Policy Paper:

Addressing Foreign Information Manipulation in the Context of European Regulations

DOI: 10.64370/SJGY6708

Publisher:
Institute of Communication Studies
st. „Jurij Gagarin“ 17-1-1, Skopje
www.iks.edu.mk

About the publisher:
Assoc. Prof. Dr. Zhaneta Trajkoska

Edition:
ResPublica

Author:
Konrad Bleyer-Simon, Dr.

Editor:
Aleksandra Temenugova

Graphic design:
Dejan Joveski

Place and year:
Skopje, 2025

This product was prepared within the scope of the "TRACE Project: Tracking, Exposing, and Countering Hidden Foreign Manipulations and Interferences”, funded by the Government of the United Kingdom, with the support of the British Embassy Skopje. The opinions and views expressed herein do not necessarily reflect the opinions and views of the British Government.

The publication was produced in collaboration with the Institute of Communication Studies and the Centre for Media Pluralism and Media Freedom, European University Institute, Florence.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

316.776.23:327.8]:34(4-672ЕУ)(047.31)

BLEYER-Simon, Konrad
Policy paper: Addressing foreign information manipulation in the context of european regulations [Електронски извор] / [author Konrad Bleyer-Simon]. - Skopje : Institute of communication studies, 2025. - (Edition ResPublica)

Начин на пристапување (URL):
https://respublica.edu.mk/wp-content/uploads/2025/06/policy-paper-addressing-fimi-in-context-of-eu-regulations-en.pdf.
- Текст во PDF формат, содржи 39 стр. - Наслов преземен од екранот. -
Опис на изворот на ден 05.12.2025. - Фусноти кон текстот. - За авторот:
стр. 39. - Библиографија: стр. 30-38

ISBN 978-608-4805-69-4

1. Гл. ств. насл.
а) Дезинформации -- Странски влијанија -- Правна рамка -- Европска Унија
-- Истражувања

COBISS.MK-ID 67636997

Policy Paper:
Addressing Foreign Information Manipulation in the Context of European Regulations

by Konrad Bleyer-Simon

Contents

ABSTRACT 5

INTRODUCTION 6

- Overview of EU policies 9
- Obligations of digital platforms under the DSA and EMFA regarding the suppression of FIMI 13
- How should national governments of both EU member states and candidate countries implement measures to deal with FIMI? 17
- What is the role of political actors in ensuring transparency and accountability in the digital space? 20
- How can media organizations improve resilience to FIMI within the existing regulatory framework? 21
- What are the best practices within the EU, and can they be applied to Western Balkan countries? 23

CONCLUSIONS AND RECOMMENDATIONS 26

- Conclusions 26
- Recommendations 28

REFERENCES 30

- Policies 30
- References 32

ABOUT THE AUTHOR 39

Abstract

This policy paper analyses the regulatory obligations and institutional responsibilities that emerge within the EU legislative framework to strengthen information integrity and increase a society's resilience to foreign information manipulation and interference (FIMI). Since many attempts to deal with harmful content originating from abroad are covered by anti-disinformation policies, we will include these attempts in our investigation. The policy paper starts with a short introduction on the problem of FIMI, followed by an overview of the regulatory landscape in the EU. It looks at 1) the relevant obligations of digital platforms under the Digital Services Act, the European Media Freedom Act (EMFA) and other relevant EU policies, 2) the ways in which governments of EU member states and candidate countries should implement EU regulations, 3) the role of political actors in ensuring transparency and accountability in the digital space, 4) the opportunities for news media organisations to improve resilience to FIMI within the existing regulatory framework, and finally, 5) provides some best practices within the EU, and investigates how they can be applied to the countries of the Western Balkans. Throughout the text, we will assess the situation – and provide recommendations – with a number of stakeholders in mind, such as technology companies (especially operators of very large online platforms and very large online search engines – VLOPs and VLOSEs), national governments, political actors, media organisations, as well as civil society and academia.

Keywords: FIMI, disinformation, EU regulation, Digital Services Act, European Media Freedom Act, FIMI, North Macedonia

Introduction

The aim of this policy paper is to assess what relevant stakeholders in the EU and the countries of the Western Balkans can and should do to counter FIMI (foreign information manipulation and interference) – but when doing so, we need to highlight that FIMI is an elusive and constantly evolving threat, which overlaps with certain other risks to information integrity. In many cases, FIMI is a form of disinformation[1] that clearly originates from sources outside of the EU, but the term covers not just certain forms of harmful content (disinformation, propaganda, etc.) but also behaviours and operating methods (TTPs – Tactics, Techniques, and Procedures), such as hack-and-leak attacks, deepfakes and coordinated inauthentic activities. The European Democracy Action Plan (2020) and the 2022 Strengthened Code of Practice (now Code of Conduct) on Disinformation mention that "foreign interference in the information space" is "often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents".

In many cases, FIMI – just as most forms of disinformation – is not illegal. Nevertheless, it can cause harm to democratic processes (such as the integrity of elections) or public order (for example, in the case of a pandemic or during a national security emergency). As a security threat (as a key component of so-called hybrid warfare), it can be reflected in national defence and national security strategies as well. As we will show later, based on the assessment of EU policies, foreign interference and information manipulation can be considered a systemic risk under Art 34 of the Digital Services Act. The Code of Conduct on Disinformation mentions that relevant stakeholders need to "recognise the necessity to continue to strengthen their commitments in order to counter and limit impermissible manipulative behaviours and practices across their services, foreign information manipulation and interference, and hybrid threats to security." Moreover, FIMI is also highlighted in the context of the national monitoring exercise of European media markets, proposed in Art. 26 of the European Media Freedom Act.

1 Following the definition of Wardle and Derakhshan (2017), we consider disinformation to be intentionally spread harmful and misleading content. The European Democracy Action Plan / Code of Practice/ Code of Conduct on Disinformation definition adds that "disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm" – such content is in most cases related to issues of public interest (especially public health and democratic participation), it is strategically disseminated – and can generate economic or political gain to its sources or disseminators. In the text, we refer to the phenomenon as "disinformation", but it has to be noted that platforms and researchers often call the same phenomenon "misinformation" or "harmful misinformation". In the European policy discourse, misinformation – in line with the Wardle and Derakhshan (2017) definition – refers to false or misleading content that was spread inadvertently.

When assessing the foreign actors that can pose the greatest threat to information integrity in Europe, the main country of origin of information manipulations mentioned is the Russian Federation – the sources are official state channels (such as government accounts), state-controlled outlets (such as the well-known *RT* and *Sputnik*), state-linked channels (for example actors where the affiliation is not publicly disclosed, but that have ties to the state, intelligence services or people with strong ties to the political elites) and state-aligned channels, where control or funding by the state cannot be proven but the narratives clearly align with those of the previously mentioned actors (see EEAS, 2025).

The European External Action Service (EEAS) found signs of foreign information attacks in several EU member states. The Doppelgänger operation, for instance, created websites mimicking existing mainstream websites in France, Germany, Italy, Poland and Spain (EUvsDisinfo, 2024) but possibly targeted other countries as well. Between late 2022 and late 2023, high numbers of foreign information attacks were recorded in Poland, Germany and France (more than 20 per country). Some attacks (between 1 and 5) were registered in North Macedonia, and other countries of the Western Balkans, as well (EEAS, 2024). In its previous report, the EEAS highlighted that foreign disinformation was spreading in 16 EU languages. Among the "other" languages (7.66% of cases) Macedonian was also listed (EEAS, 2023). From EDMO (European Digital Media Observatory) investigations it transpired that in the span of one week (20-26 March 2024), the Pravda network (initially identified by VigiNum, 2024) was active in 19 EU countries: Greece, Italy, Netherlands, Denmark, Croatia, the Czech Republic, Slovakia, Bulgaria, Romania, Finland, Sweden, Portugal, Estonia, Latvia, Lithuania, Hungary, Cyprus, Ireland, Slovenia (Sitistas et al., 2024). Research by members of the EDMO Network detected foreign interference related to the Romanian Presidential elections on 24 November and 8 December as well as the Parliamentary elections on 1 December 2024 (Checkfirst, 2024, European Commission, 2024). In turn, the results of the first round of the Presidential election were annulled by the Constitutional Court (Sarbu & Tanno, 2024).

There is also increased attention on disinformation campaigns originating from China, but in this case, there are less documented cases of interference. In February 2024, CitizenLab unveiled an information operation named "Paperwall". This Chinese-originated influence operation has built a network of 123 dummy media outlets worldwide, with a strong presence in Europe. The exposed assets included a Belgian and a Luxembourgish website (Alaphilippe, 2024). Iran has also targeted Western European countries with disinformation campaigns (Office of Public Affairs, 2020). Poland and other neighbouring countries are at times targeted by disinformation originating from Belarus (Bryjka & Legucka, 2021), while in Sweden, an impactful disinformation campaign was driven by foreign actors from Arabic-speaking countries (Giandomenico & Linderstål, 2023). Serbia is considered an amplifier or source of disinformation in many countries of the Western Balkans (see for example European Parliament, 2025).

Even if a country is not the direct target of foreign disinformation actors, this does not mean that local audiences are not exposed to narratives of foreign origin – in Hungary, for example, many pro-government media outlets use Russian state-controlled media as information sources and amplify their messages (Kapronczay, 2022; Urbán et al. 2023). Hungary might also be one of the cases (or potentially the only EU country at this point) that spreads disinformation from inside the EU to other countries. Prominent investments of Hungarian government-linked

actors are known in Slovenia and North Macedonia. In the North Macedonia context, investigations have been published about the Hungarian investors Péter Schatz and Ágnes Adamik – two people with close ties to Hungary's governing Fidesz party have bought a number of media outlets in North Macedonia (Keranov, 2025). These media outlets are in their narratives very supportive of the ruling party - Internal Macedonian Revolutionary Organization – Democratic Party for Macedonian National Unity (VMRO-DPMNE). These outlets were indirectly supported by the Hungarian government (Trpkovski, 2020), and a study by the European Parliament (2021) noted that these outlets were the sources of "numerous disinformation campaigns, not only to discredit the Social Democratic Union of Macedonia (SDSM) former government, but also to undermine the 2018 Prespa Agreement with Greece, and other Euro-Atlantic efforts of the country".

