Wilfried Martens Centre for European Studies

Enhancing Election Integrity by Strengthening EU Defences Against Disinformation

Alexander Romănishyn

Summary

June 2024

Digital platforms play a pivotal role in the dissemination of disinformation: their vast reach and engagement-driven algorithms are leveraged to spread misleading content. This makes the digital platform an extremely powerful media tool, able to have a huge impact on socio-economic and political relationships, including elections, and on the questioning of fundamental principles, such as democracy. Digital platforms have already been used several times to manipulate elections. Such platforms operate with significantly less regulation than traditional media, which have historically been subject to stricter oversight to ensure the accuracy and reliability of information. This disparity in regulatory standards underscores the importance of developing and implementing more robust regulatory frameworks for digital platforms in order to mitigate the spread of disinformation and protect the integrity of public discourse. Rigorous regulation of online media and Internet platforms is needed, as well as the continual raising of public awareness of disinformation.

This policy brief has three main objectives: (1) to analyse the existing components of the EU's strategy to combat disinformation, particularly the Digital Services Act, which provides the legal framework for digital services, and the Code of Practice on Disinformation; (2) to identify the key limitations and challenges of the current regulations; and (3) to develop policy recommendations and measures to overcome these limitations and address the threat of disinformation in the light of the upcoming elections. The brief emphasises the urgency of implementing the developed policy recommendations and measures before the upcoming elections and the need for a comprehensive, multi-stakeholder approach to safeguard the integrity of democratic processes, prevent the spread of disinformation, and ensure fair and transparent elections across the EU.

Keywords Disinformation – Digital platforms – Digital Services Act – Election integrity

Introduction

In recent years, the influential role of digital platforms and social media in shaping political discourse and influencing voter behaviour has been highlighted by the outcomes of significant elections around the world. Now, in 2024, we find ourselves in a pivotal year for democracy. Over 60 countries worldwide, with their GDP forming more than 50% of the world's total,[1] including more than 10 European nations, are holding elections. The challenges posed by politically driven disinformation have become more pressing than ever. This is particularly true in the context of the European Parliament elections, scheduled for 6–9 June 2024. Recognised as one of the world's largest transnational polls, with over 400 million eligible voters, these elections represent a crucial test for the integrity of the democratic process.

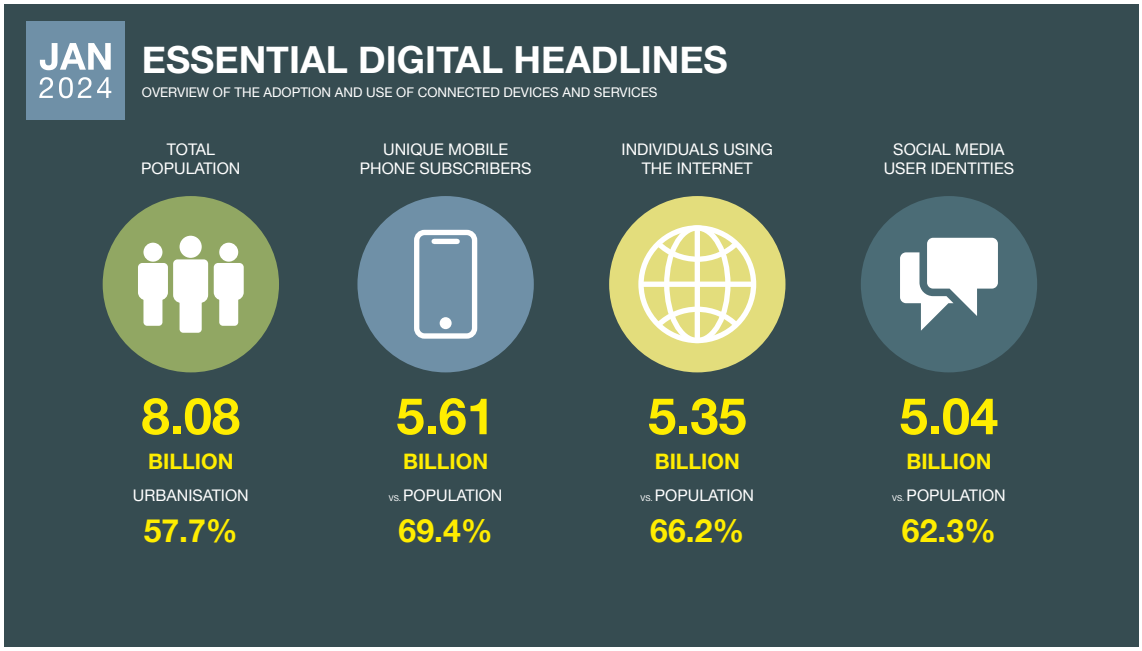
This brief explains the need for regulation and additional preventative measures with regard to disinformation on digital platforms and social media. The need for these measures stems from three important factors.

