Memo: Known information interference operations during the June 2024 elections for the European Parliament

October 2024

I. Purpose, scope and sources

1. The Vice-President of the European Commission for Values and Transparency, Věra Jourová, visited half of the EU Member States between January and June 2024, in a 'Democracy Tour' in preparation of the elections for the European Parliament held on 6 to 9 June 2024. She discussed key aspects of the Commission recommendation on inclusive and resilient elections with national authorities responsible for conduct and integrity of elections and with representatives of civil society.
2. The 'Democracy Tour' focused on the resilience of the informational space online, and four key areas of particular threat emerged from the discussions with stakeholders: **disinformation, foreign interference, the use of Artificial Intelligence (AI) technologies, and cybersecurity risks.**
3. This Memo gathers the incidents recorded during the electoral period in connection to the four threat areas, based on data available at the time of writing. It focuses exclusively on aspects related to the information space online and does not cover other aspects such as the organisation of elections or physical threats.
4. It is a working document prepared to support discussions in the framework of the European Cooperation Network on Elections on 11th October 2024 on the 2024 elections for the European Parliament and closing the 'Democracy Tour'. Prepared under the authority of the Vice-President[1], it is offered as input to the ongoing preparatory work on the Commission's broader post-election report, as announced in the Defence of Democracy Package issued by the Commission in December 2023.
5. **Based on currently available information, no major information interference operation capable of disrupting the elections was recorded. At the same time, it is widely recognised that the threat levels for information integrity during elections were high, as confirmed by the activation by the European Council of the Integrated Political Crisis Response (IPCR) arrangements for addressing foreign interference[2].**
6. To build situational awareness of the threat landscape during the election period, it has been necessary to draw upon information sources from civil society, the private sector, Member States, political parties, and EU institutions.[3] The sources supporting this memo include:

- Reports from European institutions and agencies, such as the European External Action Service (EEAS), the European Union Agency for Cybersecurity (ENISA), Europol, the Joint Research Centre (JRC), the services of the European Parliament and reporting from the Authority for European Political Parties and European Political Foundations (APPF).
- Reports from EU-level bodies and cooperation networks for national authorities, such as the European Board of Digital Services Coordinators and the NIS Cooperation Group, as well as exchanges with the European Cooperation Network on Elections (ECNE).

- Reports from national authorities.
- Publicly reported studies from civil society, including the elections report of the European Digital Media Observatory (EDMO) and the information bulletin of its elections Task Force.
- Two surveys of political parties.
- Reports from online platforms and other signatories under the Code of Practice on Disinformation[4], as well as in response to the Commission's DSA guidelines on elections.
- The database of statements of reason established under the Digital Services Act[5].
- Other publicly accessible reports from industry.

II. Disinformation

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.[6]

Key instruments in place

7. A joint press release[7] summarises the EU Institutions' approach to tackling disinformation in the European elections, including policies and legislation, raising awareness raising, building societal resilience through media literacy and fact-checking, and cooperation with relevant institutions. The EU institutions also focused on effective communication and raising awareness.

8. The Commission's pre-election Recommendation[8] (2023, part of the Defence of Democracy package) encouraged Member States to take additional measures to protect the election environment and ensure that voters receive correct information. It proposed to further develop public awareness, media literacy and critical thinking, and to support messages pre-bunking or debunking information manipulation and disinformation in elections. It also called on Member States to develop training to relevant authorities and facilitate cooperation among relevant stakeholders to tackle the information manipulation risks.

9. The ECNE intensified its preparedness, including taking part in the High-Level Event of Elections, a joint session with the Rapid Alert System and the NIS Cooperation Group and eight thematic sessions, including on inclusive participation and communication to countering disinformation and ensuring cyber security and smooth organisation of voting for different groups of voters and candidate safety.

10. A post-election report[9] published by the European Board of Digital Services Coordinators summarises all actions taken under the framework of the Digital Services Act (DSA) for elections-preparedness, including stress-tests conducted with online platforms, regulatory dialogues, and cooperation under the Code of Practice on Disinformation and with the European Digital Media Observatory's elections task force, as well as the work of the Board and of the individual Digital Services Coordinators in the Member States.

11. The Digital Services Act sets obligations for online platforms to tackle elections interference and risks to civic discourse. Very large online platforms and search engines must mitigate risks stemming from the design, functioning or use made of their service. All platforms need to set clear terms and conditions, and to put in place due process in their content moderation, including effective complaints mechanisms. They also have to report on restrictions on content and suspended accounts, including through a public database[10].