Finally, it is important to highlight the possible profit motives behind information interferences – that are also addressed by policies. The notion of potential economic gain, highlighted in many EU policy documents can be observed in the case of foreign information manipulations as well. To highlight this, we can look at some of the key actors involved in the spread of disinformation: first, politically motivated actors and their allies, secondly, online platforms, and third, a group that we like to refer to as small entrepreneurs. In the first case, many actors with the intent to mislead hire sub-contractors to do the job, for example, in the case of the Internet Research Agency, contractors were making a living by trolling and furthering the Kremlin's narratives. Secondly, online platforms themselves recognise that disinformation and other forms of harmful content can be used as a tool for increased interaction, time spent and revenues on platforms (Diaz Ruiz, 2023). Through content monetisation schemes, platforms and purveyors of disinformation can share the revenues. An investigation by the Global Disinformation Index (2021) found, for example, that *Russia Today, Sputnik, Breitbart* earned more than USD 700,000 per month through online advertising services. According to numbers published by Statista (2021), publishers of "misinformation" earned USD 2.6 billion in programmatic advertising worldwide in 2021. It is believed that more than 30 percent of online news media advertising might go to disinformation sites – NewsGuard (2021) writes, based on the U.S. experience: "for every $2.16 in digital ad revenue sent to legitimate newspapers, U.S. advertisers are sending $1 to misinformation websites" And third, as a consequence of the earlier two components, many small entrepreneurs will join, once they realise that impactful content is profitable content – a widely-covered phenomenon was the case of the so-called "Macedonian teenagers" who made money by publishing large amounts of pro-Trump articles on social media ahead of 2016 US elections.

In light of these challenges, the European Union emphasises a European approach that could overcome a fragmented regulatory landscape, prevents contradicting policies by different member states, and allows for a focus on platform governance – which would not be possible if policymakers intended to tackle the issue of internationally operating tech giants on the national level. First Germany and France, followed by the European Commission, have been spearheading regulation that focuses on the responsibilities of information intermediaries, such as social media service providers that control the dominant infrastructure of news dissemination and consumption. In this domain, while the so-called Brussels effect plays a role in providing a standard to regulate the online sphere globally (Bradford, 2019), problems still remain, as most major online platforms are US-based, and may find it hard to adapt to the requirements of oth-

er jurisdictions (Georgetown University Law Center Global Law Scholars, 2022) – this became clear when Elon Musk becaming owner of Twitter (now X) and later, when Meta decided to phase out its third-party fact-checking program. At the same time, many countries utilised soft-(er) approaches as well, in an enabling/facilitative way, to strengthen the resilience of members of society to harmful, fabricated content.

OVERVIEW OF EU POLICIES

The European Union has been at the forefront of designing policies to tackle disinformation that are widely praised for their potential. One of the first measures was the initiation of the East StratCom Task Force[2] in 2015 (at the European Council Meeting on 19-20 March) with the aim of identifying and countering harmful narratives – originating from outside the EU – that can destabilise European societies (Véritier, 2024). This was followed by a communication on hybrid threats,[3] which saw intentionally-spread misleading messages as one of its key concerns (Abbamonte & Gori, 2023:130). The sources of such narratives were, at the time, widely considered to be state-connected actors from the Russian Federation, a country that had not much earlier invaded the neighbouring Ukraine and was using its propaganda apparatus to influence public opinion in a number of countries, including EU members. The acronym FIMI (Foreign Information Manipulation and Interference) is widely used in policy discussions to refer to information-manipulation efforts by foreign state-sponsored entities – the concept overlaps with disinformation, but it identifies its targets not based on content but the behaviour of actors (tactics, techniques and procedures) (Hénin, 2023).

However, the source of harmful, untrue and misleading narratives can be more than just a foreign power. They can originate just as easily from a country's own citizens, who knowingly or unknowingly share information that can have adverse effects on society. Designing action against such content is a delicate issue, as the free communication and exchange of views of people on matters of public interest is key to an open society. It is in every EU member state protected by law – limitations need to be justified and proportionate. Not to mention that the content of disinformation messages would in most cases be considered as legally permissible communication – only concerns about its possible impact make it subject to public policy action. For this reason, European policy makers had early on put an emphasis on safeguarding fundamental rights while tackling disinformation – and had been advocating for a European approach in order to avoid a fragmented European policy landscape in light of a border-crossing problem (Nenadić, 2019, European Commission, 2018a).

The EU's approach to tackling, in particular online, disinformation rests on the notion that legal content, even if it might be considered harmful "is generally protected by freedom of expression and needs to be addressed differently than illegal content" (European Commission, 2018b).

[2] Which is part of the European External Actions Service.

[3] Hybrid threats are new forms of conflicts that rely on a wide arsenal of tools to destabilise countries. Van Raemdonck & Meyer (2024) argue that disinformation "has the potential to undermine fair election processes and endanger public health [and therefore] it qualifies as a hybrid threat."

The comprehensive approach on the EU level started with the establishment of the High Level Expert Group on Fake News and Online Disinformation. This initiative enabled a discussion between scholars, the industry, civil society and policymakers, with the aim of defining the path towards European policy initiatives to deal with the threat of disinformation. Its report (High Level Expert Group on Fake News and Online Disinformation, 2018) advocated for a multidimensional approach that assigned a great role to independent news media. Its recommendations included increased transparency of online news production, supporting the health and diversity of news media markets, highlighted the importance of media literacy measures, and asked that online platforms develop tools that empower their users.

In parallel with the work of the High Level Expert Group and the Code of Practice, the European Commission's Action Plan against Disinformation was published in 2018, with the aim of protecting the democratic systems in the context of elections, building on the work done by the East StratCom Task Force. It identified the measures that the European Commission and its High Representative were expected to take, in cooperation with the EU's member states and the European Parliament. The European Council Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats is also of great importance here. This working group has the central coordinating role in the EU for a joint EU response to hybrid threats.

The Commission's Action Plan highlighted the need to increase transparency and accountability in the digital environment, and to empower members of society to withstand disinformation, instead of relying simply on penalising publishers of disinformation. The action plan emphasised that 1) the EU should increase its capabilities to detect disinformation, 2) strengthen its responses (for example, through the establishment of a rapid alert system), as well as 3) mobilise the private sector to take action against disinformation, and 4) to raise awareness in society (through supporting fact-checking and research) (see also Gori & Abbamonte, 2023:139-140).

The issue of media literacy – which is important to foster societal resilience to disinformation – has also been addressed on the European level. The revised Audiovisual Media Services Directive (2018/1808) of 2018 emphasises that member states need to improve societies' media literacy skills, and such measures should consider the ability of critical thinking. The Digital Education Action Plan (COM/2020/624) emphasises the need to foster such skills through education and training. The Expert Group on Media Literacy meets annually to identify and facilitate good practices. However, so far, limited information is available on how the EU or its different member states fare on the issue of media literacy (Goodman, 2021).

Still in 2018, the self-regulatory Code of Practice on Disinformation was passed, ahead of the European Parliament elections of 2019. As part of this ground-breaking effort, some of the largest online platforms have committed to obligations that were otherwise not required from them by law: they promised they would prevent purveyors of disinformation from generating revenues through their services, limit the use of bots, improve the transparency of political advertising, while at the same time empowering users and researchers. In 2020, the European Digital Media Observatory (EDMO) – a project that brings together academia, policy experts, fact-checking organisations and media literacy professionals – was established to support the work done under the Code, which, by 2022, had established local hubs that represented all EU member states. Despite the promising nature of the Code of Practice's text, its impact was limited due to a lack of compliance and oversight, and in 2022, a new Strengthened Code of

Practice on Disinformation was published to address the shortcomings. It included clear metrics and monitoring mechanisms that allow the tracking of improvements, and thus contribute to the effectiveness of the initiative. At the same time, it has been a worrying development that despite an increase in signatories to this code, Twitter (later renamed X), which is one of the largest online platforms and home to a multitude of disinformation actors, has opted to exit the cooperation after it failed to fulfil many of its commitments (Pitchers, 2023).

While the Code of Practice itself was only a self-regulatory instrument, it was transformed into a co-regulatory code of conduct under the Digital Services Act, thereby serving as a guidance for platforms' mandatory risk mitigation efforts. Although not specifically disinformation-focused, the DSA is a powerful tool that establishes a framework for transparency and clear accountability on online platforms, especially those that are referred to as "very large online platforms" (VLOPs),[4] such as the previously mentioned X or the services operated by Alphabet (Google) and Meta (Facebook). The DSA, among other things, sets out obligations for these platforms to identify and mitigate systemic risks, such as disinformation, calls for a code of conduct for online advertising, and requires VLOPs to undergo a yearly audit on their own expenses.[5]

Additional protections of the online information environment in the EU can be found, among other things, in the Digital Markets Act, the European Media Freedom Act, the Artificial Intelligence Act, and the Regulation on the transparency and targeting of political advertising.

While the European approach, once fully developed, can provide significant protections for citizens who use social media or other online services all over Europe and can foster some convergence, it is important to highlight that tackling disinformation is a rather complex exercise, and the mainly platform-focused European approach is just one of its components. This was made clear during Russia's invasion of Ukraine in February 2022. Policymakers saw the threat of Russian-origin disinformation and war-propaganda based on fabricated information as imminent, not just on social media, but also spreading through broadcast services, international media outlets and messaging services. Thus, on 2 March, the official ban of the Russian international media outlets *RT* (formerly Russia Today) and *Sputnik* was published in the EU's Official Journal. A Council regulation and decision provided legal grounds to take both outlets (including different language editions) off the air and block their online content inside the EU, as a sanction to Russia for the invasion of Ukraine and as a defensive move against harmful disinformation in that critical period.[6] Later, additional channels, such as *Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24* and *TV Centre International*, were added.

[4] As well as "very large search engines" or VLOSEs.

[5] Still, in certain countries, this European approach is considered, to some extent, concerning: Ireland, Sweden and Finland, for example, published a joint non-paper that highlighted the possible risks of over-blocking if provisions are applied to content that is not "manifestly illegal". Politico (2021).

[6] European Commission President Ursula von der Leyen announced on 27 February that RT and Sputnik would be banned in the EU. The sanction was published in the Official Journal on 2 March, in the form of a Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP, integrated in the Council regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/20144. The legal basis of the regulation is art 215 TFUE under EU's external action and the common foreign and security policy (CFSP). When a decision adopted under CFSP "provides for the interruption or reduction, in part or completely, of economic and financial relations with one or more third countries, the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission, shall adopt the necessary measures. It shall inform the European Parliament thereof." Paragraph 2 of the article says that "[...] the Council may adopt restrictive measures under the procedure referred to in paragraph 1 against natural or legal persons and groups or non-State entities" and (par. 3) adds that "[t]he acts referred to in this Article shall include necessary provisions on legal safeguards." The ban outlined in the Council decision and regulation meant a discontinuation of transmission and distribution through satellite and cable, as well as the blocking of content on "IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed" of the operators RT and Sputnik.