First, digital platforms are becoming one of the most influential sources of information/disinformation, with their audiences growing and their influence increasing. One or another digital platform has an impact on every Internet user in the world. According to DataReportal,[2] there are 5.04 billion social media users globally today and this number is forecast to reach 5.17 billion by the end of 2024. This means 62% of the global population uses social media and digital platforms, making them potentially exposed to the information/disinformation available on such platforms. The population of the EU is slightly over 448 million people, with an estimated 425 million users of social media platforms. A typical social media user interacts with 6.6 such platforms and, on average, spends 2 hours and 24 minutes daily interacting with digital information on these platforms. Thus, almost every citizen in the EU is exposed to the information available on digital platforms and social media.

1 Brunswick Geopolitical, 'Eight Key Elections to Watch in 2024', *Brunswick Group*, 8 September 2023.

2 S. Kemp, *Digital 2024: Global Overview Report*, DataReportal (31 January 2024).

Figure 1 Overview of the adoption and use of connected devices and services



Source: S. Kemp, *Digital 2024: Global Overview Report*, DataReportal (31 January 2024), reproduced with permission.

The business model of digital platforms incentivises the spread of viral, emotional and engaging content, making such platforms vulnerable to disinformation from which they may profit due to increased user engagement, regardless of accuracy or integrity. Advertisers also frequently overlook the nature of the content that their advertisements accompany, focusing instead on the visibility and reach that their advertising dollars secure.[3] The digital advertising market, valued at approximately €625 billion,[4] thrives on user engagement—clicks, views and interactions—which directly translates into revenue for platforms, advertisers and influencers alike.

Moreover, fabricated content, particularly in the political realm, travels faster and further than truthful content. For instance, false information is 70% more likely to be retweeted than accurate news[5] and Facebook posts containing falsehoods receive six times more engagement than factual content.[6] The third factor is the exponential growth of disinformation. One of the key risks to global society identified in a recent report of the World Economic Forum is the spread of misinformation and disinformation, which has jumped to the number one position within the last

[3] C. Atkin, 'Are Your Ads Funding Disinformation?', *Harvard Business Review*, 21 August 2023.

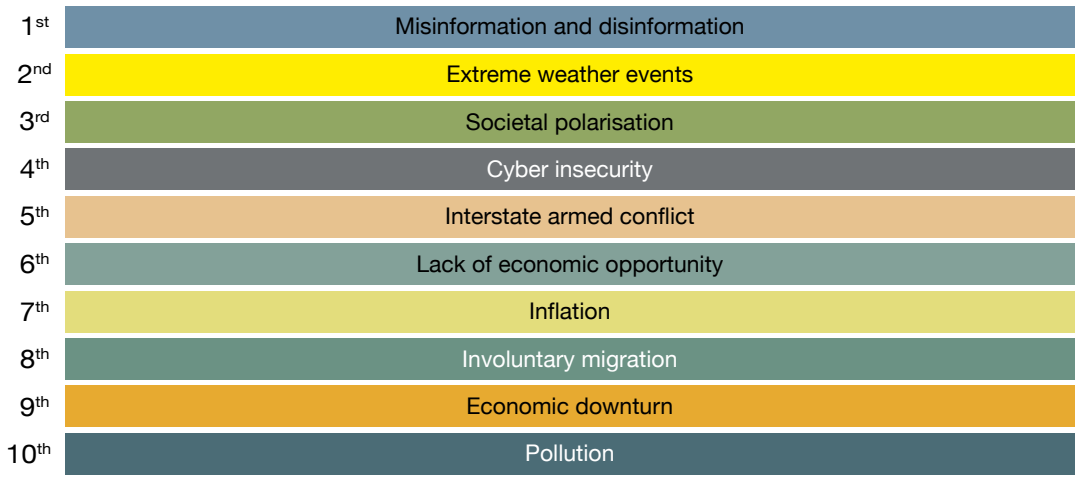
[4] C. Ruiz, 'Disinformation Is Part and Parcel of Social Media's Business Model, New Research Shows', *The Conversation*, 23 November 2023.

[5] S. Brown, 'MIT Sloan Research About Social Media, Misinformation, and Elections', *MIT Management Sloan School*, 5 October 2020.

[6] L. Edelson, 'Understanding Engagement With U.S. (Mis)Information News Sources on Facebook', *Proceedings of the 21st ACM Internet Measurement Conference* (2 November 2021).

two years (see Figure 2).[7] Since the Russian invasion of Ukraine, the spread of disinformation has grown enormously in the EU. Several disinformation campaigns have been uncovered that heavily use digital platforms as a tool to spread fake news and harmful content (e.g. the Doppelganger campaign by Recent Reliable News, a pro-Russian website).[8]

Figure 2 Global risks ranked by severity over the next two years



Source: World Economic Forum, *The Global Risks Report 2024* (10 January 2024).