12. The Commission issued guidelines[11] on how very large online platforms and very large search engines should tackle risks related to elections. Formal proceedings under the Digital Services Act were launched by the Commission against Meta and X for matters related to platforms manipulation, coordinated inauthentic behaviour and deceptive advertisements used to disseminate disinformation campaigns. The Commission also sent over fifty Requests for Information (RFIs) to designated Very Large Online Platforms and Search Engines including in relation to election risk mitigation measures and disinformation. Such RFIs send a strong signal, sometimes resulting in direct corrective action.

13. The Digital Services Act is complemented by the strengthened Code of Practice on Disinformation. Under the Code, online platforms made a series of commitments, including cooperation with civil society and fact-checkers.

To tackle election-related disinformation, a Rapid Response System between online platforms, civil society and fact-checkers was established under the Code. Based on the Code's relevant Commitments[12], the system enabled non-platform signatories to swiftly report to the platforms content, accounts or trends that pose a threat to the electoral process with the possibility of quick reaction and feedback by platforms. The signatories also committed to provide – ahead of and after the elections - targeted reporting on the measures put in place to reduce the spread of disinformation, information manipulation and foreign information manipulation and interference (FIMI) in relation to the elections.

14. The European Digital Media Observatory (EDMO) established a Task Force dedicated to the European Parliament elections[13], to monitor the European information space during the electoral period. The Task Force was assisted by a pool of AI experts to swiftly detect and expose deceptive or misleading AI-generated content. It covered the whole geographic area of the EU through all EDMO national and regional hubs. The Task Force produced daily briefs on urgent disinformation narratives, weekly insights with deeper analysis of disinformation trends, early warnings and conducted targeted investigations. It also conducted an EU-wide media literacy campaign to raise citizen awareness about the risks of disinformation during elections.

15. The new Regulation on the transparency and targeting of political advertising. While most of its provisions will take effect as of 10 October 2025, some elements were applicable already during the European Parliament elections, such as the definitions of key terms include 'political advertising' and the requirement to provide political advertising services without discrimination based on place of residence or establishment.

1. What happened? Key take-aways

16. **During the electoral period, there was an increase in the volume of disinformation related to the organisation of the elections themselves. The narratives sought to diminish trust into the organisation of the ballots and to undermine the credibility of the results. This was only a small part of the disinformation liable to influence the voters. Other, more frequent narratives addressed topics of key societal interest in an attempt to undermine trust in democratic institutions. Online platforms reported under the Code of Practice on Disinformation and the DSA on the measures taken and volumes of disinformation content actioned.**

i. Disinformation narratives

17. According to the European Digital Media Observatory (EDMO)[14], the main disinformation narratives about the EU encountered on social media platforms were:

- False stories questioning election integrity, including allegations of invalid ballots with holes or corners cut, in an attempt to discredit the ballots for the visually impaired[15], and allegations of vote fraud, vote rigging and tampering, as well as fabricated images and stories portraying the EU institutions and leadership as corrupt[16].
- False narratives alleging the escalation of the war in Ukraine and direct involvement of EU countries in the conflict, such as the false story on the 'Ukraine solidarity tax'[17] and incurring EU costs of over USD 630 billion, and conspiracy theories for example about child trafficking involving the foundation of the Ukrainian President's wife and other acts of cruelty, like organ harvesting from Ukrainian soldiers while still alive.
- Recurring false narratives on climate change, including climate denialism and conspiracy theories.
- False content portraying migrants as 'seizing power' in the EU, recycling old stories and linking them to present events.

18. EDMO's monthly assessments of how much of the total disinformation detected on online platforms was directly EU-related show a clear increase in the key periods for the electoral

process. Between May 2023 and March 2024, the figures were between 4% and 8%. In May 2024, the figure rose to 15%, the highest level since monitoring began.[18]

19. While this reflects a significant rise in EU-related disinformation, issues such as Covid-19, Ukraine, and the Israel-Hamas conflict have at times represented 30-60% of all observed disinformation. This general trend is confirmed by the study[19] carried out to assess the structural indicators under the Code of Practice on Disinformation: only 5% of the disinformation posts detected in the sample were directly referring to civic and election integrity. Medical and war-related disinformation were found to account for 16-17%, each, of the total content detected in the sample.

20. Beyond online platforms, the automated clustering[20] of articles from a list of websites repeatedly found by fact-checkers to be publishing disinformation[21] shows that the main topics covered by such websites are similar to those covered by disinformation narratives on social media.

21. The peak in the production of articles on such websites was found to have happened in the period from two weeks ahead of the ballots until election days. This is an indication of efforts to influence the elections. The same pattern was recognised in the case of national elections in some of the EU Member States in 2023.