Why these media outlets are considered parts of FIMI operations is not necessarily obvious at first. *RT* and *Sputnik* are global media networks that claim to provide "alternative views" (Erlanger, 2017) in a number of languages. Both are subsidiaries of the Russian state-owned Rossiya Segodnya news agency and partly funded by the Russian state. Their editorial independence is questionable, considering their strict connection with the Russian government. Studies report how the outlets publish not just factual news, but also numerous fabricated or misleading stories, including conspiracy theories (Yablokov, 2015). The so-called "nutrition labels" used by NewsGuard to categorise news outlets based on their trustworthiness highlight that both outlets severely violate journalistic standards: they repeatedly publish false content, rarely clarify errors and fail to effectively differentiate between news and editorial (NewsGuard, 2022a & b). RT provides broadcasting in four languages spoken in the EU, through RT English, RT-UK, RT-Germany, RT-France, RT-Spanish. Not only do they fail to uphold journalistic standards, but, based on a 2017 report drafted and coordinated by the US Department of Justice, the Central Intelligence Agency and the National Security Agency argued that the two outlets were part of Russian propaganda efforts, and together with a "network of quasi-government trolls'' they ran an influence campaign that jeopardised the integrity of the 2016 US presidential election (US National Intelligence Council, 2017). Based on interviews with past and current employees, Elswah and Howard (2020) argued that RT was "an opportunist channel that is used as an instrument of state defence policy to meddle in the politics of other states."

The ban has found immediate implementation across the EU, by media authorities, institutions and operators by any means involved in its implementation. However, this measure may not be among the most effective, due to limitations in enforcement – the websites of the outlets remained available for some time after the Council decision in certain member states. In Hungary, there were even complaints by civil society organisations that, despite the ban, media outlets, including the public service media, kept relying on *RT* as a source for their reporting on the situation in Ukraine, just to name a few (Kapronczay, 2022). At the same time, we can also see that the EU-wide ban doubled down on member state efforts. The regulators in the Baltic countries and Poland had acted even a few days before (Munch, 2022) the Council regulation, and independently from it, by suspending the retransmission of a number of other Russian-origin television programmes on the ground of threats to national security or in application of art. 3.3 of the EU's Audiovisual Media Services Directive (AVMSD), stating that a member state can limit freedom of reception and retransmission when an audiovisual media service provided under the jurisdiction of another state prejudices or presents a serious and grave risk of prejudice to public security, including the safeguarding of national security and defence. Even in previous years, the AVMSD was effectively used by member states to limit Russian broadcasting, especially in the Baltic states,[7] as it allows for the suspension of transmitting programmes that incite

[7] In a 2021 opinion, the European Regulators Group for Audiovisual Media Services (ERGA) found that the Latvian National Electronic Mass Media Council's decision No. 68/1-2 on restricting the retransmission of Rossija RTR on the country's territory for 12 months was substantiated and compatible with the AVMSD, as the service provider had repeatedly infringed the material provision of Art. 6(1) of the Directive ("Without prejudice to the obligation of Member States to respect and protect human dignity, Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any: incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter") in a way that, in the specific context of a former member of the Soviet Union with a significant ethnic Russian population, is "suitable to aggravate tensions impeding a peaceful coexistence of sovereign nations and ethnicities". In addition, the opinion also mentions that prohibitions have taken place before, both in Latvia and Lithuania. See: ERGA (2021).

hatred (as seen in the case of Latvia and "Rossiya RTR", European Commission, 2021). On 2 February 2022, the German Commission for Authorisation and Supervision (ZAK) also decided to ban *RT*'s German edition (Etteldorf, 2022).[8]

The EU ban was extensively criticised in the freedom of expression community for being an arbitrary political decision.[9] Therefore, Art. 17 of the European Media Freedom Act (EMFA) proposed a coordinated approach, which would be initiated by at least two national regulators and overseen by the newly established European Board for Media Services (the body to be succeeding the European Regulators Group for Audiovisual Media Services).

All these measures highlight the complexity of the disinformation problem. Not only does a successful approach require a multitude of coordinated responses, policymakers also need to be aware of, and be willing to correct, unintended consequences of their measures. The European approach cannot work without the cooperation of member states. Moreover, the differences in countries' level of resilience and the nature of the threat they face will keep national regulation on the agenda. As such, there is a need to understand on the country level what can make an individual state's actions against disinformation successful, and how a country in the EU can best seize the opportunity provided by the European approach and complement it with optimal measures.

OBLIGATIONS OF DIGITAL PLATFORMS UNDER THE DSA AND EMFA REGARDING THE SUPPRESSION OF FIMI

The first notable attempts to address disinformation and other information challenges to democracy on social media took place in France and Germany (see Crauford Smith, 2019, Tworek & Leerssen, 2019). Apart from the experiences of the 2016 U.S. election and Brexit, a major trigger was the alleged foreign interference in the 2017 presidential elections in France. In both countries, the legislative attempts were criticised for their possible chilling effect on freedom of expression (see Craufurd Smith, 2019, Claussen, 2018).[10] The German Network Enforcement Act (NetzDG) is aimed mainly at illegal content on social networks, but it may also address disinformation indirectly. It introduces a transparency and redress mechanism – compelling large social networks and digital platforms to block and/or delete "manifestly illegal" content, which has been reported by users, within 24 hours, on platforms that have more than 2 million users

[8] It sanctioned RT's German edition for failing to possess the correct licence for broadcasting in Germany (the broadcaster had a Serbian licence and never applied for a German one). The statement said "[t]he organisation and distribution of the TV program via live stream on the internet, via the mobile and smart TV app 'RT News' and via satellite must be discontinued."

[9] One of the most vocal critics from the scholarly field is Dirk Voorhoof (2022), Professor Emeritus at Ghent University. He emphasised that such procedures need to be based on specific legislation and be imposed by either a court or a regulator, basing the measure on a Decision and a Regulation, and allowing political rather than judicial authorities to "impose a ban on certain media outlets, on the basis of rather vague and ambiguous grounds, is unprecedented".

[10] The study on comment removals by The Future of Free Speech (2024) project found that the share of illegal content among removed YouTube and Facebook comments was much lower than in France and Sweden, and saw in this a sign of possible over-removal of content due to the Netz DG. At the same time, once the DSA is applicable, the Netz DG cannot be applied anymore. See for example: Engage (2023).

in the country. For reported content that is less obviously illegal the deadline is seven days. The French approach was influenced by the German regulation (see Türk, 2024), however, with an emphasis on elections and a clear reference to disinformation.

Following the platform regulation in Germany and France, the European Commission, has been spearheading regulation that focuses on the responsibilities of information intermediaries, such as social media service providers that control the dominant infrastructure of news dissemination and consumption. The DSA (that overwrites certain laws on the member state level) has a number of references that apply to FIMI as well – albeit mainly focused on disinformation (in the broader sense, including also TTPs and other harmful activities). The regulation highlights in its text that it addresses not just the spread of illegal content but also "the societal risks that the dissemination of disinformation or other content may generate". It specifically mentions manipulative targeting techniques that "can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups." Online platforms, such as the popular social media or streaming services are especially risky. As such, it asks the providers of these platforms not to use specific targeting methods.

The DSA introduces the categories of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), covering services that have more than 45 million users per month in the EU. The regulation highlights that VLOPs and VLOSEs "pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation." Moreover, it asks that "[t]hey should also consider awareness-raising actions, in particular where risks relate to disinformation campaigns." Furthermore, it asks for the nomination of Digital Services Coordinators in every EU member state in order to assist the Commission in monitoring and enforcing the obligations in the DSA.

Transparency in this context is a relevant component, as VLOPs and VLOSEs need to provide access to their repositories of advertisements and manipulative content "with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality". The repositories should, among other things, include information about "the natural or legal person who paid for the advertisement". In the context of FIMI and disinformation, especially following articles need to be paid attention to: Article 24 on Transparency reporting obligations for providers of online platforms, Article 26 on Advertising on online platforms, Article 27 on Recommender system transparency, as well as section 5 of the regulation, which describes the obligations for these service providers to manage systemic risks. These include Article 33 on Very large online platforms and very large online search engines, Article 34 on Risk assessment, and Article 35 on Mitigation of risks. The text of the DSA also mentions that the Commission can initiate "voluntary crisis protocols" for rapid responses to online challenges. "Such can be the case, for example, where online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information."

The risk mitigation measures related to non-illegal but still harmful content can be best addressed by the Code of Conduct on Disinformation. Although, following the commitments described by this code are not mandatory – not all VLOPs are signatories, and even the ones that subscribed did not sign up to all commitments –, the code highlights a set of measures that could effectively limit the harmful effects of disinformation and foreign interference. Both the

DSA and the Code of Practice require VLOPs and VLOSE to regularly report on the actions they have taken.

The Code of Conduct on Disinformation has 43 commitments and 128 specific measures; it is signed by more than 40 signatories, including platforms of large technological companies, industry associations, civil society and fact-checkers. Already before it became a Code of Conduct under the DSA, the preceding Code of Practice was considered a significant achievement when dealing with disinformation, as well as foreign information manipulation and interference, as it made platforms commit to actions that would otherwise not be required of them by law.

The Code highlights six main areas: 1) Scrutiny of Ad Placements, 2) Political Advertising, 3) Integrity of Services, 4) Empowering Users, 5) Empowering the Research Community, and 6) Empowering the Fact-Checking Community. It asks for the monitoring of commitments through self-reports and third-party structural indicators – all of which can be accessed through the Transparency Centre (https://disinfocode.eu/). In order to make the Code futureproof, a permanent Task-Force adapts commitments to new developments. The 2022 Code differentiates between disinformation and Disinformation: the capital D Disinformation includes not just disinformation, but also misinformation, FIMI and a number of other forms of information manipulation.

The six above mentioned areas propose a range of concrete actions, such as demonetising disinformation (focusing both on revenues generated through disinformation and money spent on amplifying disinformation), providing citizens with the necessary tools to deal with manipulated content (such as strengthened media literacy and the ability to report problematic pieces of content), transparency of services (so that opaque algorithms cannot amplify disinformation), transparency of political advertising, so that funders and targeting methods can be scrutinised, empowering researchers, so that sufficient information is available on the disinformation problem and solutions, and finally, fostering cooperation between platforms and fact-checkers, including the funding of fact-checking organisations.

