dizikes, P. (2018). *Study: On Twitter, false news travels faster than true stories*. MIT News. Retrieved from: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

time promoted fact-checking education, urging people to verify information by themselves. These attempts were only partially successful, as most users do not take such action (and most likely never will).

The prevalence of disinformation, particularly coming from Russia, was already evident across the Internet before 2019, but it was not until the COVID-19 pandemic that it was recognised as a major global issue and infodemic.[8] False information about the virus, its origin, treatment, and vaccination spread much faster than true information, posing a significant threat to public health on a societal and global level. Only then were CSOs' monitoring, investigative and educational responses combined with legislative measures and policy, state-based counter-disinfodemic measures, and technological or economic responses (which are relevant to the policies and practices of institutions mediating content).[9] More funds were allocated to organise fact-checkers and CSOs, but their effectiveness was limited by the mostly online format used during the pandemic. The pandemic period and the subsequent outbreak of war in Ukraine caused a spike in disinformation in the European infosphere.

Despite that, strong legal action at the EU level was not introduced until 2022, with the publication of the Digital Services Act (DSA) and the sanctions imposed on Russia and the blocking of Russian media. CSOs that have been dealing with disinformation for years have emphasised the need to regulate online platforms as well as work with the public at the grassroots level to build positive narratives. The focus is not only on countering false narratives but also on building a positive image of groups and issues targeted by disinformation, such as the LGBTQ+ community, women's rights, or migrants. Fact-checking is undoubtedly important, but it alone cannot solve the problem of disinformation. While education can play a role, it has its limitations, and imposing top-down restrictions (like the removal of content by social media platforms) can often be perceived as censorship. Therefore, the most effective way to combat disinformation is not only to identify and remove malicious content, such as hate speech, but also to work with people to mitigate the negative consequences of disinformation, such as deepening polarisation and eroding social trust.

8 WHO. *Infodemic*. Retrieved from: https://www.who.int/health-topics/infodemic#tab=tab_1.

9 Posetti, J. and Bontcheva, K. (2020). *DISINFODEMIC. Dissecting responses to COVID-19 disinformation*. United Nations Educational, Scientific and Cultural Organization. Policy brief 2. Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000374417.

Analysis of the main challenges

Disinformation has become increasingly prevalent and diverse, covering a range of socially significant topics such as the rights of the LGBTQ+ community, women, migration, climate change, war, health, and security. As a result, most CSOs have to contend with disinformation in some capacity. This is particularly true for CSOs that work with refugees or other vulnerable groups. As part of its research work[10] in 14 European countries, TechSoup, together with local partners from all over Europe, collected insights from activists and representatives from various non-governmental organisations regarding the challenges they face in their daily work. Various common problem areas were identified in all four regions where the research was carried out (the Baltics, the Black Sea region, the Western Balkans and the Visegrad region).

Funding

Financial stability remains a significant challenge for most organisations in every region. Persistent issues relate to financing, notably the lack of funding for long-term activities, which often results in project-based approaches. Consequently, organisations grapple with financial instability and precarious employment arrangements for activists. Donor-provided funds are earmarked for specific purposes and cannot be utilised for internal organisational needs, such as developing administrative structures or acquiring new equipment. This funding framework constrains the exploration of more innovative activities, restricting organisations to primarily replicating past initiatives, often with limited effectiveness.

Human resources

Organisations in all four regions face common challenges related to staff rotation and the lack of qualified personnel. Large staff turnover (due to low salary rates) often results in a loss of institutional knowledge. Most CSOs work

10 Hive Mind. (2023). *Decoding Disinformation: Navigating Civil Society Challenges in CEE - Disinformation and Civil Society Regional Mapping Reports*. Retrieved from: https://en.hive-mind.community/blog/500,decoding-disinformation-navigating-civil-society-challenges-in-cee-disinformation-and-civil-society-regional-mapping-reports.

with young, inexperienced individuals who require training in various skills such as project management, communication, and fundraising strategies. This chronic need for qualified human resources affects the quality of work done by CSOs in the four regions.