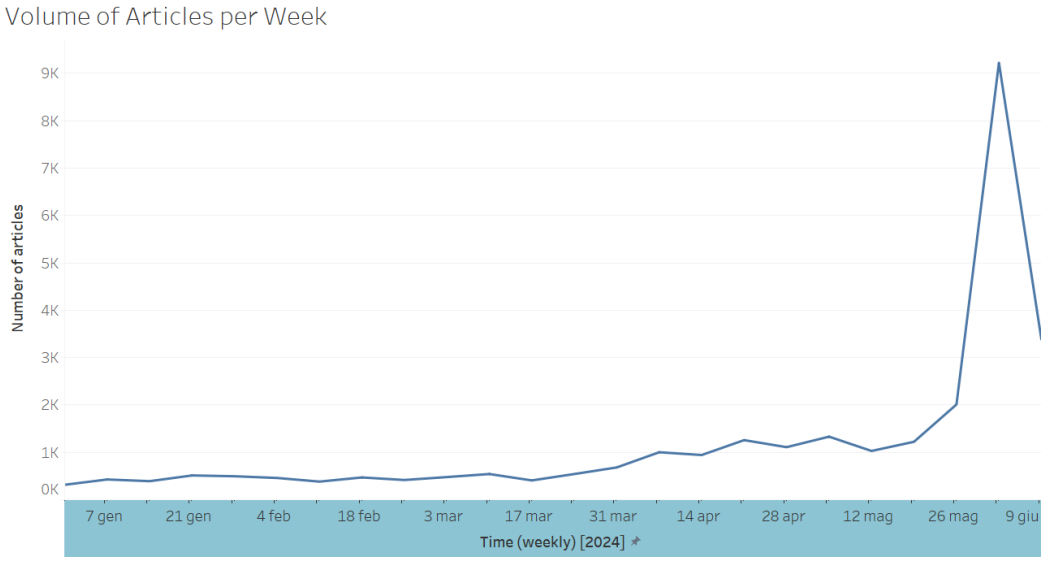

Figure 1 Volume of articles on the EP elections from unverified sources, per week (1st January 2024-10th June 2024). Source: internal analysis by the JRC

ii. Disinformation on online platforms

22. During the electoral period, specific actions were taken by online platforms, in cooperation with civil society, including dedicated policy changes, support and cooperation with fact-checking organisations, pre-bunking actions and cooperation with authorities.[22] They also actioned content, by providing additional information (e.g. fact-checking labels) or removing it.

23. Under the Rapid Response System established through the Code of Practice on Disinformation, fact-checkers and civil society sent 18 notifications, including multiple pieces of content, of which 12 were actioned.[23] Just under half of the notifications were addressed to

Meta, around one third to YouTube and around one third to TikTok. Platforms provided feedback on all these flags - which pertained to different types of content, such as political advertising, or accounts impersonating or amplifying political actors. The reports from signatories show that this cooperation was seen as successful by all actors involved.

24. Platforms state that they generally action content based on the definitions of disinformation (and, often, misinformation[24] and other types of related content, like incitement to violence) established in their terms and conditions. A precise comparison cross-service on the scale of disinformation spread is difficult to make. Examples from the figures reported under the Code of Practice on Disinformation include[25]:

    - Meta removed[26] from its services almost 1.6 million pieces[27] of content in EU Member States that violated bullying and harassment, hate speech, and violence and incitement policies. Misinformation labels were added to over 11.3 million pieces of misinformation, and 3,200 ads were removed under the misinformation policy.[28]
    - YouTube terminated over 1,000 channels and removed 140 EU elections-related videos, applying their general terms and conditions.
    - TikTok removed[29] over 2,600 pieces of content for violating its civic and election integrity policies, and over 43,000 of violating misinformation policies.[30]

25. An analysis[31] of 1,321 posts in 26 Member States fact-checked as disinformation by the European Fact-Checking Standards Network's Elections24Check project between February and June 2024 found that 45% of examples received no visible action by the very large online platforms. The study found that Meta took action on around 80% of the posts, TikTok 40%, X 30%, and YouTube 25%.

26. TikTok and YouTube had the highest rate of engagement with content considered to be disinformation – i.e. largest number of views or interactions with the content. But the content was harder to find on these platforms by searching for keywords, according to the measurement of the 'Structural Indicators' under the Code of Practice on Disinformation[32]. Facebook and Instagram were found to have higher levels of discoverability[33], but lower levels of engagement.

27. Overall, the tests show[34] that it was easier to discover disinformation content by searching for keywords on online platforms than in previous periods tested: the rate of disinformation discoverability was 21% across platforms and countries. Among the list of Member States covered by the tests, it was easiest to discover content in Spain, followed by France, Poland and Slovakia. While the indicators cover a limited number of platforms and countries, they appear to be a useful tool for comparative analysis beyond reporting on volumes of actioned content.