The Code will be one of the possible risk mitigation measures under the DSA, but in order to become a meaningful and effective tool, stakeholders, such as policymakers and civil society need to make sure that there are sufficient incentives, otherwise platforms can try to limit their compliance. YouTube's 2025 transparency report, for example, made clear that the service is backtracking from its promises. It writes, "Google has revised its subscription to focus on reasonable, proportionate and effective measures to mitigate systemic risks related to disinformation that are tailored to our services. Accordingly, Google has exited certain commitments that are not relevant, practicable or appropriate for its services, including all commitments under the Political Advertising and Fact-Checking chapters" (Google, 2025). One of the stakeholders highlighting how risky this limited compliance can be is the European Fact-Checking Standards Network (EFCSN): "The EFCSN remains concerned that major platforms have not signed the Code at all while other big technology companies have withdrawn from important commitments to protect European citizens from misinformation and disinformation. Signing just a few commitments that are easy for platforms to meet is not enough in the fight for information integrity, because, as the European Commission's opinion states, "the Code constitutes a set of interlinked Commitments that support each other, and it is therefore most effective when fully implemented by the signatories" (EFCSN, 2025).

The protections from manipulative and misleading advertising practices, which can at times be misused by foreign actors as well, were reiterated by **Regulation 2024/900 on the transparency and targeting of political advertising**. It highlights that "behavioural profiling and other analysis techniques, are increasingly used to target political messages to groups or individual voters or individuals, and to amplify their impact." Not only are the data processing techniques that enable this form of targeting detrimental to citizens' fundamental rights and freedoms, the advertising practice also "negatively impacts the democratic process as it leads to fragmentation of the public debate about important societal issues, selective outreach and, ultimately, the manipulation of the electorate. It also increases the risk of the spreading of information manipulation and foreign interference." In this regulation, it is especially Article 5 that is relevant, as **it limits the abilities of foreign actors to run advertising related to the topics of elections and referenda, during the campaign periods.**

In addition, relevant approaches can be found in the Artificial Intelligence Act (albeit its focus with high-risk AI is overwhelmingly different from the technologies used to enable FIMI operations) and the Digital Markets Act (as it effects the operations of large tech companies, and, for example, imposed interoperability could break the market power of platforms that currently amplify disinformation).

In addition to tech regulation, platforms' responsibilities are also mentioned in the context of the EU's media freedom policies. **The European Media Freedom Act (EMFA) considers quality media an "antidote against disinformation and foreign information manipulation and interference".** As such, not just **governments need to protect independent journalistic actors but also online platforms have an obligation to foster the prevalence of trusted news media content**. In fact, disinformation and foreign information manipulation are considered risks to media pluralism and media freedom, and as such, the EMFA recommends that monitoring exercises by authorities and civil society consider them, when assessing risks to the health of the media environment (Article 26). In addition, the EMFA is relevant when it comes to the prioritisation of trustworthy content. Article 18 on Content of media service providers on very large online platforms describes under what conditions news media can provide preferential treatment to news media outlets. This preferential treatment, however, has been criticised by civil society and fact-checkers, as it can easily be misused. For example, media outlets regulated by partisan or captured regulators could not be excluded from such a scheme. Given the expansion of Hungarian media in North Macedonia, this might be a risk in the specific country context as well. The Structured dialogue, under Article 19 follows up on this issue, and provides additional opportunities to deal with FIMI. It prescribes that the newly established European Board for Media Services "shall regularly organise a structured dialogue between providers of very large online platforms, representatives of media service providers and representatives of civil society in order to: [...] monitor adherence to self-regulatory initiatives which aim to protect users from harmful content, including disinformation and foreign information manipulation and interference". While not platform-specific, Article 17 on the "Coordination of measures concerning media services from outside the Union" provides an opportunity to adequately address concerns related to media service providers from outside the EU that may spread disinformation, such as in the case of the controversial sanctions against *RT, Sputnik* and other Russian-origin media.

Apart from regulation and self-regulation, there are also a number of softer approaches on the EU-level, such as grants for independent media, media literacy activities, research, open-source intelligence and fact-checking. These approaches can also be found in EU projects aiming at Candidates and non-EU members. Among other things, the EU enabled the creation of the European Fact Checking Standards Network (EFCSN) to introduce high standards in fact-checking and foster cross-border collaboration and the exchange of experiences among fact-checkers. In North Macedonia, *Vistinomer / Metamorphosis Foundation* is a verified member of the network since 2023 (as well as a signatory to the International Fact-Checking Network).

HOW SHOULD NATIONAL GOVERNMENTS OF BOTH EU MEMBER STATES AND CANDIDATE COUNTRIES IMPLEMENT MEASURES TO DEAL WITH FIMI?

EU institutions are key players of anti-disinformation policymaking, as the EU wants countries to stand united when it comes to threats that can affect all members of the European community. In today's Europe where not only people and goods but also information is supposed to travel freely across borders, one country's inactivity might turn into the others' vulnerability. In this environment, certain national laws are being overwritten by EU regulation, such as in the case of platform regulation – with the German NetzDG being a prime example. EU Candidates should make sure to transpose the relevant provisions of the DSA and the EMFA, and assess whether platforms operating on their territory comply with their commitments under the Code of Conduct on Disinformation. When applying EU regulation in individual countries, governments should not regard all EU regulation as self-implementing, as they have many components that need to be adapted to the local situation. Moreover, additional measures might be needed on the national level that address countries' own specifics problems and vulnerabilities, in order to make sure that citizens have access to a safe, reliable and high-quality information sphere.

To guide policymakers, we can look at Epstein's (2020) four criteria for effective regulation of disinformation: action i) should keep undesirable side-effects (harm) minimal, ii) should be proportionate to the threat, iii) able to adapt to changes in technology, and iv) determined by independent agencies.

i) Undesirable side-effects are constantly part of the discussion in European policymaking, especially the potential of anti-disinformation policies suppressing freedom of speech. In many countries, proposed laws were not passed, exactly due to this concern. In the case of Germany's platform-specific law, the Netz DG, local stakeholders provided assessments that imply the law's expected chilling effect did not materialise, however, some concerns still emerge, for example, in a recent research that highlighted the high share of legal content removed online in Germany, but also in other EU countries (The Future of Free Speech, 2024). The case of Hungary's amendment of the Criminal Code's provision on scaremongering, at the same time, is an example of a policy that was intentionally designed in a way that it could be used against lawful communications, potentially including journalists covering issues of public importance – another example of Hungarian measures that may be cause for concern is the Act on the Protection of Sovereign-

ty, which provides an opportunity for authorities to go after civil society and media that are critical of governmental actions.[11]

The previously mentioned undesirable side-effects are, in fact, closely related to the ii) proportionality of measures. Action taken against disinformation can often be considered an interference with the freedom of expression – as communicators might be prevented from effectively conveying their messages to audiences or might be penalised for something that is not necessarily illegal. Especially the use of criminal law can be problematic.

iii) Changes in technology are hard to keep pace with – neither ex-post measures, nor platform regulation can react as quickly as policymakers would desire. Cooperations with technology companies can be helpful in this exercise – but on the national level this is not commonly mentioned in the policy discourse (however, the Code of Practice on Disinformation and the Digital Services Act made sure that platforms seek opportunities to cooperate with some national actors, especially fact-checking organisations). Even with more active public-private cooperation, we can expect that purveyors of disinformation keep finding new channels and new formats – however, a resilient user base can withstand even unexpected threats if they are provided with the necessary media and information literacy skills.

To do so, the work of experts is invaluable. This also means that iv) independent and diverse actors are needed to make sure that this knowledge is produced and applied in the policymaking process. In fact, significant weaknesses can be observed in countries where policymaking is politicised and trust in institutions is limited.

The involvement of diverse and independent actors means more than just institutions (media regulators, electoral commissions, educational institutions) but also a strong involvement of civil society and the private sector. In fact, civil society actors and news media have provided significant contributions to the actions taken to tackle disinformation in most EU countries. Their measures are important complements to public policies, even in countries where anti-disinformation policymaking is, in general, considered strong. Not to mention that the activities of these actors aim at strengthening societal resilience instead of targeting communicators, and as such are less likely to be considered threats to freedom of expression.

In some countries, it can be seen that public funds are made available to civil society actors working on disinformation – however, there are signs that the extent of this funding is not enough. Further support is provided by the European Commission (through EDMO and dedicated grants) as well as other grant making organisations. Throughout the years, many recommendations stressed the need to support quality media – starting from the recommendations of the High Level Expert Group on Disinformation and Fake News to the Irish Future of Media Commission report and the Belgian expert group on fake news and disinformation – but so far, news media play a marginal role in disinformation policies.[12] Past research also shows that a

[11] The Act on the Protection of Sovereignty defines the tasks of the newly established Office for the Protection of Sovereignty, which include the detection of information manipulation and disinformation activities, in cases they may infringe or threaten the sovereignty of Hungary. In principle, this power allows for action against foreign influence operations originating from countries widely considered threats to Europe's security, but the wording of the law implies that the Hungarian government sees the challenge originating from allies, such as the United States (see Bleyer-Simon et al., 2024). The Venice Commission (2024) considers that the law poses a serious risk of stifling voices critical of the government.

[12] Bateman and Jackson (2024) consider the most effective measures to be those that aim at supporting media literacy and supporting local journalism, as well as those that are capable of changing the recommendation algorithms of online platforms.

strong public service media can be a good antidote against information manipulations (Humprecht et al. 2020). It can be seen that many public service media have a mandate in fostering media literacy – in part because the Audiovisual Media Services Directive emphasises the need for member states to foster media literacy. At the same time, public service media in Europe are often underfunded (or in some countries captured by interest groups) and may be struggling when it comes to reaching certain demographics – especially young people.

While there might be some disagreement on the kinds of policy approaches that one considers most successful (and approaches might differ from country to country), having a clear strategy, a wide coalition of actors and a wide range of policy tools at one's disposal is likely the most viable approach in the long-run. Some countries already understood the need to build a comprehensive strategy to coordinate between different actors and policy domains – this is for example the case in Germany, France and Finland. In Ireland, the need for a comprehensive strategy has been highlighted in policy documents, but it could not yet manifest, in part because there was significant opposition against supporting action that limits otherwise legal communications. A complex threat, like FIMI, requires a whole-of-society approach to deal with – including government bodies, the security apparatus, the media and civil society. Preferably, a strong strategy covers many different aspects, including national security, election integrity, and especially the building of societal resilience. It can include a series of actions promoted by public authorities, such as the establishment of a strong regulatory framework, the running of awareness-raising campaigns, provision of funding (while also guaranteeing the independence of funded activities), establishment of communication channels with platforms, fostering cooperation among authorities or other stakeholders and many other initiatives.