The weaponisation of disinformation for use in the war in Ukraine and in EU countries is a growing concern. In 2015 the East StratCom Task Force, part of the European External Action Service, established EUvsDisinfo, a database for collecting cases of what the organisation considers pro-Kremlin disinformation. An OECD report published in November 2022 states: 'Since February 2022, [EUvsDisinfo] has tracked more than 237 disinformation cases relating to Ukraine, and more than 5,500 disinformation total cases about Ukraine since its establishment in 2015 (out of more than 13,000 examples of pro-Kremlin disinformation)'.[9] Recent research conducted by the ISE Group across four EU countries (Poland, Germany, France and Austria)[10] indicates a significant increase in the impact of disinformation narratives on socio-economic and political processes. The number of narratives in use has more than doubled in EU countries, with the majority targeting Poland, where over 1,800 were discovered in 2023. These attacks primarily aim to foster

7 World Economic Forum, *The Global Risks Report 2024* (10 January 2024).

8 A. Alaphilippe, *Doppelganger: Media Clones Serving Russian Propaganda*, EU DisinfoLab (27 September 2022).

9 OECD, *Disinformation and Russia's War of Aggression Against Ukraine* (3 November 2022), 19.

10 E. Malitskaya, 'Fighting Russian Disinformation in Europe', *ISE Group*, 14 March 2024.

social division, put pressure on governments to change policies, manipulate the economy and discredit institutions.

The presence of the three factors outlined above explains the need for the additional regulation of digital platforms and social media, as well as the introduction of further preventative measures in society. The next section discusses the current regulations and their limitations.

The key components of the EU's strategy to combat disinformation

The EU's Digital Services Act (DSA) and the Strengthened Code of Practice on Disinformation (hereafter, the Code of Practice) are the two key components of the EU's strategy to combat disinformation. The DSA provides a legal framework for digital services, while the Code of Practice is a self-regulatory tool, through which signatories voluntarily commit to a set of practices to counter the spread of disinformation.

The DSA aims to ensure the transparency of content moderation practices and provide measures to tackle the presence of disinformation, harmful content and hate speech on online platforms such as social networks and content-sharing platforms. The DSA came into force for all platforms on 17 February 2024. The Act also provides a framework for cooperation between the Commission and law enforcement, and for monitoring the implementation of all its obligations.[11] Companies that fail to comply with the DSA's rules could face fines of up to 6% of their global turnover.

To enhance the effectiveness of the DSA, a complementary Code of Practice was developed. This Code provides a detailed framework to help online platforms and other stakeholders combat disinformation, particularly in the context of the EU elections. The Code is a first-of-its-kind tool through which relevant players active in the online information ecosystem in the EU have agreed to self-regulatory standards to fight disinformation. Signed in June 2022, the Code of Practice contains 44 commitments and 128 specific measures, covering demonetising the dissemination of disinformation,

[11] *European Commission*, 'The Impact of the Digital Services Act on Digital Platforms' (3 November 2023).

ensuring the transparency of political advertising, empowering users, enhancing cooperation with fact-checkers, and providing a broad range of commitments and measures to counter online disinformation.

The challenges and limitations of the existing measures

The DSA and the Code of Practice have been criticised for their potential limitations in addressing disinformation during EU elections by a variety of stakeholders—the European Parliament's Committee on Foreign Interference in all Democratic Processes in the EU, Including Disinformation; tech companies; social media platforms; civil society; academic institutions; and fact-checkers. Several specific examples of these criticisms are laid out below.

Lack of clear definition

The DSA lacks a clear legal definition of disinformation, which could lead to fragmentation across EU member states in terms of its application. This could undermine its effectiveness in combating disinformation during EU elections, as different interpretations and applications of the law could result in varying levels of protection for electoral processes. For example, the lack of a definition could result in some EU member states being more aggressive in their interpretation of the law, potentially leading to over-censorship, while others may be more lenient, allowing disinformation to spread.

The Code of Practice defines disinformation as 'verifiably false or misleading information which, cumulatively, (a) is created, presented and disseminated for economic gain or to intentionally deceive the public; and (b) may cause public harm, intended as threats to democratic political and policymaking processes as well as the protection of EU citizens' health, the environment or security'. In this definition, which lacks a legal basis, false or misleading information becomes 'disinformation' through its interaction with 'bad actors': those who disseminate it for economic gain or to deceive. It thus lays the groundwork for firms to regulate disinformation as an issue of bad behaviour, bypassing the more problematic and burdensome idea that these firms should become the arbiters of truth.[12]

[12] S. Galantino, 'How Will the EU Digital Services Act Affect the Regulation of Disinformation?', *SCRIPTed* 20/1 (February 2023).

Challenge of obligations

The DSA primarily imposes the obligation to combat disinformation on very large online platforms (VLOPs), while other digital services that also spread disinformation are not subject to the same obligations or the same level of scrutiny and accountability.