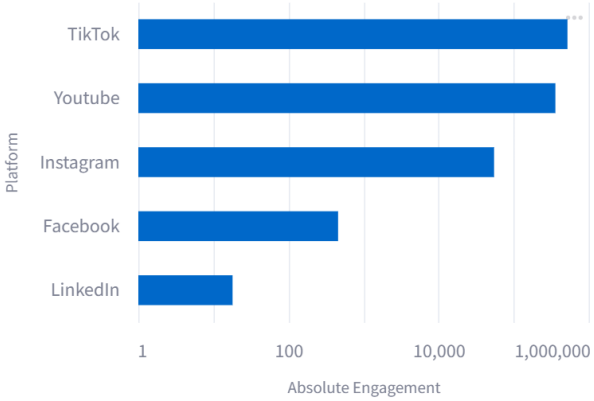

Figure 2 Absolute engagement with disinformation content over the electoral period (based on 3 tests) Source: TrustLab - Code of Practice 2 - Dashboard

28. Some online platforms have reported on the source of disinformation narratives traced on their service, following the DSA guidelines on elections[35]. For example, Meta reported that the majority of threats targeting the elections were domestic rather than foreign, with most of the disruptions taking place in Croatia, France, Germany, Poland and Italy. They observed relatively small information manipulation networks linked to individuals associated with local elections or campaigns, mainly focused on inauthentic amplification.[36]

29. In addition, some research noted that algorithmic recommendations potentially mislead social media users, without necessarily linking to mis- or disinformation content. An experiment conducted on German language TikTok carried out searches for politicians and political parties. The results found that while 30% of search results produced links to relevant factual information, but over half of search results promoted unrelated materials or diverted users to information about other parties.[37]

2. Evolving risks

30. EDMO's Task Force for the European Parliament Elections contributed clear and consistent data about narratives associated with disinformation. Its reporting showed that most narratives have cross-border spillovers, but they are often adapted to the specific national contexts The snapshot of narratives overlapping with future European elections is likely to evolve.

31. Reports observed that political polarisation, mis- and disinformation, and specific incidents of harassment and violence contributed to an 'antagonistic environment' for politicians and candidates, media outlets, and journalists in member states, most significantly targeting women, LGBTI, and immigrant communities.[38]

32. Some political parties flagged that the tone of the electoral debate was not only influenced by disinformation, but also by harassment and different forms of violence. 20 political parties[39] stated that they had recorded incidents of violence against their candidates. This included not only physical violence, but also smear campaigns online, in particular against female candidates, young candidates, national minorities and people of colour, as well as replies to political content with trans- and homophobic content.

33. This begs a context-specific situational awareness for each election to provide a clearer picture of the quality of discourse and threats to political participation. This should account for the methodological challenges encountered in gathering data for this analysis: lack of aligned definitions, and of a systematic understanding of the interaction between disinformation and the overall tone of debate, as well as related issues such as online harassment, threats, and violence.

III. Foreign interference: Foreign Information Manipulation and Interference (FIMI)

Foreign interference in the information space, 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.[40]

FIMI is a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.[41]

Key instruments in place

34. On 24 April 2024, the Belgian Presidency activated the Integrated Political Crisis Response (IPCR)[42] arrangements in information-sharing mode in relation to foreign interference in the framework of the June 2024 European elections. This facilitated exchange of information among Member States and EU institutions.

35. A series of actions were taken by the European External Action Service (EEAS). Since important advancements were made, in cooperation with the European Centre of Excellence for Countering Hybrid Threats in Helsinki, to improve the understanding of hybrid threats to address the phenomenon by which actors seek to exploit vulnerabilities by using in a coordinated way a mixture of diplomatic, technological, and other measures.

36. The Strategic Compass on Security and Defence, which includes an EU Hybrid Toolbox brins together all the relevant instruments to hybrid threats for elections, including the FIMI Toolbox.

37. The Rapid Alert System coordinated by the EEAS supported the cooperation across Member States, including during the European elections, in addition to wider-scope of the cooperation between Member States in ECNE.

38. The EUvsDisinfo website and social media, run by EEAS and supported by their situational analysis capability and strategic communication, were regularly reporting about elections interference by Russia and its proxies.

39. The new tools under the DSA ensured that online platforms contribute to the solutions - including through a table-top exercise, roundtable discussions with platforms, the guidelines set by the Commission, and ongoing investigations into X and Meta's compliance with the rules, which also address FIMI aspects.

40. The Code of practice on disinformation was also an important tool of cooperation and delivered practical solutions, not least through the above-mentioned Rapid Response System and the unprecedented transparency reporting.

41. Through its EU-wide network of researchers and fact-checkers, EDMO conducted in-depth investigations into foreign information manipulation operations.

42. Regulation 2024/900 on the transparency and targeting of political advertising, once applicable, will limit political advertising in electoral periods to sponsors who are citizens of the Union or fulfil other conditions. Aspects beyond the concerns in the information space are addressed in the Commission's pre-elections Recommendation and Regulation 1141/2014 on the statute of funding of European Political Parties and European Political Foundations.