The EU adopted a Strategic Compass in March 2022 with the aim of strengthening the bloc's security and defence policy by 2030. One of the aspects is a catalogue of instruments to tackle and respond to FIMI operations. The so-called **FIMI Toolbox** emphasises the need to improve situational awareness (among other things through monitoring and detection, the systemic collection of evidence, open-source intelligence – OSINT – investigations and information sharing), resilience building (such as strategic communications, a rapid alert system and capacity building), "disruption and regulation" (referring to laws and policies aiming at preventing and deterring or responding to FIMI attacks, including transparency measures), as well as diplomatic responses (such as international cooperation or sanctions on media service providers). It is also important for countries in Europe (not just members of the EU) to play close attention to the activities of the European External Action Service's (EEAS) activities related to FIMI.[13] In its work on monitoring and addressing FIMI, it focuses particularly on attempts originating from Russia and China. The *EUvsDisinf*o website is operated with the aim of raising awareness of the Kremlin's information manipulation efforts, while China's strategy is described in the paper *EU-China: A Strategic Outlook*. As FIMI is part of hybrid warfare, the EEAS also contributes with its expertise to the EU's EU civilian and military (CSDP) missions. Through its diplomatic activities, it manages a Rapid Alert System, manages extended frameworks with NATO and G7

[13] For a more detailed description, see: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

members, and contributes to the development of sanctions. The 3 EEAS Threat Reports (EEAS 2023, 2024 & 2025) present insights from EU member states, as well as a number of partner states, however, the lack of disaggregated data doesn't allow us yet to extract a lot of information specific to the countries of South East Europe.

Countries that build up their defence mechanisms against FIMI need to conduct a thorough assessment of the country's needs and capabilities, as well as the extent of the disinformation problem, while keeping in mind that there is no one-size-fits-all solution, and every country is different when it comes to the society's resilience and the extent to which it is targeted by disinformation. They also need to build up capacity to sufficiently monitor the effectiveness of local policies. Measures cannot be simply reactive. There is a need to emphasise resilience building including through strengthening media literacy and civic education, fostering trust in society, empowering trustworthy media, securing the independence of the public service media. Given the border-crossing nature of the phenomenon, countries need to look at the options of synergies with other countries in Europe and beyond – this can take place bilaterally, but also under the umbrella of international organisations. In the EU, examples of such projects include the Rīga-based NATO Strategic Communications Center of Excellence, OECD Expert Group on Governance Responses to Mis- and Disinformation, and the Atlantic Council's Digital Forensic Research Lab (DFRLAB). In addition, EDMO Hubs are active in all countries of the EU. There are also cases in which foreign governments (such as the United States) or international organisations (such as UNICEF) contribute by developing or funding media literacy and fact-checking projects, or broader anti-disinformation activities.

WHAT IS THE ROLE OF POLITICAL ACTORS IN ENSURING TRANSPARENCY AND ACCOUNTABILITY IN THE DIGITAL SPACE?

Mapping exercises, for example the factsheets of EU Disinfo Lab (2023), show that political parties are often among the sources of disinformation – the governing party of Hungary with many of its allied actors is one of the prime examples.[14] In Malta, the public inquiry set out to establish whether and how far the state is responsible for the circumstances that led to Daphne Caruana Galizia's assassination unveiled evidence of a state-orchestrated campaign aimed at dehumanising and discrediting Caruana Galizia, which contributed to the climate of hostility that made her assassination possible (Daphne Caruana Galizia Foundation, 2021). The Hungarian example shows that proxies of the state, such as groups of influencers can also play a role in amplifying fake narratives in favour of state actors (HDMO, 2024). In other EU member states, evidence shows that far-right and populist parties are spreading false narratives. Examples are the Slovenian Democratic Party, the Freedom Party of Austria (Schäfer, 2023), and Chega in Por-

[14] For cases when disinformation can originate from politicians, and even the governing party or state institutions, see relevant chapters of Echeverría, García Santamaría & Hallin (2025).

tugal (Pardal, 2023) – but to some extent all EU member states and candidates face disinformation that originates from certain politicians, even if only fringe ones. According to an analysis of the EU DisinfoLab, the first debunked narratives during the 2022 French presidential election also came from politicians (Hénin, 2022).

Most FIMI efforts are about interfering in political processes including elections (directly or indirectly), destabilising the EU and its members or candidates, or helping elect politicians who could foster foreign interests, local politicians can – even inadvertently – become amplifiers of foreign disinformation. Parties that sympathise with the Kremlin's narrative can find themselves supporting made-up narratives originating from abroad (see Nestoras, 2019).

In this context, it is the task of politicians to constructively work on counter-measures. Members of Parliament need to put FIMI, disinformation and the strengthening of information resilience on the policy or legislative agenda. In addition, politicians – no matter if in office or running for it – should refrain from producing disinformation or reproducing FIMI narratives, even if they would – in the short run – benefit them. Instead, in order to get out positive messages, they should build coalitions with civil society and establish transparent communication strategies and working relations with media – in a way that is respectful to the independence of both civil society and the media.

HOW CAN MEDIA ORGANIZATIONS IMPROVE RESILIENCE TO FIMI WITHIN THE EXISTING REGULATORY FRAMEWORK?

According to Nikodinoska & Chausidis (2025), the media system of North Macedonia experiences numerous challenges, such as a weak media market and ineffective regulation. It is important to address these challenges, as independent media can provide effective remedies to disinformation and foreign information manipulation. A strong public service media is especially emphasised in the literature, as key to the resilience of societies to disinformation (see Humprecht et al. 2020). Public service media, in general, act as a trusted source of information for society, but in many cases, they have dedicated tasks, such as the fostering of media literacy, or they run their own fact-checking projects, such as Belgium's Francophone Public broadcaster *RTBF* (the Faky fact checking project) or the Flemish public broadcaster *VRT*. In Poland, the *FakeHunters* project is run by another public institution, the Polish Press Agency. Similarly, independent private media can be significant remedy to information challenges, by holding government and institutions to account and helping society make sense of the world, as well as make informed decisions about matters of public life.

Public and private news media are regulated by both, regulation (at least in the case of broadcast and on demand media) and self-regulation, which provide some indication to media outlets how to handle and verify facts. The effectiveness of self-regulatory codes and journalistic associations diverges across countries, as ethical codes are not legally binding – but certain control mechanisms can facilitate their enforcement. One of the impactful documents is the German press code by the German Press Council (Deutscher Presserat), which extends to both print and online media. In Belgium, the francophone ethics body (Conseil de déontologie journalistique)

issued decisions on alternative media outlets that were infringing the ethics code (EDMO Belux, 2023), showing that self-regulatory instruments can adapt to the new media environment. Although self-regulation is in most cases voluntary and ethics bodies have no legal jurisdiction or public authority, there are countries where their decisions are closely followed and observed. In Greece, parliament ratified a law in December 2022 to form a Special Committee charged with overseeing the compliance of online media to "journalistic ethics". Noncompliant media can lose state advertising funds – a crucial source of revenue for media in Greece - for up to two years (Dimitriadis, 2023). In Cyprus, the Journalists' Code of Conduct includes special provisions focusing on mis- and disinformation: "Trust in the media and journalists is supreme value of Journalism. Mis/Disinformation, fake news that may be spread through media or social media are detrimental and dangerous phenomena for democracy and freedom of press. Therefore, any involvement of media or journalists in spreading fake news or mis/disinformation is unacceptable."[15] The Journalistic Ethics Committee of Cyprus does not have the authority to impose penalties or award compensation. However, the committee can investigate claims of violations or threats to freedom of the press, either on its own or in response to complaints. Parties involved have the opportunity to present their positions. If the committee finds a violation or threat, it discloses its findings, leading to ethical satisfaction rather than legal conviction for those accused of spreading disinformation. The decisions and findings of the committee are made public.[16]

News media are experiencing a crisis for at least two decades, which leaves them financially vulnerable, lacking resources to conduct costly investigations, and with significantly eroded public trust. It is not enough for media to just follow self-regulation; they also need to rebuild trust and reach out to young generations. This would require them to work more transparently, strengthen research methods, and revise their ethical codes – a possible example is the code of fact-checking organisations under the EFCSN, that was created as a response to the current "post-truth" environment.

In order to serve audiences in the long-run, it is also important to address systemic weaknesses of their operational models. They need to look for sustainable revenue sources, including new audience revenues, and potentially engage in discussions with policymakers about the opportunities and conditions of public funding. They also need to stop relying on certain strategies that promise benefits in the short-run, but erode trust and further decrease profitability in the long-run – such as low quality, clickbait and sensationalist content. Instead, they need to prioritise content that has public value. Long-term success also requires experimenting with new methods of reaching audiences, and new formats of content presentation. Journalists in the 2020s need to be interactive and innovative. Moreover, the developments in the last few years also show that journalism can only strive if it breaks out of its Facebook/TikTok/YouTube-dependence – as the platform-logic requires media to maximise the number of clicks, thereby making long-term planning impossible.

[15] Journal Code 2022. https://cmec.com.cy/en/journalists-code-of-conduct/journal-code-2022/#item-2
[16] Rulings. https://cmec.com.cy/en/rulings/

WHAT ARE THE BEST PRACTICES WITHIN THE EU, AND CAN THEY BE APPLIED TO WESTERN BALKAN COUNTRIES?

According to a study by Metamorphosis (Trojachanec & Rizaov, 2024), North Macedonia has no coherent response to FIMI and its cybersecurity strategy is limited. In 2019, the Plan for Resolute Action against the Spreading of Disinformation was published, followed by the Strategy for Building Resilience and Tackling Hybrid Threats in 2021. Pankovski and Rechica (2022) highlighted after the passing of the strategy that key institutions lacked competencies and incentives to properly address disinformation and FIMI. Trojachanec & Rizaov (2024) add that "poor media professionalism and political turmoil" add to the problem. The paper mentions that the only one of five parliamentary bodies taking significant action against FIMI was the Defence and Security Committee of Parliament.

In January 2025, the new Macedonian government adopted the National Cybersecurity Strategy 2025-2028. Priority Area 3 on a Cyber-Resilient Society highlights in Specific Objective 1 the need to "[r]aise awareness on cybersecurity and disinformation in cyberspace" – there are no studies yet assessing its effectiveness. Art 394-d of the Criminal Code deals with spreading online hate speech, with a possible penalty of one to ten years imprisonment.[17] Vujić (2024) mentions that weak enforcement mechanisms in North Macedonia might limit the implementation of the DSA – the country, just like some of its neighbours, has underfunded regulatory bodies and outdated infrastructure. Neither is North Macedonia part of the EU digital space, in which a local Digital Services Coordinator helps with the enforcement of the DSA. When considering how to strengthen its resilience to FIMI, North Macedonia can look at the examples of other countries, especially those of the EU, that have been experimenting with a range of approaches to tackle information challenges – the EU experience also shows what approaches need to be avoided, as some measures turned out to be ineffective or detrimental to human rights, and as such cannot be part of a good response. The European experience shows that the most important measures focus on resilience building – such as media literacy, education, and a strong and trusted news media. It can also be seen that successful countries have comprehensive strategies that involve multiple ministries/departments, which constantly cooperate and coordinate.