Effective communication

Communication presents a great challenge in the researched regions. In the Baltics, the struggle lies in crafting compelling narratives and effectively communicating messages to engage the public and stakeholders. The Western Balkans, in particular, confront the arduous task of effective communication, given the governments' tight control over public discourse. CSOs addressing sensitive topics are often labelled as 'foreign agents' or 'traitors'. In the Visegrad region, notably Hungary, maintaining long-term communication efforts is problematic due to the pervasive influence of government messaging and openly anti-CSO campaigns.

Relationship building

Activists face unique challenges when it comes to building and sustaining relationships with various actors and institutions. In the Baltic region, CSOs have identified a need for training in effective communication and collaboration with the media and other organisations. Despite the potential benefits to all parties involved and their connections with communities, there is a lack of effective cooperation between CSOs. In the Western Balkans, civil society organisations face an uphill battle in building trust with their audiences, particularly around polarising topics and disinformation campaigns. CSOs must establish their credibility and undertake positive campaigns to foster trust and citizen involvement while understanding the needs of society. The Visegrad region experiences competition among CSOs, hampering cooperation. Enhanced collaboration between CSOs could benefit all parties and improve relationships within the activist community. Similarly, in the Black Sea region, trust-building is complex, especially over polarising or disinformation-targeted topics. Fostering trust involves encouraging citizens to engage in addressing local issues and needs. Addressing these shared concerns is vital for bolstering the effectiveness and impact of civil society organisations in these regions.

Boosting countering disinformation

CSOs across the Baltics stressed the importance of continued professional development to combat disinformation. They highlighted the need to enhance their ability to monitor and track disinformation campaigns across various platforms and languages. Knowledge of fact-checking tools is also crucial due to developments in the ever-evolving field of data analysis. In the Western Balkans, CSOs lack the organisational and financial capacity to effectively respond to disinformation. They would benefit from stronger cooperation with other CSOs that specialise in countering disinformation. The region also lacks a decision matrix to measure the depth and intensity of disinformation, which hinders their ability to respond effectively. The Visegrad region faces a need for greater organisational and financial capacity to counter disinformation. An early warning system was identified as a valuable tool to prepare for crises resulting from disinformation, such as the migration crisis. Romania, Bulgaria, and Moldova in the Black Sea region are under constant threat from disinformation campaigns. These affect the fieldwork of CSOs and undermine public trust. Vulnerable groups that CSOs work with, such as refugees and ethnic minorities, are often targeted, posing risks of social unrest and violence.

Digital transformation

CSOs in the Baltics are emphasising the significance of building positive narratives and acquiring digital skillsets. The region faces challenges in terms of accessing digital tools for data visualisation, graphic design, and video editing. Moreover, they have difficulties with maintaining an effective online presence and with developing a comprehensive digital transformation strategy. In the Western Balkans, CSOs require knowledge about fact-checking tools and critical thinking skills that can be useful in their work, especially due to the constant changes in the field of data analysis. In the Visegrad region, activists underlined that digital transformation is crucial for CSOs to become more efficient, effective, and transparent. Resources and trainings are required for a successful digital transformation. Similarly, CSOs in Romania, Bulgaria, and Moldova mentioned the need to embrace digital transformation to improve their daily operations, data storage, and project management. However, they require additional skills and resources to implement this transformation completely.

Strategic planning

In Kosovo, the majority of CSOs have a highly trained and professional staff. However, they lack the necessary skills for developing strategies, collecting data, and effectively implementing fundraising activities. A common weakness among regional CSOs in Kosovo is a lack of strategic planning. They tend to focus on short-term projects and activities, neglecting longer-term ones. Due to limited resources for campaigns, their capacities to respond effectively to crises are further reduced. On the other hand, in the Visegrad region, only larger organisations have the capability to build and implement crisis communication strategies. These organisations have clearly defined target audiences and messages in their crisis communication strategies.