1. What happened? Key take-aways

43. **A handful of major Kremlin-linked operations that remained active during the election period have been exposed at the time of writing this analysis. The tactics, techniques and procedures (TTPs) used in these campaigns helps to define the FIMI risk profile that the EU elections faced from FIMI.**

44. The following examples illustrate the main tactics, techniques and procedures used in FIMI operations led by Russia-linked actors likely active during the electoral period.

45. The websites of the Czech News Agency and Polish Press Agency were hacked in April and May 2024. False reports on the alleged assassination of the Slovak President, Peter Pellegrini by Ukrainians, were published on the Czech's Agency's website[43]. The hackers published an article on the Polish's Press Agency that falsely informed about a call to mobilisation to go to Ukraine by Prime Minister Tusk. This is consistent with the Ghostwriter[44] tactics, but no formal attributions have been made.[45]

46. According to internal documents assessed in an extensive FBI affidavit as well as by a consortium of independent media outlets, the Russian Social Design Agency (SDA) is responsible for a range of Kremlin led information interference operations around the world, including in EU countries.[46] Operations Doppelganger, Matryochka, Overload, and Portal Kombat share characteristics of SDA's strategies, though the exact boundaries between operations is at present unclear.

47. Doppelganger[47] activities targeting the EU Parliamentary Elections were detected in France and Germany, and to a lesser extent Poland, Italy and Spain. The European External Action Service's investigation[48] found that 7 legitimate media outlets were impersonated, while 47 other inauthentic news outlets were used to promote FIMI about the elections. Thousands of inauthentic accounts on X and Facebook were used to drive traffic to over 100 articles that mentioned the elections.[49] Over 1,200 posts were discovered on X during June 2024 that appear to follow the sharing pattern associated with Doppelganger. The focus of the posts was to cease support for Ukraine, discredit Western governments and political parties, and to generate fear around the decline of the West. Those posts generated over 4 million views.[50]

48. Matryochka posts fake content, such as reports, graffiti, and memes, and has been active since September 2023. The approach typically uses two layers of sock puppet accounts. The first group seeds the fake content, while the second group quotes the materials and attempts to overwhelm media outlets, public figures, and fact checkers with spurious requests to investigate the fake content.[51]

49. Similarly, Overload targeted 800 fact checking organisations and newsrooms sending fake content through tweets and over 200 emails, with the intent to overload their capacity. Fact checkers have produced over 250 articles that debunk these deliberately created fake assets, demonstrating some success for the campaign.[52]

50. From early June, accounts using techniques associated with Matryochka and/or Overload adapted to include QR codes in their social media posts that could potentially be weaponised to deliver malicious code or redirect to harmful websites.[53]

51. Possibly in conjunction with Portal Kombat[54], 55 articles were published across the Russian 'Pravda' network in multiple Member States and languages reporting on the results of the European elections having negative consequences for Ukraine. A targeted EDMO investigation found that the network spread significantly ahead of the elections, and activated in 19 additional EU countries in the span of one week (20-26 March 2024)[55]. The websites typically spread pro-Russian narratives on the war in Ukraine. A further 45 articles were published across the Pravda network in multiple Member States, as well as other unverified sources, reporting on the European elections not leading to meaningful change. Additional

Pravda articles amplify official Kremlin sources claiming that the EU elections were held under severe restrictions.

52. In early June 2024, internal documents from the Fund for Support and Protection of the Rights of Compatriots Living Abroad (Pravfond) revealed an extensive Russian influence operation headed by former intelligence operatives and reported to be active in 48 countries across Europe and the world. The fund is said to have spent millions of euros financing propaganda websites targeting Europeans to replace sanctioned Russian state media, as well as supporting the legal defence of sanctioned Russian individuals.[56]

53. Some attempts to use FIMI tactics for triggering real life events included the pro-Kremlin channel Rybar, which disseminated fake maps of farmer's protests and claimed that 'about 27,000 farmers are now heading from Poland, Romania, Germany, the Netherlands, France and Spain towards Brussels to gather in front of the European Parliament on June 9'.[57]

2. Other risks, beyond FIMI

54. Foreign interference is known to include a diversity of tactics, techniques, and procedures, and extends beyond information interference operations. Hybrid threats, such as attacks on elections officials, on elections infrastructure or results, or cyberattacks[58], have been documented in the past and are inherent to the risk profile of elections.[59]

55. Other tactics are related to corruption, elite capture, espionage and cyberespionage. During the spring of 2024, incidents of MEP's spying on behalf of Russia and China were widely reported, highlighting the connection between FIMI and espionage.[60] According to an April 2024 resolution by the European Parliament, this includes 'credible allegations' that several MEPs had accepted payment to spread pro-Kremlin propaganda.[61]

56. Cyberespionage is also a constant interference threat. Available reports do not point to a ramping up of the cyberespionage activities beyond the established operations of persistent top threat actors known to the competent authorities.