For instance, during the 2022 French presidential election, smaller platforms such as Telegram and Discord were utilised to disseminate disinformation and hate speech without encountering the same level of oversight as that experienced by larger platforms such as Facebook and Twitter. Concerns have also been raised by the European Parliament regarding the absence of regulation for platforms such as Reddit and Telegram, where disinformation proliferates largely unmonitored.[13]

The European Fact-Checking Standards Network (EFCSN) has reviewed the implementation of the Code of Practice by major digital platforms. The EFCSN has criticised some platforms for not fully implementing the measures they have committed to and for misrepresenting their policies in reports. The Network also calls for effective implementation of the DSA on other platforms which are instrumental in spreading disinformation, such as Telegram.[14]

The DSA Observatory has discussed the impact of the DSA on the right to freedom of expression, focusing on risk-mitigation obligations. It suggests that intermediaries (i.e. digital platforms) should be subject to *ex ante* regulatory oversight and required to engage in the adoption of codes of conduct. It also emphasises the need for proper *ex post* assessment of due diligence measures and appropriate appeal mechanisms for all interested parties.[15]

Resources and capacity

Implementing the DSA requires significant financial resources, motivation, the development of private and public enforcement mechanisms, and the modernisation of internal processes to ensure compliance with the new regulations. As an example, platforms are called upon to modernise their internal compliance and organisational designs, which involves investing in the remodelling of internal responsibilities and processes related to content moderation, transparency reports,

---

13 European Parliament, *Resolution on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation*, 2022/2075(INI) (1 June 2023), item AJ.

14 *EFCSN*, 'The EFCSN Reviews Big Tech's Implementation of the EU Code of Practice on Disinformation' (24 January 2024).

15 J. Barata, 'The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations', *DSA Observatory*, 27 July 2021.

advertising restrictions and data access requests.[16] It also requires a mixture of private and public enforcement, which entails additional investment in enforcement mechanisms and processes.[17] On the public side, the engagement of regulatory agencies and government bodies to investigate, sanction and monitor compliance with the DSA's requirements is necessary. Resources must also be allocated to these authorities to enable the effective enforcement of the regulations. On the private side, mechanisms have to be developed to allow private entities, individuals and organisations to take legal action to ensure compliance with the DSA. This may include the ability to bring lawsuits against non-compliant entities or to seek redress for violations through civil courts. It requires investment in the legal processes and mechanisms needed to support private enforcement actions.

The Parliament considers it necessary that the EU supports capacity-building for fact-checking and tackling disinformation. Despite some financial resources being made available, the funding of civil society organisations and the media is fragmented and often project-based, which can dilute the impact of media literacy projects.[18]

Cooperation and engagement

Both the DSA and, particularly, the Code of Practice encourage multi-stakeholder cooperation between online platforms and fact-checkers to combat disinformation. However, the effectiveness of this cooperation depends on the willingness and ability of these parties to engage in these efforts.

For instance, the key commitments of the Code of Practice regarding cooperation between online platforms and fact-checkers include setting up agreements, integrating and using fact-checking services, and providing access to data. However, an analysis by the EFCSN revealed that most VLOPs and search engines are still far from fulfilling their promises of cooperation and do not have effective risk-mitigation measures against disinformation in place, as required by the DSA (see Figure 3).[19]

16 L. Riede, 'The DSA Has Been Signed – Now What? Three Key Strategic Challenges for Platforms', *Freshfields, Bruckhaus*, *Deringer*, 19 October 2022.

17 M. Husovec, 'Will the DSA Work?', *VerfBlog*, 9 November 2022.

18 European Parliament, *Resolution on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation*, item P.

19 *EFCSN*, 'The EFCSN Reviews Big Tech's Implementation of the EU Code of Practice on Disinformation'.

Figure 3 Compliance of VLOPs at a glance

Service	Agreements and fact-checking coverage	Integration and use of fact-checking	Access to information for fact-checkers
YouTube	●	●	●
Google Search	●	●	●
Facebook	●	●	●
Instagram	●	●	●
TikTok	●	●	●
WhatsApp	●	●	●
Bing	●	●	●
LinkedIn	●	●	●
X (formerly Twitter)	●	●	●
Telegram	●	●	●

● No progress or no information

● Not enough progress or not enough information

● Some progress

Source: EFCSN, *Fact-Checking and Related Risk-Mitigation Measures for Disinformation in the Very Large Online Platforms* (January 2024), reproduced with permission.

Integrating multi-stakeholder engagement into the process of implementing policies related to the DSA and the Code of Practice would enable a more balanced and carefully considered approach. For example, at the national level, French law calls for collaboration between platforms and news agencies, publishers and journalists to tackle disinformation.[20]

Regulatory overreach

There are concerns that the DSA's provisions could potentially result in regulatory overreach, with the European Commission having too much power to direct how platforms tackle disinformation, particularly in the context of EU elections. The DSA's requirement for online platforms to remove or restrict access to illegal content, including disinformation, could lead to the removal of legitimate political speech and debate, potentially chilling free expression during election periods.

For instance, the German Network Enforcement Act (NetzDG), which requires social media platforms to remove illegal content within a certain timeframe, has been criticised for leading to the over-blocking of content.[21] This criticism reflects broader concerns that could also be applicable to the DSA's approach to disinformation.

[20] France, *Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information* (22 December 2018).

[21] J. Pohlmann, A. Barbaresi and P. Leinen, 'Platform Regulation and "Overblocking" – The NetzDG Discourse in Germany', *Communications* 48/3 (2023).

If platforms are required to comply with strict content-removal regulations under the DSA, they may similarly err on the side of caution and over-remove content, including during sensitive periods such as EU elections. This could potentially undermine the independence of online platforms by compelling them to act as arbiters of truth, and could stifle innovation by creating a risk-averse environment for platform operators. The NetzDG example serves as a cautionary tale for the implementation of the DSA, highlighting the need for careful consideration of how regulations may affect online discourse and the importance of safeguarding against overreach that could inadvertently harm the democratic processes such regulations seek to protect.