Policy recommendations

To combat the problem of disinformation in the European Union, a comprehensive approach is required. Our research went further than the EU's borders, but challenges still remain. The crucial issue in disinformation responses is to support CSOs that are already working in the field. By learning from past responses and identifying necessary improvements, we can offer effective policy recommendations to empower policymakers and stakeholders to address the issue.

Firstly, policymakers must prioritise and expand digital literacy and media education programmes to counter disinformation effectively. These initiatives should span all EU member states and target individuals of all age groups. The focus should be on nurturing critical thinking skills and the ability to distinguish between credible sources and unreliable ones, while also addressing polarisation and fears within societies.

Further policy support for existing fact-checking organisations like the International Fact-Checking Network and the European Digital Media Observatory is essential. These entities play a pivotal role in ensuring access to verified information and analysing ongoing trends in the region. Collaboration among civil society organisations is also crucial. These partnerships should act as platforms for sharing best practices, pooling resources, and devising effective

strategies for countering disinformation (understood also as strengthening their resilience, building positive narratives, and creating effective digital safety and security strategies), with the primary goal of enhancing the capacity of these organisations to respond proactively to disinformation while fostering trust within communities.

The creation and implementation of early warning systems should be a joint effort between policymakers and civil society organisations. These systems should be capable of detecting disinformation campaigns at their inception, enabling swift and effective responses. Their importance becomes evident when pre-empting crises triggered by disinformation, particularly those that affect vulnerable groups.

Policymakers must provide support for the digital transformation of civil society organisations, including the allocation of resources, comprehensive training, and access to the necessary tools for adapting to the evolving digital landscape. This adaptation includes mastering data visualisation, graphic design, video editing, and strategies for maintaining a robust online presence.

Conducting a comprehensive review of funding mechanisms for civil society organisations is an imperative. Reforms should focus on securing greater financial stability and flexibility, as well as catering to internal organisational needs, including administrative development and equipment upgrades. Policymakers should also explore innovative funding models that encourage experimentation in countering disinformation.

Championing initiatives that extend beyond countering false narratives is vital. Policymakers should promote positive images for groups targeted by disinformation, including the LGBTQ+ community, women, and migrants. The promotion of values such as tolerance, empathy, and inclusivity in public discourse can significantly mitigate the impact of divisive disinformation campaigns.

The European Union should ensure the common implementation of the DSA and develop a robust regulatory framework for online platforms. This framework must prioritise transparency and accountability in content moderation. Additionally, it should include clear mechanisms that foster cooperation between online platforms and civil society organisations to effectively track and address disinformation, such as common and transparent regulations for trusted flaggers (fact-checking organisations).

Summary

In conclusion, the battle against disinformation is a multifaceted challenge that demands a united and comprehensive effort to counter or mitigate its negative effects. As disinformation continues to threaten the values of democracy and human rights upon which the European Union is founded, the role of civil society organisations becomes increasingly vital. From a historical perspective, we've seen the evolution of this issue from the early stages of hate speech and foreign-sourced disinformation to its localisation and the proliferation of misinformation. The COVID-19 pandemic and the infodemic that accompanied it exposed the urgent need for combined efforts, both in terms of monitoring and policy response. While fact-checking organisations and open-source intelligence entities have made significant contributions, the adoption of strong legal measures at the EU level, such as the Digital Services Act, marks a pivotal step forward. However, addressing the challenge of disinformation goes beyond mere fact-checking and regulation. It necessitates proactive engagement with citizens and a nurturing of trust among societies. By heeding the policy recommendations outlined here, policymakers can equip the European Union to tackle this issue comprehensively and construct a more resilient, well-informed society.