IV. Artificial Intelligence

Key instruments in place

57. The use of generative AI and deep fakes is regulated by the AI Act, including as regards labelling by the content creator, and risk management obligations. The provisions should apply as of July 2026.

58. Very large online platforms and search engines are already subject to the rules of the Digital Services Act[62], with a clear obligation to mitigate risks to electoral processes and civic discourse, including when linked to the spread of manipulated content. The Commission provided detailed guidelines to platforms for mitigating system risks for electoral processes under their DSA obligations, including on the misuse of generative AI technology and on the role of recommender systems in shaping public opinion[63]. Platforms are expected to clearly label AI-generated content related to electoral processes, and they should limit the amplification of deceptive AI-generated content through their recommender systems. The Commission also sent requests for information on generative AI risks and on recommender systems which also touched upon their impact on electoral processes.[64]

59. Digital companies also committed on a voluntary basis to address the risks of misuse of their generative AI technology and the spread of deepfakes through social media platforms. The largest industry players are part of the Code of practice against disinformation, and made additional voluntary commitments under the 'Munich

tech accord'[65].

60. Following the Commission Recommendation (EU) 2023/2829 on inclusive and resilient electoral processes in the European Union (EU), European political parties signed a Code of Conduct for the 2024 European Parliament elections, including a commitment to 'abstain from producing, using, or disseminating misleading content' such as 'any type of deceptive content using audio, images or video and generated with or without artificial intelligence to falsely or deceptively alter or fake candidates, officials or any electoral stakeholder.' The Code does not ban the use of AI, but asks for clear labelling, and encourages the use of watermarking and provenance signals.

61. Regulation 2024/900 on the transparency and targeting of political advertising, once applicable, will also include disclosure obligations on the use of AI systems in the targeting of political advertising.

1. What happened? Key take-aways

62. **The use of AI in influence operations has increased in recent years. AI tools available today are used for cheaper, faster and higher-quality manipulative techniques. During the European elections, AI does not seem to have been used to a large extent.**

63. **However, examples show the span of tactics that can be used, and their severe risks of manipulation. Political parties have used AI to a small extent in their campaigns.**

64. In the weeks before the vote, the amount of fact-checked disinformation containing AI-generated content detected by EDMO remained constant, at around 4% of the overall amount of fact-checked disinformation (5% in the months before).[66]

65. According to Meta, influence operations from Russia, including Doppelganger, made use of Generative AI to provide 'only incremental productivity and content-generation gains'.[67] Similarly, Open AI reports that FIMI content developed with the support of their models 'do not appear to have meaningfully increased their audience engagement or reach as a result of their use of our services'.[68] Microsoft also assessed a low impact of AI to influence the elections.[69]

66. The use of AI is generally complementing manual content creation. The Doppelganger operation purchased multiple OpenAI program accounts through five separate email addresses to generate and edit content alongside manual methods[70]. Other uses observed by Open AI, Meta, and Microsoft include generation of text content, of news reader videos, fictitious journalist personas, images, comments and replies, website tags, and translations. A recently unravelled operation, named A2Z, seems to have used generative AI for creating comments on social media and for designing images in a series of campaigns that are thought to have a commercial purpose, according to Open AI[71]. Among other tactics, fake personas are reported to have supported right-wing parties in France. The Russian-affiliated operation known as CopyCop was reported to have disseminated YouTube videos including AI-generated faces and voices impersonating French and EU political leaders.[72]

67. AI was not only a tool for disinformation and foreign interference. AI was also part of the domestic political communication. Investigations by DFRLab, Alliance4 Europe and AI Forensics collected **131 instances of unlabelled generative-AI content** shared by political parties on platforms such as Instagram, X, Facebook, Vkontakte and Telegram. According to investigations, French and Italian political parties associated with the Identity and Democracy (ID) movement used unlabelled generative AI as part of their electoral campaigns. Primarily, the parties involved were France's Rassemblement National and Italy's Lega. Many of the AI-

generated images depicted EU flags and institutions.[73] In the case of Lega, the images were amplified as advertisements that reached an estimated 3 million Meta users.[74] Similar images continued to be used during the 2024 French elections.[75]

68. The investigations show that AI generated images were also used in posts criticising the French Member of the European Parliament and President of the Renew Group, Valérie Hayer and the President of France, Emmanuel Macron. Other reports show how AI was used for political messaging centred around entertainment, like an AI-generated song in support of Rassemblement National with an impersonation of Céline Dion,[76] or TikTok deepfake videos of members of the Le Pen family dancing and videos where the faces of two candidates were edited onto videos of female influencers that seemed to promote far-right parties.[77]

69. Most political parties surveyed either explicitly stated that they had not used AI in their campaign materials or implied that this was not the case. Only one political party[78], from the Netherlands, confirmed the use and labelling of AI content published on Meta's platforms.