The Electronic Frontier Foundation has expressed concerns about the potential of the DSA to result in enforcement overreach, highlighting the risk of drastic and overbroad government enforcement powers. The Foundation warns that such powers could lead to an unpredictable and inconsistent environment, encouraging forum shopping and potentially enabling abuse in countries with anti–human rights views.[22]

Chatham House has also discussed the global trend towards more active government direction of digital platforms, noting the diversity of approaches and the lack of established norms. This diversity and the pursuit of digital sovereignty could lead to a fragmented 'Venn diagram' of national Internets, potentially undermining openness and the benefits of a global Internet.[23]

Lack of harmonisation

The application of the DSA's provisions is not harmonised across Europe, which may lead to inconsistencies in regulating disinformation during EU elections. Enforcement of the DSA may be challenging in certain countries due to political factors. For instance, obstacles to the implementation of the DSA were experienced in Slovakia in the context of the general elections held on 30 September 2023. The elections were marked by the extensive dissemination of political disinformation across online platforms, highlighting the difficulty of implementing the DSA in environments where political leaders themselves may contribute to this.[24]

---

22 K. Komaitis, 'Enforcement Overreach Could Turn out to Be a Real Problem in the EU's Digital Services Act', *The Electronic Frontier Foundation*, 18 February 2022.

23 Y. Afina et al., *Towards a Global Approach to Digital Platform Regulation*, Chatham House (8 January 2024).

24 T. Hartmann, '"Disinformation Led by Political Leaders": Slovak DSA Enforcement Challenged', *Euractiv*, 21 September 2023.

Furthermore, the DSA introduces rules that are closely related to other areas of law (i.e. data protection, audio-visual media regulation, consumer protection, telecommunications, terrorism content) which are already regulated at the national level.[25] This may lead to inconsistencies in how the DSA is applied across the different member states.

Enforcing the DSA may also be challenging in some EU countries due to the complex interplay between national and EU authorities, and the uncertainty surrounding the practical application of the DSA's rules. This lack of clarity in the rules and the readiness to implement them may impact businesses, especially those that do not operate VLOPs, as they need to have a clear understanding of how the regulations will be applied in practice.

The challenges seen in Slovakia, the relationship between the DSA and other areas of law, and the complex interplay between national and EU authorities all underscore the need for a nuanced approach to DSA enforcement. This includes considering the political context and the role of political leaders in spreading disinformation. It also highlights the importance of collaboration between EU institutions, member states and online platforms to effectively address the multifaceted nature of disinformation and its impact on the democratic process.

Limited impact on artificial intelligence–based amplification

The provisions of the DSA may not have a substantial effect on curtailing the amplification of disinformation by artificial intelligence (AI) at a systemic level. AI algorithms are designed to maximise user engagement, which can inadvertently lead to the rapid spread of sensational or false information. The DSA's focus on transparency may not be enough to counteract the speed and scale with which AI can disseminate disinformation. AI technologies also have the ability to target specific demographic groups with tailored disinformation campaigns, making them powerful tools for influencing electoral outcomes. The current provisions of the DSA might not be robust enough to effectively prevent or counteract such targeted disinformation campaigns, especially if they originate from foreign actors or are conducted through covert methods.[26]

The European Parliament also highlights the crucial role of AI algorithms designed to benefit platforms' business models through the amplification of false

[25] B. Zeybek and J. Hoboken, 'The Enforcement Aspects of the DSA, and Its Relation to Existing Regulatory Oversight in the EU', *DSA Observatory*, 4 February 2022.

[26] J. Heesen, 'AI and Elections – Observations, Analyses and Prospects', *Israel Public Policy Institute*, 2 March 2022.

and misleading narratives. Its resolution highlights how these algorithms create filter bubbles that limit or distort the information available to individual users, and notes that platforms have not done enough to counter this.[27]

Independent fact-checking organisations, such as those involved in research into and analysis of digital media environments, have also pointed out the difficulties of ensuring that digital platforms' algorithms prioritise fact-based, independent journalism over sensational or false information. The Center for News, Technology & Innovation emphasises the need for cross-industry collaboration to ensure that platform algorithms select and prioritise fact-based content, highlighting the challenges posed by algorithmic selection in promoting an informed public.[28]

The European Commission's study on the DSA's risk-management framework for online disinformation campaigns acknowledges the systemic risks posed by AI-driven disinformation, particularly from foreign efforts such as those promoting the ideas of the Kremlin.[29] The study highlights how endeavours by companies including Meta and Twitter to limit the algorithmic amplification of Kremlin-sponsored disinformation have only been partially effective, as they are limited to manually curated sets of accounts and do not address AI-based amplification systemically.

All of the above factors indicate a recognition of the limitations of the current provisions of the DSA to effectively address AI-driven disinformation campaigns.