The Role of NGOs in Building a Resilient Society: The US Perspective

Maya SOBCHUK,
Thomas J. Watson Fellow

In a 2021 white paper, the US Cyberspace Solarium Commission noted that American trust in their mediascape is quickly eroding: 'in 2000, 12 percent of the adult population in the United States rated their trust level in mass media as "not at all"; by contrast, 51 percent had either a great deal of trust or a fair amount of trust. In 2020, 33 percent of American adults had no trust in mass media, while only 40 percent had a great deal or fair amount of trust'.[1] The rise of disinformation and the American public's gradual awareness of it is certainly driving this shift toward distrust. It is chipping away at American democratic institutions and societal cohesion. Non-governmental organisations (NGOs) are key actors in combatting this issue in the United States – and although there is certainly room for improvement, they have helped make progress in this domain. This article will provide an overview of the current and historical civil society landscape of countering disinformation in the United States, note the major players, analyse the main challenges in this fight, and provide policy recommendations to better build societal resilience to this ever-growing threat.

Often regarded as the hallmark event in the disinformation landscape in the United States is the 2016 election, when Russia was found to have facilitated the victory of President Donald J. Trump by way of the information space. The US intelligence community's findings[2] of Russian malign influence and the

1 United States Cyberspace Solarium Commission. (2021). *Cyberspace Solarium Commission - Disinformation White Paper.* Retrieved from: https://www.solarium.gov/public-communications/disinformation-white-paper.

2 Gaddy, C.G., *et al.* (2022). *What the Mueller Report Tells Us about Russian Influence Operation.* Brookings. Retrieved from: https://www.brookings.edu/articles/what-the-mueller-report-tells-us-about-russian-influence-operations/.

widespread publication of this proof in 2019[3] catapulted the term 'disinformation' into the mainstream, turning it into a buzzword that has been admitted to the American conscience. That a foreign body could infect American perceptions with its own priorities and create thoughts and actions unaligned with the American national desire prompted action from the leadership in the United States. Civil society and non-governmental organisations were of course already addressing the issue, but this event shifted disinformation resilience higher on the ladder of American priorities and singled it out as an urgent emerging threat to American democracy.

Given that one of the United States' founding principles is freedom of speech and expression, the delicate balance between countering disinformation and guaranteeing full freedom of speech is a notable part of the conversation in the United States. This principle was put to the test most dramatically during the COVID-19 pandemic, when the public discourse about how best to respond created waves of disinformation about vaccines and their efficacy, stifling public health efforts. A UNESCO study found that 'one in four popular YouTube videos on the coronavirus contained misinformation'.[4] The pandemic showed how the First Amendment can be weaponised to block malicious actors from criticism and regulation. Simultaneously, there is a real danger of making the situation worse by over-regulating freedom of speech in the name of combatting mis- and disinformation.

The threat itself has only grown since that time, with the rise of emerging technologies and their employment for disinformation purposes outpacing efforts to counter it. The period following the Trump election and the release of the Mueller report saw the emergence of new efforts focused on the issue, as well as an expansion of the topic as a priority issue within already existing organisations. It also integrated the counter-disinformation efforts of civil society with national security interests. 2023 in particular has witnessed the transition

3 United State Department of Justice. Office of the Special Counsel. (2016). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Retrieved from: https://www.justice.gov/archives/sco/file/1373816/download.

4 UNESCO, International Telecommunication Union, Broadband Commission for Sustainable Development. (2020). *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*. Broadband Commission Research Report on 'Freedom of Expression and Addressing Disinformation on the Internet', Bontcheva K. and Posetti, J. (eds), Geneva: International Telecommunication Union. p.60.

of these efforts into the American legal framework,[5] highlighting both the positive effect NGOs have had in this fight as well as the growing priority this has in the US legal and wider government systems.

A major American player in the disinformation space is the National Endowment for Democracy and specifically its subsidiary the National Democratic Institute (NDI). They conduct programmes themselves, but they specialise in distributing grants to other civil society actors combatting disinformation. They fund counter-disinformation efforts as well as those focussed on adjacent topics like independent media and media literacy, hence building resilience to disinformation before it occurs. Although they are private NGOs, they receive most of their funding from the US government. Their mandate is global and not domestically focused on the United States, but they are worth mentioning nonetheless due to the priority disinformation receives as a topical issue. It demonstrates the American effort and willingness to devote significant financial resources to combat disinformation worldwide.