70. Generative AI applications like chatbots could be misused to generate misleading content, or they could themselves, through flawed design and insufficient testing, 'hallucinate' and mislead users. Experiments by Democracy Reporting International[79] – an active civil society signatory of the Code of Practice on Disinformation – and by Correctiv[80] – an investigative and fact-checking organisation part of the EDMO network – indicated that three of the most used chatbots (Google Gemini, Microsoft Copilot, and ChatGPT) failed to provide accurate answers to questions about the elections. The chatbots either fabricated information, recommended non-existent Telegram channels, or provided incorrect details about candidates. AI Forensics[81] and Democracy Reporting International[82] – further investigated the safeguards implemented by digital companies on their chatbots during the elections, showing some progress, but also some inconsistencies across models and languages.

71. Digital companies reported[83] [84] [85] on the policy changes and measures taken to combat the misuse of generative AI during elections. This includes the adoption of standards on content provenance[86] and applying labels to manipulated content, in particular by allowing users to flag when their content is generated through generative AI. Some also reported offering to users tools for checking the integrity of content (e.g. Microsoft), labelling more prominently content that poses a significant risk of misleading the public on important topics (e.g. Meta, YouTube), or prohibiting certain types of AI generated content (e.g. TikTok's policies to ban content that shows fake authoritative sources, crisis events, or falsely showing public figures in certain context such as making an endorsement or being endorsed or bullied). Google and Microsoft also reported measures to ban practices that seeks to manipulate search rankings.

72. Companies that offer generative AI features, like Microsoft[87] and OpenAI[88], reported introducing specific corrections such as limitations to accepted prompts for reducing risks that their tools are used to generate misleading content. Google also reported[89] introducing new watermarking technologies for its Gemini app.

2. Evolving risks

73. The most prominent risk related to AI is a 'strengthened capability to produce content en masse', including in marginal languages[90]. With limited exceptions, highly-manipulative

'deepfakes' were not prominent during the European elections. Instead, AI was used to produce 'shallowfakes', combining out of context captions with the image of politicians or events, and 'cheapfakes', with rather obvious manipulation of video and image. Such content is easy to produce and will continue to be a challenge.

74. Researchers and civil society draw the attention to the use of manipulated content, not just for its capacity to mislead voters, but also for creating a 'liar's dividend', where authentic content can be disputed as false.[91]

75. The application areas of AI are not limited to manipulated content. AI can be misused for example for hypertargeting and profiling audiences, or drawing situational intelligence and, on this basis, producing highly targeted content. Industry reporting did not cover these risks.

76. In addition, AI, and, more broadly, technologies on which digital services are built, presents in itself vulnerabilities to misuse, or could inadvertently encourage disinformation. The guidelines[92] published by the Commission under the Digital Services Act, flag the potential role of platforms' recommender systems in amplifying disinformation and FIMI, and the need to carefully assess risks stemming from the design of those systems, including through adversarial testing. The Commission sent requests for information to YouTube and TikTok on the role of their recommender systems in amplifying risks to electoral processes and civic discourse.[93]

77. When platforms themselves offer features that can be used for the creation of deceptive, biased, false or misleading generative AI content, the guidelines also flag the need to mitigate risks and monitor their performance, and gives examples of other measures that should be put in place, to the extent technically feasible[94].

78. The NIS Cooperation Group's[95] compendium on elections cybersecurity and resilience provides an overview of hybrid threats, including how the use of artificial intelligence can interfere with elections. It provides a detailed list of potential security vulnerabilities for AI systems in the context of elections, including vulnerabilities to cyberattacks, 'poisoning' attacks, for example by tampering with AI training datasets, or inherent biases in the training datasets in AI-based data applications used for different electoral processes.

79. At the same time, the threat landscape related to AI use is fast-evolving. ENISA stressed[96] that 'some threat actors are experimenting with AI for information manipulation seemingly to assess how AI can be exploited in this context'.

V. Cybersecurity

Key instruments in place

80. The Commission's pre-election Recommendation encouraged Member States to take several measures to protect the election-related infrastructure and ensure resilience against cyber and other hybrid threats.

81. Several networks of national for cyber and hybrid action were active (e.g. the NIS Cooperation Group, the Joint Mechanism for Electoral Resilience, the Computer Security Incident Response Team Network, the EU Cyber Crisis Liaison Organisation Network - CyCLONe).

82. The NIS Cooperation Group, supported by ENISA, the European Commission and the European External Action Service (EEAS), published and updated a Compendium on Elections Cybersecurity and Resilience.