In addition to the European approach of disinformation regulation and policy making, all EU member states have national measures to tackle disinformation on the national level. Nordic countries, including the three Baltic states emphasise media literacy to strengthen the resilience of society – Estonia and Finland particularly excel in this domain – but also take significant steps to counter foreign information manipulations with cybersecurity strategies. Notwithstanding this, there may still be challenges in the future, due to large language models and artificial intelligence – which can significantly change the way content is produced and consumed. International cooperation also plays an important role: apart from commitments made to the EU's Democracy Action Plan and the reliance on EU policy tools, some countries were

[17] Criminal Code of North Macedonia. https://legislationline.org/sites/default/files/2023-09/criminal%20code%20of%20Macedonia.pdf

driving their own international initiatives. The Baltic countries, for example, played an important role in the establishment of the East StratCom Task Force and the NATO StratCom Centre of Excellence. Countries bordering Russia, Belarus or Ukraine are also more likely to have taken measures to block certain foreign content providers that regularly publish propaganda or disinformation. Non-legal approaches on disinformation are, in general, more common in the EU than legal approaches. There are many proposed laws that did not pass in the end, either due to stiff criticism, changes in government or shifting priorities. In certain cases, soft measures, strategy documents or recommendations did not lead to actions.

Many countries have criminal code provisions that can be applied to publishers of disinformation – these can be articles dealing with slander, defamation, threats to public order. There are also measures aimed at actors who aim to influence elections with false information. Malta, Cyprus and Greece even mention "false news" in their criminal laws. The Lithuanian Criminal Code's Art. 285 deals with false information about "imminent danger or serious disaster to the public or an object of national importance." Some criminal law provisions are aimed specifically at foreign threats. In Denmark, for example, influencing decision-making and public opinion on behalf of foreign actors is prohibited under the Law on Foreign Influence and under the Penal Code's Art. 108 (Simonsen, 2024). The Penal Code also prohibits propaganda aimed at helping the enemy during war or occupation. Criminal law approaches, however, are considered controversial, as they can have a chilling effect on freedom of expression, and can only be applied in the most egregious cases of disinformation (and if the publisher is known) but cannot significantly mitigate the problems associated with rapidly spreading false narratives and conspiracy theories. In several countries, proposed laws to penalise purveyors of disinformation were heavily criticised, and could not be adopted. Germany and France are the two countries that are well-known for their laws focusing on online platforms – other countries, such as Italy and Bulgaria, tried to follow this approach but could not pass laws – the concerns were, in these cases as well, often related to freedom of expression.

Since disinformation and foreign interference are complex threats, affecting multiple domains of policy, a number of EU member states look at ways to involve a wide range of actors and to coordinate the actions they take. According to the 2024 Media Pluralism Monitor, Germany, Finland, France and Ireland can be considered some of the countries that have a robust disinformation strategy, but coordination can be found in other countries as well. In Ireland, the Future of Media Commission report (published in 2022) concluded that a coordinated strategy is needed for the country. The National Counter-Disinformation Strategy is led by the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media. It established a working group to develop a National Counter-Disinformation Strategy, which is composed of representatives from industry, academia, civil society, and government departments. While there is no tangible outcome of this work yet on the policy level, the establishment of the working group marks a first step towards devising coherent and comprehensive disinformation strategies (Flynn, 2024:27). The terms and references of the group highlight the need for media literacy initiatives in a targeted, complex governmental approach, the need for a comprehensive assessment of existing tools (both national and international best practices) to counter disinformation and address evolving threats, support for innovation in fact-checking and research, as well as contribution to the long-term assessment of EU-level policies (the Code of Practice on Disinformation and the Digital Services Act). In Germany, where the Federal Ministry of the Interior is tasked with

identifying disinformation, responses are coordinated by a special task force of the ministry. Education and strengthening resilience is a task of the Federal Ministry of the Interior, the Federal Ministry of Family Affairs, and the Federal Agency for Civic Education (Bundeszentrale für politische Bildung, BpB). Information exchange takes place under the Federal Ministry of Foreign Affairs and the Federal Ministry of Defence.

All EU countries have fact-checking organisations that are actively monitoring the information environment and debunk disinformation narratives. Some of them also cooperate with online platforms as local, third-party fact-checkers. Their funding, however, is in most cases vulnerable. One of the sources of revenue is the European Commission through the European Digital Media Observatory and dedicated grant programs. In many countries, public service media has its own fact-checking programs, but for private fact-checking projects support only exists in a handful of countries, such as in Croatia, where the Agency for Electronic Media launched a public call in 2023 for grant distribution for establishing an independent network of fact-checkers. Certain news media in member states also have dedicated programs to address disinformation. Media literacy is in most EU countries included in the national education curriculum, however, according to the Media Pluralism Monitor 2024 data collection, there are cases in which the availability or quality of media literacy courses is inadequate, and its focus is not always society's resilience to disinformation (Centre for Media Pluralism and Media Freedom, 2024).

For the countries of Southeast Europe, no EU member can count as clear role model, but there are best practices across the bloc. Belgium and Portugal, for example, are countries where robust structural fundamentals, such as strong media literacy efforts and high degrees of media freedom, contribute to resilience in society, despite a lack of dedicated anti-disinformation policymaking. Similarly, Finland is well-prepared for challenges in the information sphere, but in this case, dedicated measures, such as complementing the country's high-quality and inclusive education with the active cooperation between Defence Forces and other governmental agencies, strengthen resilience. EU member states that joined in the 2000s, especially Bulgaria and Romania, are in a worse position than most old members of the EU, as they had less time to develop effective institutions – this influences their responses to the disinformation threat. State capture and corruption can also paralyse the policy community's ability to create effective policies. Greece's contextual variables might show the impact of a long economic crisis and austerity measures, while in Hungary, democratic deficits have led to weaknesses in disinformation policymaking.

Conclusions and recommendations

CONCLUSIONS

The experiences of European countries show that there is no one-size-fits-all approach, but a number of successful policies can be adapted to other country contexts, after careful assessment. The different measures need to be assessed in the context of the existing knowledge, as well as blind spots, related to the disinformation phenomenon and disinformation policymaking. Jungherr (2024:10), for example, highlights that the arguments about the effect of disinformation "are speculative and might be overblown", while the sources of a high vulnerability to or prevalence of disinformation might, in fact, be related to certain societal factors, such as inequality in society (see Jungherr, 2024 & Kreiss, 2021) or low education levels (as highlighted in the Media Literacy Index, 2023), that might drive polarisation in society and make the population more vulnerable to misleading and fabricated content, including those spread by foreign actors – some of these problems need to be addressed by social or education policies, separately from anti-disinformation or anti-FIMI action.

The mix of policies and the choice of priorities is different across countries in the EU. It was observed elsewhere that countries with a higher GDP per capita tend to introduce more anti-disinformation measures than those with a lower GDP per capita (Cipers et al., 2023). In addition, it can be highlighted that EU member states are not affected to the same degree by disinformation. Having an unstable, war-torn or hostile neighbour can increase the extent of foreign disinformation operations. But the risks might also be higher in cases when a country is preparing to enter the European Union or NATO, or has an ethnically divided society, such as in the case of North Macedonia. Larger countries with a strong influence on EU decisions are also more likely to become targets of these campaigns – as can be seen in the example of widely publicised foreign information manipulation attempts in France and Germany. Countries that see an immediate threat coming from foreign-origin (especially Russian) disinformation are more likely to pay attention to designing their own policies on FIMI and disinformation. This is despite the fact that disinformation is not always originating from abroad – there

is also plenty of homegrown information manipulation. While domestic disinformation may not be as prominent in the public discussion as foreign information manipulation or hybrid threats, in practice, it seems like it is often addressed by the same or similar measures – this shows that foreign and domestic disinformation are not fundamentally different phenomena.

Hard law approaches remain part of the toolbox, but their impact is disputed – and might in cases infringe on freedom of expression. Many criminal codes in Europe have provisions that can be used to deal with the most egregious forms of disinformation – many of which predate the current policy focus on disinformation or as some call it "fake news" – but these are usually the cases that overlap with hate speech or the kinds of fabricated content that violate the personal rights of individuals. In some of the countries, criminal law provisions were applied by courts against publishers of disinformation content that had a high potential of disturbing public peace. However, relying on criminal law sanctions can be concerning for the freedom of expression (Ó Fathaigh et al., 2021) and might have only a limited impact on the overall spread of disinformation. Dragomir et al. (2023), for example, argue that the occasional fines imposed by courts are not sufficiently effective to disincentivise those who aim at publishing such content. Moreover, such ex-post measures have no effect on foreign actors publishing disinformation (unless acting through local proxies). Similarly, traditional media regulation (including self-regulation) contains many provisions that can contribute to the truthfulness of information published (be it licensing requirements for broadcasters or a right to reply) – however, most of them cannot be applied to the numerous new actors creating, disseminating and amplifying content online. The online information environment also limits the effectiveness of sanctions or bans of certain propaganda or disinformation outlets: online audience members who are genuinely interested in those outlets (or are attracted to the forbidden fruit) can easily find ways to access the content – be it through VPNs or messenger channels.

Cooperation between agencies is crucial. Since FIMI and disinformation are complex problems requiring a whole-of-society approach, the responses need to be coordinated. A number of policy fields need to be included, from foreign policy, internal affairs and national security to education. Authorities need to establish a long-term strategy, that builds on EU regulation, such as the DSA and EMFA, one that enhances situational awareness (monitoring and analysing disinformation, as well as effectively sharing information between key actors), is capable of rapid responses, and involves foreign allies, as well as local civil society and the media.

Resilience building is key (see Pollicino & Somaini, 2020). Societal information resilience is defined as a society's ability to create systems of trustworthy information provision, its readiness to support knowledge institutions and its investment in the kinds of information literacy that would help people identify trustworthy sources (Humprecht et al. 2020). Resilience may be influenced by the levels of trust in the media or the extent of political polarisation (see Dragomir et al., 2024 and Humprecht et al., 2020) – and as mentioned earlier in this text, by inequalities in society or the quality of education. Education should in this context mean more than just media education: critical thinking skills, knowledge of natural sciences, history and the functioning of the democratic order, are all relevant when facing made-up claims. From the currently prominent measures, fact-checking and media literacy can be seen as contributing to a society's resilience. These are especially important if we consider that individual pieces of disinformation or "atoms of content" (Wardle, 2023) fit into broader narratives that are shared by whole communities.