On the domestic front, disinformation-fighting efforts in the non-profit sector commonly revolve around the media literacy angle. Notable organisations in this area are the News Literacy Project and Media Literacy Now, which 'leverages the passion and resources of the media literacy community to inform and drive policy change at local, state, and national levels in the U.S. to ensure all K-12 students are taught media literacy so that they become confident and competent media consumers and creators'.[6] The connection to young people and the school system is an integral part of the disinformation-countering approach in the United States. Another common structure of disinformation-fighting campaigns is their integration into branches of broader journalism-focused NGOs. Take, for instance, the Scripps Howard Fund, a philanthropic charity that funds journalism efforts. They have awarded a USD 3.8 million grant to the International Center for Journalists to 'help journalists produce investigative reporting to identify and debunk falsehoods and to ferret out the shadow figures

5 Although this bill focuses on AI, a notable portion is dedicated to countering AI-enabled disinformation. The White House. (2023). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Retrieved from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

6 Media Literacy Now. (2023). *Mission & What We Do: Media Literacy Now*. Retrieved from: https://medialiteracynow.org/about/mission/.

behind disinformation campaigns'.[7] This synergy between the journalism space and efforts to counter disinformation highlights the role of journalists and strong independent media in countering disinformation, therefore prompting this kind of approach from the NGO space. The American branches of RSF, Internews, and PEN – some of the most prominent global journalism and media freedom organisations – all feature disinformation-fighting programmes as part of their portfolios. PEN America's advocacy revolves around the nexus of freedom of speech and false information, addressing a longstanding debate regarding a foundational American pillar (and one that, as mentioned previously, has been found to block progress on combatting disinformation).

Also actively working on the issue are networks of organisations who have joined forces to collaborate and support one another, sometimes on a specific issue area. They have understood that collaboration is key on a topic as omnipresent as disinformation. One example is the Disinfo Defense League, a 'network of intersectional organizations fighting disinformation which affects communities of color' that brings together 'organizers, researchers and disinformation experts disrupting online radicalized disinformation infrastructure and campaigns'.[8] They have over 200 members contributing to their efforts.

Perhaps the biggest part of the disinformation conversation in the United States is taken up by the Think Tank Network, which is highly influential in investigating and mapping the threat and drawing national attention to the issue. The United States houses some of the most prominent think tanks in the world, which are part of a flourishing research environment with significant access to resources. Their research provides guidance to lawmakers; in the legal fight against disinformation, particularly on the federal level, policymakers draw heavily on think tank reports and insights. One good example of this is the Atlantic Council's Digital Forensic Research Lab, which claims to have 'operationalized the study of disinformation by exposing falsehoods and fake news, documenting human rights abuses, and building digital resilience worldwide'.[9]

7 International Center for Journalists. (2022). *Disarming Disinformation: ICFJ Launches 3-Year Initiative to Combat Dangerous Falsehoods.* Retrieved from: https://www.icfj.org/news/disarming-disinformation-icfj-launches-3-year-initiative-combat-dangerous-falsehoods#:~:text=The%20%243.8%20million%20initiative%20called,shadow%-20figures%20behind%20disinformation%20campaigns.

8 DISINFO Defense League. (2023). Retrieved from: https://www.disinfodefenseleague.org/.

9 Atlantic Council. (2023). *Atlantic Council's Digital Forensic Research Lab.* Retrieved from: https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/.