Approaches to addressing the challenges and limitations

In the light of this upcoming year of elections, it is necessary to create a list of policy recommendations that places the maximum focus on both ensuring the public's awareness of disinformation and engaging with multiple stakeholders. The main goal of this brief is to reach as many interested parties as possible and to raise public awareness of and build societal resilience to disinformation in the EU.

27 European Parliament, *Resolution on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation*, item AN.

28 *Center for News, Technology & Innovation*, 'How Can We Ensure That Algorithms Identify and Promote Fact-Based, Independent Journalism?' (8 February 2024).

29 European Commission, *Digital Services Act: Application of the Risk Management Framework to Russian Disinformation Campaigns* (Luxembourg, August 2023).

While formulating these policy recommendations we cross-checked them with a number of previous studies and the opinions of the independent fact-checking agencies, government institutions and intergovernmental organisations mentioned in the previous section. We have selected the most frequently mentioned and most urgent policy recommendations that would both reach the broader public and overcome the limitations of the DSA and the Code of Practice.

The table below summarises the list of policy recommendations and measures in its rows and the issues in the columns. Where a tick appears at the intersection of the two, it means that the respective policy recommendation helps to overcome these limitations of the DSA or the Code of Practice. Most of the selected policy recommendations could be implemented quickly to help to combat disinformation during the election period.

Please note that this is not an exhaustive list of policy recommendations, but simply a list of the most substantial and impactful, to be implemented as soon as possible, selected based on the criteria of quick implementation and strong public outreach.

Table 1 Policy recommendations

Policy recommendation	Description	Lack of clear definition	Challenge of obligations	Resources and capacity	Cooperation and engagement	Regulatory overreach	Lack of harmonisation	Limited impact on AI
Multi-stakeholder disinformation summits	Regular summits with various stakeholders to find alignment on disinformation strategies.	✔	✔	✔	✔		✔	✔
Disinformation resilience index	An index measuring resilience to disinformation across the member states.	✔			✔			
Diplomatic disinformation dialogues	High-level dialogues with countries involved in disinformation campaigns.		✔		✔			✔
Disinformation intelligence centre	A body set up to analyse and respond to disinformation campaigns using AI.						✔	✔

Policy recommendation	Description	Lack of clear definition	Challenge of obligations	Resources and capacity	Cooperation and engagement	Regulatory overreach	Lack of harmonisation	Limited impact on AI
Blockchain verification	Use of blockchain technology to create immutable records of political advertising and moderation.		✔					✔
Disinformation firewall	Use of AI-driven tools to filter out disinformation content.							✔
Open AI for disinformation detection	Use of open-source AI solutions to detect disinformation at scale.		✔		✔			✔
Promotion of digital literacy as a fundamental right	Advocacy of digital literacy as a fundamental right for all citizens.			✔				
Public awareness campaigns	Campaigns to raise public awareness about the risks of foreign interference.	✔	✔		✔	✔		✔
Resilience training for public officials	Training for officials on securing the digital presence and responding to disinformation.			✔	✔	✔	✔	
Civic engagement grants	Grants for local initiatives promoting civic engagement and democracy support, and for acting as disinformation watchdogs.			✔	✔			
Disinformation rating system	A rating system assessing the reliability of online information sources.	✔		✔				
Self-regulatory council	An industry-led council to enforce standards and mediate disinformation disputes.		✔			✔		
Public–private partnership programmes	Programmes incentivising collaboration on disinformation countermeasures.			✔	✔			✔

Source: Author's own compilation.

The matrix below categorises the policy recommendations based on their potential impact and the time needed for implementation. This impact scale is used to assess the potential effectiveness of a given recommendation in achieving its intended outcomes—that is, preventing the spread of disinformation and ensuring fair and transparent elections in the EU. Regarding the time for implementation, those marked as suitable for short-term implementation could be set up relatively quickly, within a few months, while short- to long-term recommendations could be implemented quickly but will require sustained effort over time to achieve their full impact. Those marked as being for 'long-term implementation' may take a year to put in place.

Table 2 Impact and implementation timelines for policy recommendations

	Short-term implementation	Short- to long-term implementation	Long-term implementation
High impact	→ Multi-stakeholder disinformation summits	→ Public–private partnership programmes	→ Legal cyber-diplomacy framework → Blockchain verification
Moderate impact	→ Public awareness campaigns	→ Open AI for disinformation detection → Resilience training for public officials	→ Disinformation firewall → Promotion of digital literacy as a fundamental right
Low impact	→ Civic engagement grants → Self-regulatory council	→ Diplomatic disinformation dialogues → Disinformation rating system	

Source: Author's own compilation.

Taking the above into consideration, the following five policy measures are recommended and should be implemented:

- multi-stakeholder disinformation summits,
- public–private partnership programmes,
- public awareness campaigns,
- resilience training for public officials, and
- open AI for disinformation detection.

Policy recommendations

Combating disinformation should be of serious concern for European policymakers. European member states and Brussels need to get to grips with the fact that various political actors are spreading malicious disinformation and potentially harmful content with the aim of destabilising democracies and socio-political relations in the EU, creating socio-economic conflicts and tension, influencing governments and misleading the population during elections. With the use of emerging technologies such as AI and deepfakes, the spread of disinformation will be even quicker and potentially more harmful. Thus, the EU has to be on track to develop and enforce proper regulations and must continually review the implementation of new measures.