RECOMMENDATIONS

To the government:

- Actions against FIMI need to be based on a comprehensive strategy, designed after a thorough assessment of the country's capacities and vulnerabilities.
- Measures cannot be simply reactive, countries should emphasise resilience building in society (which includes media literacy, civic education, fostering trust in society, empowering trustworthy media, providing sufficient funding to and securing the independence of the public service media)
- Look at the options of synergies with other countries – consider regional partners, but also international or multilateral organisations and countries that have already developed strong defence mechanisms. Pay close attention to the European Union's FIMI Toolbox and the activities of the EU's External Action Service.
- Involve civil society and the media in the process (including on how to adopt/implement regulations) – consider state funding to these actors in a way that does not compromise their independence
- Don't think of all the regulations as self-implementing, they also have components that need to be adapted to the local situation
- Build up capacity to sufficiently monitor the problem
- Don't forget about possible side-effects, such as limiting freedom of expression
- Avoid criminal law approaches, as much as possible
- Create an enabling environment for independent media, which includes transparency, safeguards for independence, as well as possible state support. In the case of the public service media, both independent appointment procedures and adequate levels of funding need to be guaranteed.

To the news media:

- Strengthen journalistic associations and unions, as well as establish (if not yet existent) press councils in order to enable effective self-regulation that fosters quality, independent news production.
- Look for sustainable revenue streams and new formats that can help operate as a watchdog in the long-run.
- Look at best practices, such as those originating from the European fact-checking community.

To the civil society and donors:

- Provide trainings to the journalistic community that help journalists identify and counter FIMI and disinformation – including OSINT methods, fact-checking methodologies, and the use of novel tools.

- Emphasise fact-checking, as well as media and information literacy programmes – in the latter case also focusing on marginalised groups, linguistic minorities and senior citizens, who are often more vulnerable to FIMI and disinformation campaigns.

To politicians:

- Commit to truthful communication and point out if other politicians or parties fail to do so, create a climate of constructive dialogue with voters, civil society and the media (and respect their independence)
- Foster the discussion on constructive approaches to information integrity and resilience in the policy and legislative process

To online platforms:

- In order to protect the countries of Southeast Europe from harmful information manipulations and foreign information manipulation, online platforms are asked to follow the commitments of the Code of Conduct on Disinformation. Among other things, empower audiences to identify and report harmful content, act against inauthentic activities, demonetise purveyors of disinformation and closely collaborate with the fact-checking community.

References

POLICIES

1. 2022 Strengthened Code of Practice on Disinformation. https://ec.europa.eu/news-room/dae/redirection/document/87585

2. 22 December 2018 law (No. 2018-1202) on the Fight Against Manipulation of Information. LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559

3. Action Plan Against Disinformation – Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions. Action Plan Against Disinformation. JOIN(2018) 36 final. https://commission.europa.eu/system/files/2018-12/eu-communication-disinformation-euco-05122018_en.pdf

4. Artificial Intelligence Act – Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

5. Audiovisual Media Services Directive – Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. PE/33/2018/REV/1. https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng

6. Council of the European Union (2022). Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32022R0350

7. 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. https://eur-lex.europa.eu/eli/dec/2022/351/oj/eng

8. Digital Education Action Plan 2021-2027 – COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digital Education Action Plan 2021-2027 Resetting education and training for the digital age. COM/2020/624 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

9. Digital Markets Act. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). PE/17/2022/REV/1. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng
10. Digital Services Act. Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

11. European democracy action plan – COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS On the European democracy action plan. COM/2020/790 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0790

12. European Media Freedom Act. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (Text with EEA relevance) PE/4/2024/REV/1. https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng

13. Network Enforcement Act (NetzDG). Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. https://www.gesetze-im-internet.de/netzdg/index.html

14. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng

15. Treaty on the Functioning of the European Union. Consolidated versions of the Treaty on European Union and the Treaty on the functioning of the European Union. https://op.europa.eu/en/publication-detail/-/publication/3c32722f-0136-4d8f-a03e-bfaf70d16349

REFERENCES

1. Abbamonte, G. & Gori, P. (2023). European Union. In Pollicino, O. (ed). Freedom of Speech and the Regulation of Fake News. Intersentia, 129-164.

2. Alaphilippe, A. (2024). PAPERWALL: Chinese information operation targets Belgium and Luxembourg. *EU Disinfo Lab.* https://www.disinfo.eu/paperwall-chinese-information-operation-targets-belgium-and-luxembourg

3. Bateman, J & Jackson, D. (2024). Countering Disinformation Effectively. An Evidence-Based Policy Guide. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en&center=global

4. Bleyer-Simon, K., Polyák, G. & Urbán, Á. (2024). *Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023.* Country report: Hungary. European University Institute.

5. Bradford, A., (2019). *The Brussels Effect: How the European Union Rules the World*. New York, 2020; online edn, Oxford Academic, https://doi.org/10.1093/oso/9780190088583.001.0001.

6. Bryjka, F. & Legucka, A. (2021). Russian and Belarusian Disinformation and Propaganda in the Context of the Polish-Belarusian Border Crisis. *PISM.* https://pism.pl/publications/russian-and-belarusian-disinformation-and-propaganda-in-the-context-of-the-polish-belarusian-border-crisis

7. Centre for Media Pluralism and Media Freedom (2024). *Monitoring Media Pluralism in the Digital Era. Application of the Media Pluralism Monitor In the European Member States and in Candidate Countries in 2023.* Centre for Media Pluralism and Media Freedom. https://cadmus.eui.eu/handle/1814/77028

8. Checkfirst (2024). *Ads, Influence, and Democracy: Meta's Role in Romania's 2024 Presidential Election*. https://checkfirst.network/research-note-metas-role-in-romanias-2024-presidential-election/

9. Cipers, S. & Meyer, T. & Lefevere, J. (2023). Government responses to online disinformation unpacked. *Internet Policy Review,* 12(4). https://doi.org/10.14763/2023.4.1736 Checkfirst, 2024,

10. Claussen, V. (2018). Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation. *Media Laws*, 3(3), 110-136.

11. Craufurd Smith, R. (2019). Fake news, French Law and democratic legitimacy: lessons for the United Kingdom?. *Journal of Media Law*, 11(1), 52-81.

12. Daphne Caruana Galizia Foundation (2021). *Courtesy translation of public inquiry report.* https://www.daphne.foundation/en/2021/11/20/public-inquiry-translation

13. Diaz Ruiz, C. (2023). Disinformation on digital media platforms: A market-shaping approach. *new media & society*, 14614448231207644.

14. Dimitriadis, D. (2023). Disinformation landscape in Greece. *EU Disinfo Lab.* https://www.disinfo.eu/wp-content/uploads/2023/06/20230623_GreeceDisinfoFS.pdf

15. Dragomir, M., Rúas-Araújo, J., & Horowitz, M. (2024). Beyond online disinformation: assessing national information resilience in four European countries. *Humanities and Social Sciences Communications*, 11(1), 1-10.

16. Echeverría, M., García Santamaría, S., & Hallin, D. C. (2025). *State-Sponsored Disinformation Around the Globe: How Politicians Deceive their Citizens*. Routledge.

17. EDMO Belux (2023). *Regulating Disinformation. Look-up on the Legal Framework in Belgium*. https://belux-edmo.s3-accelerate.amazonaws.com/wp-content/uploads/2023/08/Regulating_disinformation_legal_framework_Belgium.pdf EEAS, 2025).

18. EEAS (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence.* https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

19. EEAS (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence. January 2024.* https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

20. EEAS (2025). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations. March 2025. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

21. EFCSN (2025). *EFCSN Statement on Platforms' Reduced Commitments to the Code of Practice on Disinformation.* https://efcsn.com/news/2025-01-22_efcsn-statement-on-platforms-reduced-commitments-to-the-code-of-practice-on-disinformation/

22. Elswah, M. and Howard, P. N. (2020). "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT), *Journal of Communication,* Volume 70, Issue 5, October 2020, Pages 623–645. Retrieved from https://doi.org/10.1093/joc/jqaa027

23. Engage (2023, 4 October). *Digital Platform Regulation: Germany's Implementation Draft Bill of the Digital Services Act*. https://www.engage.hoganlovells.com/knowledgeservices/insights-and-analysis/digital-platform-regulation-germanys-implementation-draft-bill-of-the-digital-services-act

24. Epstein, B. (2020). Why it is so difficult to regulate disinformation online. In Bennett, W. L. & Livingston, S. (eds.). *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*, 190-210.

25. ERGA (2021). *ERGA Opinion on decision No. 68/1-2 of the Latvian National Electronic Mass Media Council restricting the retransmission of the channel Rossija RTR in the territory of Latvia for 12 months*. https://erga-online.eu/wp-content/uploads/2021/04/2021-03-10-ERGA-Opinion-on-decision-No.-68-1-2-of-the-Latvian-National-Electronic-Mass-Media-Council-as-adopted.pdf

26. Erlanger, S. (2017, March 8). *Russia's RT Network: Is It More BBC or K.G.B.*? New York Times. Retrieved from https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html

27. Etteldorf, C. (2022). [DE] German media regulator bans RT DE television channel in Germany. *IRIS* 2022-3:1/23. https://merlin.obs.coe.int/article/9408

28. EU Disinfo Lab (2023). *The disinformation landscape across Europe*. https://www.disinfo.eu/publications/disinformation-landscapes-in-european-countries/

29. European Commission (2018a). *Action Plan Against Disinformation.* JOIN (2018) 36 final. https://commission.europa.eu/system/files/2018-12/eu-communication-disinformation-euco-05122018_en.pdf

30. European Commission (2018b). *Tackling online disinformation: a European Approach.* COM/2018/236 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

31. European Commission (2019). *Latvia's decision to suspend broadcast of the Russian language channel "Rossiya RTR" complies with EU law.* Digibyte | Publication 06 May 2019. https://digital-strategy.ec.europa.eu/en/news/latvias-decision-suspend-broadcast-russian-language-channel-rossiya-rtr-complies-eu-law

32. European Commission (2024). *Commission, online platforms and civil society increase monitoring during Romanian elections.* https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243

33. European Parliament (2021). *Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them.* https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2020)653621

34. European Parliament (2025). *Motion for a European Parliament Resolution on the 2023 and 2024 Commission Reports on Kosovo (2025/2019(INI)).* https://www.europarl.europa.eu/doceo/document/A-10-2025-0075_EN.html

35. EUvsDisinfo (2024). *Doppelganger strikes back: FIMI activities in the context of the EE24.* https://euvsdisinfo.eu/uploads/2024/04/EEAS-DataTeam-TechnicalReport-FINAL.pdf

36. Flynn, R. (2024). *Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023. Country report: Ireland.* European University Institute.