Also influential in this space is Freedom House; although disinformation is not their primary focus, their efforts to map democracy levels worldwide are underpinned by the state of disinformation in the US and globally. Their yearly *Freedom on the Net report* provides insights on the state of the Internet space, which is directly influenced by efforts to disinform. Although not part of the NGO landscape, also vital in this work are university-affiliated research institutions that are focused on the information space, such as the Shorenstein Center at Harvard University, the Internet Observatory at Stanford University, and the University of Washington's Center for an Informed Public. Due to the scale and presence of these think tanks, disinformation-fighting efforts in the United States often come in the form of their reports. While these investigations are necessary to accurately evaluate and understand the threat, more connections must be made to addressing the issue on the ground.

Due to this challenge, there is a gap between the efforts of NGOs and the American audience; their efforts usually result in briefings for policymakers and do not bleed into American society in a way that arms the average American citizen against disinformation. While it is true that some of the organisations mentioned above aim to bridge this gap, since so much of these efforts crystalise in the form of reports, awareness about current threats and developments remains in the community of practitioners and policymakers who already have disinformation at the top of their agenda. These reports are undeniably important – however, in order to build a more resilient society in the United States, the upward trend of community outreach and engagement must continue.

An additional challenge is that this problem is often treated as an international issue rather than a domestic one, a dynamic that is reflected in the nature of non-profit programmes in the United States. While it is true that disinformation plaguing the country often has foreign origins from malign state and non-state actors – particularly given that Russian influence in the 2016 election was a turning point in how Americans view disinformation as a problem – it is problematic that the perception around this threat is often framed as a foreign problem affecting domestic issues, not something that can be home-grown. In reviewing the plethora of reports written on the issue, it is clear that American disinformation evaluations lean in the direction of this being a primarily foreign threat – a flawed perspective. Unequivocally, addressing and stabilising the global situation is positive for the United States, which seems to be part of

the logic behind the outward-facing direction of so many NGOs and funding grantees. However, equal effort should be directed domestically; this begins with acknowledging that the problem is born and cultivated within American borders, and that responsibility lies with American actors too, not only foreign ones. In conclusion, although the United States allocates funding and directs its major national institutions to counter the disinformation threat from abroad, more energy must be devoted to countering disinformation within the country.

Just as important in the disinformation space is the presence of a pluralistic, independent mediascape, which is shrinking in the United States due to a consolidation of outlets and a lack of financial stability. According to Northwestern University, about a fifth of the country's population is 'either living in an area with no local news organizations, or one at risk, with only one local news outlet and very limited access to critical news and information that can inform their everyday decisions and sustain grassroots democracy'.[10] With so much of the country at risk of becoming news deserts – areas with no access to a local newspaper – and 7% of American counties already being one,[11] disinformation is at higher risk of spreading. Independent media is a key component in the fight against disinformation by curbing its spread in the first place. If disinformation is to be properly addressed, it is up to the NGO space to either expand the number of these outlets or provide funding for already existing ones. Part of the solution, therefore, is the allocation of resources to independent media outlets, particularly on the local level.

Additionally, the opportunity for a legal framework to counter disinformation is ripe in the United States. Holding social media companies accountable through legislation and regulation, as well as working with them on curbing the rapid magnification of disinformation on their platforms, is a clear, feasible policy recommendation. Although more can be done, it is a space in which the United States has made significant regulatory advancements. For example, the introduction of the Honest Ads Act, inspired by foreign influence in

10 Karter, E. (2022). *As Newspapers Close, Struggling Communities Are Hit Hardest by the Decline in Local Journalism*. Northwestern Now. Retrieved from: https://news.northwestern.edu/stories/2022/06/newspapers-close-decline-in-local-journalism/.

11 Karter, E. (2022). *As Newspapers Close, Struggling Communities Are Hit Hardest by the Decline in Local Journalism*. Northwestern Now. Retrieved from: https://news.northwestern.edu/stories/2022/06/newspapers-close-decline-in-local-journalism/.

the 2016 election, as well as the 2023 Executive Order on the Safe, Secure, Development and Use of Artificial Intelligence, will both have an impact on how disinformation is being spread and regulated. One difficulty, however, is that the delicate balance between free speech and censorship is playing an outsized role in the American debate on this issue, particularly due to the priority level the ideal of free speech has in the American conscious and legal framework. Nonetheless, regulation is a stride that provides a high level of positive gains with minimal effort, at least from the NGO or government perspective.