The EU should put additional shared resources into research and uniting efforts to combat disinformation. It is important to focus on measures that (1) could be applied in the short term, (2) address the broadest range of challenges and limitations, and (3) have a significant impact. In this regard, it makes sense to concentrate on implementing the most urgent policy recommendations.

The five policy recommendations selected for implementation above are:

1. *Multi-stakeholder disinformation summits.* The organisation of such events would encourage dialogue and cooperation among the various stakeholders, and could lead to the building of comprehensive strategies to protect against disinformation. The European Commission, with its experience of establishing the Code of Practice, would be well-suited to lead these summits, bringing together government representatives, technology firms, civil society and academia. The summit agenda could include discussion of the setting up of a disinformation resilience index, a disinformation intelligence centre and diplomatic disinformation dialogues, among other tools.

2. *Public–private partnership programmes*. Setting up such partnerships would facilitate collaboration between governments and the private sector, particularly technology companies, to combat disinformation. The European Commission's Directorate General for Communications Networks, Content and Technology should spearhead such programmes, leveraging private-sector resources and expertise.

3. *Public awareness campaigns*. The implementation of public awareness campaigns would educate the public on disinformation and its countermeasures. The Directorate General for Communication of the European Commission should lead these campaigns, using various media channels to raise public awareness and enhance societal resilience to disinformation.

4. *Resilience training for public officials*. Such training would equip officials with the skills needed to recognise and counter disinformation. The European Institute of Public Administration should offer these trainings, ensuring that public officials are prepared to safeguard the integrity of public institutions and democratic processes.

5. *Open AI for disinformation detection*. The recommendation here is to invest in open-source AI solutions that can detect and flag disinformation at scale. This investment is crucial to enhance the capabilities of the various stakeholders to identify and mitigate the spread of false information. The European Innovation Council and Small and Medium-sized Enterprises Executive Agency, in collaboration with research institutions and technology companies, is considered the ideal entity to lead the development and deployment of these AI tools. By leveraging open-source frameworks, these solutions can be widely adopted, adapted and improved upon, contributing to a more resilient information ecosystem across the EU.

Conclusion

Disinformation, a modern weapon with a devastating potential to disrupt society, poses a clear and present danger to the integrity of European elections. This weapon of mass manipulation demands a multifaceted response, one that goes beyond mere policy statements and requires a collective effort from all stakeholders. EU leaders must engage the broader public and dedicate maximum resources across various levels to this threat. This combating of disinformation can be effectively waged through the combined efforts of a wide range of stakeholders, including:

- EU policymakers—by championing robust regulations and fostering international and multi-stakeholder cooperation to disrupt disinformation at its source.
- Big tech companies and digital platforms—by implementing transparency measures, removing harmful content and collaborating with fact-checkers to curb the spread of disinformation.
- Fact-checkers and the media—by building trust through verifying information, providing media literacy training and debunking disinformation campaigns.
- Think tanks and researchers—by providing continuous analysis, identifying emerging trends and providing expertise to develop strategies against disinformation.
- Civil society—by promoting media literacy and awareness campaigns, engaging in the monitoring of disinformation and reporting suspicious content.
- The broader public—by engaging critically with information, reporting suspicious content and advocating for online spaces free from manipulation.

By actively engaging all stakeholders and continuously reviewing and updating its recommendations, the EU can build a robust shield against disinformation, ensuring its elections remain the cornerstone of its democratic values.

Bibliography

Afina, Y. et al., *Towards a Global Approach to Digital Platform Regulation,* Chatham House (8 January 2024), accessed at https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation/02-global-regulatory-trends.

Alaphilippe, A., *Doppelganger: Media Clones Serving Russian Propaganda,* EU DisinfoLab (27 September 2022), accessed at https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf.

Atkin, C., 'Are Your Ads Funding Disinformation?', *Harvard Business Review*, 21 August 2023, accessed at https://hbr.org/2023/08/are-your-ads-funding-disinformation.

Barata, J., 'The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations', *DSA Observatory*, 27 July 2021, accessed at https://dsa-observatory.eu/2021/07/27/the-digital-services-act-and-its-impact-on-the-right-to-freedom-of-expression-special-focus-on-risk-mitigation-obligations/.

Brown, S., 'MIT Sloan Research About Social Media, Misinformation, and Elections', *MIT Management Sloan School*, 5 October 2020, accessed at https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections.

Brunswick Geopolitical, 'Eight Key Elections to Watch in 2024', *Brunswick Group*, 8 September 2023, accessed at https://www.brunswickgroup.com/eight-key-elections-to-watch-in-2024-i25831/.

Center for News, Technology & Innovation, 'How Can We Ensure That Algorithms Identify and Promote Fact-Based, Independent Journalism?' (8 February 2024), accessed at https://innovating.news/article/algorithms-quality-news/.

Edelson, L., 'Understanding Engagement With U.S. (Mis)Information News Sources on Facebook', *Proceedings of the 21st ACM Internet Measurement Conference* (2 November 2021), doi:10.1145/3487552.3487859.