37. Georgetown University Law Center Global Law Scholars (2022). *Law and Disinformation in the Digital Age.* https://www.law.georgetown.edu/wp-content/uploads/2022/04/Law-and-Disinformation-in-the-Digital-Age.pdf

38. Giandomenico, J. & Linderstål, H. (2023). Disinformation landscape in Sweden. *EU Disinfo Lab.* https://www.disinfo.eu/wp-content/uploads/2023/05/Sweden_DisinfoFactsheet.pdf

39. Goodman, E. (2021). Media literacy in Europe and the role of EDMO. *European Digital Media Observatory.* https://edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf

40. Google (2025). *Report March 2025*. https://disinfocode.eu/reports

41. Global Disinformation Index (2021): *Monetising Disinformation in the EU.* https://www.europarl.europa.eu/cmsdata/232164/revised_Agenda%20item%207_Clare%20Melford_GDI_Deck_EU-Ad-funded_Disinfo.pdf

42. HDMO (2024). In Hungary, sponsored disinformation ran rampant during the campaign for EU elections, and platforms made good money out of it. *EDMO.* https://edmo.eu/publications/in-hungary-sponsored-disinformation-ran-rampant-during-the-campaign-for-eu-elections-and-platforms-made-good-money-out-of-it/

43. Hénin, N. (2022) What did disinformation look like during the 2022 French presidential election? An overview based on fact-checking articles. *EU disinfo Lab.* https://www.disinfo.eu/publications/what-did-disinformation-look-like-during-the-2022-french-presidential-election-an-overview-based-on-fact-checking-articles/

44. Hénin, N. (2023). FIMI: Towards a European redefinition of foreign interference. *EU Disinfo Lab.* https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

45. High Level Expert Group on Fake News and Online Disinformation (2018): *A multidimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation.* Brussels: European Commission. https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expertgroup-fake-news-and-online-disinformation.

46. Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *The international journal of press/politics*, 25(3), 493-516.

47. Jungherr, A. (27 Jun 2024): Foundational questions for the regulation of digital disinformation, *Journal of Media Law*, DOI: 10.1080/17577632.2024.2362484

48. Kapronczay, S. (2022). *Complaint to the EC.* Retrieved from https://www.politicalcapital.hu/pcadmin/source/documents/TASZ-PC_EC-complaint-PublicBroadcast_Russia_War.pdf

49. Keranov, D. (2025, Mar. 20). Hungary's Power Play In North Macedonia. *GMFUS*. https://www.gmfus.org/news/hungarys-power-play-north-macedonia

50. Kreiss, D. (2021). Social Media and Democracy: The State of the Field, prospects for Reform. *The International Journal of Press/Politics,* 26(2), p. 505–512.

51. Media Literacy Index (2023). *"Bye, bye, birdie": Meeting the Challenges of Disinformation.* https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

52. Munch, E. (2022, 25 February). *Situation in Ukraine prompts reactions from NRAs across Europe. European Platform for Regulatory Authorities.* https://www.epra.org/news_items/nras-react-to-the-crisis-in-ukraine

53. Nenadić, I. (2019). Unpacking the "European approach" to tackling challenges of disinformation and political manipulation. *Internet Policy Review,* 8(4), 1-22.

54. Nestoras, A. (2019). How the Kremlin is manipulating the Refugee Crisis. *Institute of European Democrats.* https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January2019.pdf

55. NewsGuard (2021). *Special Report: Top brands are sending $2.6 billion to misinformation websites each year*. https://www.newsguardtech.com/special-reports/brands-send-billions-to-misinformation-websites-newsguard-comscore-report/

56. NewsGuard (2022a, February 20). RT.com. Retrieved from https://www.newsguardtech.com/wp-content/uploads/2022/02/RT-NewsGuard-Nutrition-Label-02202022.pdf

57. NewsGuard (2022b, February 20). SputnikNews.com. Retrieved from https://www.newsguardtech.com/wp-content/uploads/2022/02/SputnikNews-NewsGuard-Nutrition-Label-02202022.pdf

58. Nikodinoska, V. & Chausidis, T. (2025). Deprived Media Market, Low Ethical Standards, Need for Effective Legislation. The Future of the Media in North Macedonia – Facts and Trends. SEENPM. https://futureofmedia.seenpm.org/wp-content/uploads/2025/03/Ourmedia-North-Macedonia-EN.pdf

59. Office of Public Affairs, U.S. Department of Justice (2020). *United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps.* https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps

60. Ó Fathaigh, R., Helberger, N., & Appelman, N. (2021). The perils of legally defining disinformation. Internet policy review, 10(4), 2022-40.

61. Pankovski and Rechica (2022) https://cess.org/wp-content/uploads/2022/02/CESS-Policy-Brief_6-2022_EN.pdf

62. Pardal, F. (2023). Disinformation Landscape in Portugal. *EU Disinfo Lab.* https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_PT_DisinfoFS.pdf

63. Pitchers, C. (2023, June 5). Twitter has chosen 'confrontation' with Brussels over disinformation code of conduct. Euronews. https://www.euronews.com/my-europe/2023/06/05/twitter-has-chosen-confrontation-with-brussels-over-disinformation-code-of-conduct

64. Politico (2021). "Safeguarding freedom of speech online – a joint non-paper on the DSA by Sweden, Ireland and Finland" (18 June 2021). https://www.politico.eu/wp-content/uploads/2021/06/18/joint-non-paper-on-the-DSA-final46.pdf

65. Pollicino, O., & Somaini, L. (2020). Online disinformation and freedom of expression in the democratic context: The European and Italian responses. In Misinformation in Referenda (pp. 171-193). Routledge.

66. Pollicino, O. & Somaini, L. (2020). Online disinformation and freedom of expression in the electoral context: the European and Italian responses. https://ssrn.com/abstract=3552680

67. Sarbu, M & Tanno, S. (2024). Romania's top court annuls presidential election result. *CNN.* https://edition.cnn.com/2024/12/06/europe/romania-annuls-presidential-election-intl/index.html

68. Schäfer, C. (2023). Disinformation landscape in Austria. *EU Disinfo Lab.* https://www.disinfo.eu/wp-content/uploads/2023/06/20230621_AustriaDisinfoFS.pdf

69. Simonsen, S. (2024). Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Member States And Candidate Countries in 2023 Country Report from Denmark. In Media Pluralism Monitor.

70. Sitistas, T, Canetta, T., Panizio, E. (2024). Russian disinformation network "Pravda" grew bigger in the EU, even after its uncovering. *EDMO.* https://edmo.eu/publications/russian-disinformation-network-pravda-grew-bigger-in-the-eu-even-after-its-uncovering/

71. Statista (2021). Programmatic advertising revenue of misinformation publishing sites in the United States and worldwide in 2021(in billion U.S. dollars). https://www.statista.com/statistics/1253292/misinformation-publishers-advertising-revenue/

72. The Future of Free Speech (2024). Preventing "Torrents of Hate" or Stifling Free Expression Online? An Assessment of Social Media Content Removal in France, Germany, and Sweden. https://futurefreespeech.org/wp-content/uploads/2024/05/Preventing-Torrents-of-Hate-or-Stifling-Free-Expression-Online-The-Future-of-Free-Speech.pdf

73. Trojachanec, M. & Rizaov, G. (2024). Stability Under Threat: FIMI in North Macedonia. Metamorphosis. https://metamorphosis.org.mk/wp-content/uploads/2024/09/fimi-north-macedonia-report-final-for-publishing-30-09-2024.pdf

74. Trpkovski, G. (2020, Feb 14). How Hungarian Olive Oil Kept Macedonian Media Afloat. BalkanInsight. https://balkaninsight.com/2020/02/14/how-hungarian-olive-oil-kept-macedonian-media-afloat/?fbclid=IwAR2Wa0OQfm0aF1q4GrfyBY0uCOSlhVjn-sFhBmAetiuiUvmBTkfDC5nfjSg

75. Tworek, H., & Leerssen, P. (2019). An analysis of Germany's NetzDG law. First session of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

76. Türk, P. (2023). France. In Pollicino, O. (ed). Freedom of Speech and the Regulation of Fake News. Intersentia, 199-238.

77. Urbán, Á., Horváth, K. & Polyák, G. (2023). How public service media disinformation shapes Hungarian public discourse. Media and Communication, 11(4), 62-72.

78. US National Intelligence Council (2017). Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections (ICA 2017-01D). Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

79. Van Raemdonck, N., & Meyer, T. (2024). Why disinformation is here to stay. A socio-technical analysis of disinformation as a hybrid threat. In Addressing Hybrid Threats (pp. 57-83). Edward Elgar Publishing.

80. Venice Commission (2024). European Commission for Democracy Through Law (Venice Commission) Hungary Opinion on Act LXXXVIII of 2023 on the Protection of National Sovereignty. Adopted by the Venice Commission at its 138th Plenary Session (Venice, 15-16 March 2024). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)001-e

81. VigiNum (2024). *PORTAL KOMBAT. A structured and coordinated pro-Russian propaganda network.* https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

82. Vériter, S. L. (2024). Small-state influence in EU security governance: Unveiling Latvian lobbying against disinformation. *JCMS: Journal of Common Market Studies*, 62(6), 1538-1559.

83. Voorhoof, D. (2022, May 8). EU silences Russian state media: a step in the wrong direction. The 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/

84. Vujić, M. (2024). Implementing the Digital Services Act in the Western Balkans: Risks of Illegal Content Regulation. Partners for Democratic Change Serbia. https://www.partners-serbia.org/public/news/implementing-dsa-wb.pdf

85. Wardle, C. & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking.* Strasbourg: Council of Europe.

86. Wardle, C. (2023). Misunderstanding Misinformation. Issues in Science and Technology, 39(3). https://issues.org/misunderstanding-misinformation-wardle/

87. Yablokov, I. (2015). Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). Politics, 35(3–4), 301–315. Retrieved from https://doi.org/10.1111/1467-9256.12097

About the author

Konrad Bleyer-Simon Dr. is a Research Associate at the Centre for Media Pluralism and Media Freedom (European University Institute), a researcher at the Austrian Academy of Sciences, and works on the Policy Analysis and Research task of the European Digital Media Observatory. He's involved in EDMO's work on structural indicators and chairs the EDMO Hubs Policy and Analysis Working Group. He holds a doctoral degree from the Freie Universität Berlin, his research focuses on platform regulation, disinformation and the viability of news media.

Institute of Communication Studies

НЕ ВЕРУВАЈ ПРОВЕРУВАЈ! #користифакти

www.iks.edu.mk
info@iks.edu.mk

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product was prepared within the scope of the "TRACE Project: Tracking, Exposing, and Countering Hidden Foreign Manipulations and Interferences", funded by the Government of the United Kingdom, with the support of the British Embassy Skopje. The opinions and views expressed herein do not necessarily reflect the opinions and views of the British Government.

Institute of Communication Studies

НЕ ВЕРУВАЈ
ПРОВЕРУВАЈ!
#користифакти