Lastly, I suggest a higher degree of fusion between technology companies and the civil society sector. While collaboration between the US government and technology companies is ongoing, particularly in relation to the aforementioned legal progress, NGOs do not experience the same degree of access. Addressing disinformation is requiring an increasing amount of technical and data expertise to understand the nature of its spread and the increasing role of artificial intelligence in the problem. As AI magnifies the disinformation threat at a rate non-governmental organisations cannot keep up with, a technological, AI-driven solution is necessary. Currently, these domains are far-removed, with technology companies providing their own ideas for solutions for the disinformation crisis. However, NGO actors have a more direct reach to the communities most affected and understand the issue from a different angle. Training the NGO space and civil society on these more technical aspects requires partnering with technology companies. This would also require a consideration of whether to make their data and algorithms open to the public for civil society to conduct platform audits, although this conversation has caused controversy in the United States given its sensitivity to the privacy and the business rights of companies. This suggestion is particularly pertinent in the United States, which houses the headquarters of the world's biggest platforms responsible for rampant disinformation. Given the combination of physical access and companies' legal obligations to their countries, NGOs in the United States are therefore uniquely positioned to effect change in their country and around the world.

Closing up remarks

Dr. Adam CZARNOTA,
Rector of the Riga Graduate School of Law

This volume is the final result of a project initiated and coordinated by the Riga Graduate School of Law.

All contributions in this volume deal with one of the most important issues in the 21st century – misinformation. As was written in the opening notes, misinformation itself is not a new social phenomenon, but what is new is the unprecedented social impact of misinformation. Due to technological development, it is relatively easy to spread misinformation. As always in the history of humanity, new technological devices possess a double Janus face. They can serve societies, but they can also create danger. At stake is the foundation of social cohesion, not only freedom of speech but the cornerstone of a democratic society – the issues of national security and the fundaments of the economic system.

The voice from Baltic states is critical since these societies have already learned what misinformation means and what its social consequences are. That pluralism of opinions and worldviews is valuable, and that access to reliable information is crucial for the well-being of society and a healthy social, political, and economic system. Citizens of Baltic states also knew that crucial are healthy institutions.

The general theme of the contributions is societal resilience to disinformation. In the volume, the reader will find Baltic states, the European Union, and even transatlantic perspectives. The issues presented and discussed are sources of disinformation, legal regulation, and policy initiatives undertaken on three levels: state, transnational, and international. We learned about dealing with the issue in the Baltic states, the European Union, and the USA. A reader will find legal frameworks that regulate misinformation as well as policies and

initiatives undertaken to fight against misinformation. New legislation and legal institutions are important, but they by themselves cannot build a system that will make societies immune to fake information. Legal institutions could provide the proper environment and stimulate social forces to prevent the spread of misinformation. It is a crucial problem in democratic societies.

Overregulation could put restrictions on the rights of citizens, especially freedom of speech, and restrict pluralism of opinion, but leaving social space for disinformation without restrictions could lead to undermining the social base of democratic societies such as trust and other social capitals.

In the volume, a reader will find policy recommendations on what has to be done in order to build social resilience to misinformation. General findings and policy recommendations across all contributions can be summarized as follows:

- Policies to fight misinformation should not be reactive but proactive; more strategic way of approach is needed.
- The approach should be focused on finding a balance between freedom of speech and the necessity to regulate.
- Education of citizens in the area of credibility of information is crucial.
- Enhancing accountability of digital sources of information.
- Last but not least, general conclusion – institutional changes are necessary to provide a proper framework for building a societal immune system against misinformation.

The present volume is the first step in the right direction, which we hope will lead to further discussion and political, legal, and social initiatives.