EFCSN, *Fact-Checking and Related Risk-Mitigation Measures for Disinformation in the Very Large Online Platforms* (January 2024), accessed at https://efcsn.com/wp-content/uploads/2024/03/EFCSN-%E2%80%93-Fact-checking-and-related-Risk-Mitigation-Measures-for-Disinformation-in-the-Very-Large-Online-Platforms.pdf.

EFCSN, 'The EFCSN Reviews Big Tech's Implementation of the EU Code of Practice on Disinformation' (24 January 2024), accessed at https://efcsn.com/cop-review/.

European Commission, *Digital Services Act: Application of the Risk Management Framework to Russian Disinformation Campaigns* (Luxembourg, August 2023), accessed at https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1.

European Commission, 'The Impact of the Digital Services Act on Digital Platforms' (3 November 2023), accessed at https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms.

European Parliament, *Resolution on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation*, 2022/2075(INI) (1 June 2023), accessed at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.pdf.

France, *Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information* (22 December 2018), accessed at https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000037151987.

Galantino, S., 'How Will the EU Digital Services Act Affect the Regulation of Disinformation?', *SCRIPTed* 20/1 (February 2023), accessed at https://script-ed.org/article/how-will-the-eu-digital-services-act-affect-the-regulation-of-disinformation/.

Hartmann, T., '"Disinformation Led by Political Leaders": Slovak DSA Enforcement Challenged', *Euractiv*, 21 September 2023, accessed at https://www.euractiv.com/section/law-enforcement/news/disinformation-led-by-political-leaders-slovaks-dsa-enforcement-challenged/.

Heesen, J., 'AI and Elections – Observations, Analyses and Prospects', *Israel Public Policy Institute*, 2 March 2022, accessed at https://www.ippi.org.il/ai-and-elections-observations-analyses-and-prospects/.

Husovec, M., 'Will the DSA Work?', *VerfBlog*, 9 November 2022, accessed at https://verfassungsblog.de/dsa-money-effort/.

Kemp, S., *Digital 2024: Global Overview Report*, DataReportal (31 January 2024), accessed at https://datareportal.com/reports/digital-2024-global-overview-report.

Komaitis, K., 'Enforcement Overreach Could Turn out to Be a Real Problem in the EU's Digital Services Act', *The Electronic Frontier Foundation*, 18 February 2022, accessed at https://www.eff.org/deeplinks/2022/02/enforcement-overreach-could-turn-out-be-real-problem-eus-digital-services-act.

Malitskaya, E., 'Fighting Russian Disinformation in Europe', *ISE Group*, 14 March 2024, accessed at https://ise-group.org/disinformation.

OECD, *Disinformation and Russia's War of Aggression Against Ukraine* (3 November 2022), accessed at https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

Pohlmann, J., Barbaresi, A. and Leinen, P., 'Platform Regulation and "Overblocking" – The NetzDG Discourse in Germany', *Communications* 48/3 (2023), 395–419, doi:10.1515/commun-2022-0098.

Riede, L., 'The DSA Has Been Signed – Now What? Three Key Strategic Challenges for Platforms', *Freshfields, Bruckhaus, Deringer*, 19 October 2022, accessed at https://technologyquotient.freshfields.com/post/102hzio/the-dsa-has-been-signed-now-what-three-key-strategic-challenges-for-platforms.

Ruiz, C., 'Disinformation Is Part and Parcel of Social Media's Business Model, New Research Shows', *The Conversation*, 23 November 2023, accessed at https://theconversation.com/disinformation-is-part-and-parcel-of-social-medias-business-model-new-research-shows-217842.

World Economic Forum, *The Global Risks Report 2024* (10 January 2024), accessed at https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

Zeybek, B. and Hoboken, J., 'The Enforcement Aspects of the DSA, and Its Relation to Existing Regulatory Oversight in the EU', *DSA Observatory*, 4 February 2022, accessed at https://dsa-observatory.eu/2022/02/04/the-enforcement-aspects-of-the-dsa-and-its-relation-to-existing-regulatory-oversight-in-the-eu

About the author

Alexander Românishyn is a policymaker and economist, having served as Deputy Minister of Economy of Ukraine. His expertise in public policy, corporate finance, digital transformation and resilience has been instrumental in shaping economic, innovation and digital strategies, as well as in the recovery efforts of Ukraine. In the private sector, Alexander has led numerous successful merger and acquisition transactions in the Central and Eastern European region with EY, Midland Group UK and Volwest Group. Additionally, he has contributed to research and publications in digital, technology, disinformation, innovation and related fields. Românishyn holds a Master's degree in Finance and a Bachelor's degree in Economics and Business from the National University of Kyiv-Mohyla Academy and is a dedicated mentor in the European innovation ecosystem.

Credits

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party, dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE 1000

For more information, please visit www.martenscentre.eu.

Internal editor: Dimitar Lilkov, Senior Research Officer
External editing: Communicative English bv
Typesetting: Victoria Agency

Printed in Belgium by INNI Group

This publication receives funding from the European Parliament.