Additionally acyber-preparedness exercise[97] was organised with different election stakeholders in the Member States, bringing together national electoral bodies and national CSIRTs and the European institutions[98].

83. An inter-institutional Cyber Crisis Task Force, involving the EuropeanCommission services, EEAS, ENISA, Europol and CERT-EU was also set up.

84. The Commission monitored the situation on cyber incidents and disinformation and provided input to three Integrated Situational Awareness and Analysis under the Integrated Political Crisis Response arrangements activated during the electoral period. The Commission's situation centre was also active over the elections period and participated in exchanges with the EU CyCLONe network.

85. Europol supported the EU elections integrity through monitoring and coordination focused on cyberattacks and disinformation threats and produced an Early Warning Notification (EWN) on the potential involvement of organised crime and terrorist/violent extremist actors on disinformation linked to the elections, disseminated in the context of the IPCR.

86. The European Cooperation Network on Elections frequently discussed the cyber security risks in the context of elections. In addition, in November 2023, an EU tabletop exercise on cybersecurity of elections was organised with this Network to support common preparedness in case of incidents.

87. In the wider survey to political parties, 45 of the 59 respondents said they had in place measures to understand their exposure to risks of cyber incidents. Some of them undertook targeted risk assessments for the elections, and many said they had received briefings from authorities, such as cybersecurity agencies. Political parties also reported on the main partners they relied on for support, including national cybersecurity agencies and ENISA, as well as electoral authorities in some Member States, hired cybersecurity and IT firms, and briefing materials from online platforms such as TikTok and Meta.

1. What happened? Key take-aways

88. **During the electoral period, minor cybersecurity incidents were recorded, mostly in the form of Distributed Denial-of-Service (DDoS) attacks led by pro-Russian hacktivist groups. This suggests that the cyberattacks were intended as interference in the information domain, to gain visibility, rather than to effectively and persistently damage the infrastructure.**

89. The ODIHR Special Election Assessment Mission was informed by some national institutions that there had been some attempts at cyber-attacks, but they had been dealt with by relevant authorities. National authorities also informed the ODIHR Special Election Assessment Mission about their respective measures and trainings on cybersecurity and cyber-hygiene. [99]

90. ENISA collected open-source information on DDoS attacks recorded during elections and reported a very limited number of low-impact incidents, notably targeting websites of public organisations in the EU Member States – mostly linked to the transportation sector, followed by government websites and healthcare related institutions. Most of the observed targets were located in Ireland, followed by Poland and Italy.

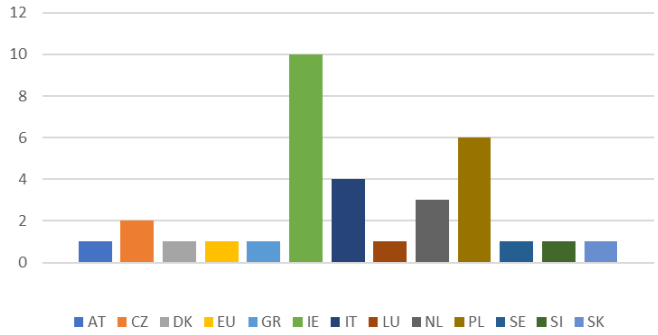

Figure 3 Number of websites repeatedly targeted by cyberattacks, per Member States. Source: ENISA

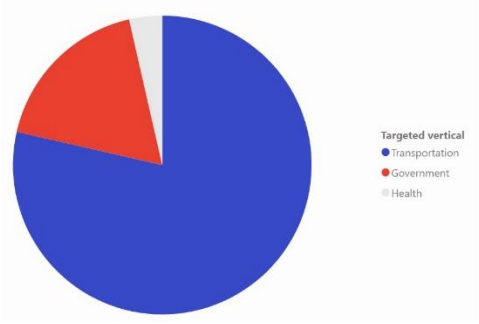

Figure 4 Distribution of DDoS targets between 7 and 9 June 2024, per sector. Source: ENISA

91. The DDoS attacks were conducted by a number of known pro-Russian hacktivist groups, in particular NoName057, CARR, HackNeT and CyberDragon. They did not seek to persistently damage the infrastructure, but, when successful, they led to outage of public websites for a short duration.

92. The pro-Russian hacktivist group hacker group NoName057 was reported to have been the most active, successfully targeting websites in 9 Member States, without producing a significant impact. On June 6th, hacker group NoName057 claimed on its Telegram channel that an alliance of at least 9 cyber attacker groups would launch a campaign targeting the internet infrastructure in Europe.[100] The time sequence of the attacks, closely linked to the ballot dates in several Member States, indicates that the intent was rather attention-grabbing.

NoName057 announced cooperation with other hacktivist groups NoName057 targets **NL** & EU entity	Multiple attacks from NoName057 and affiliated groups in **CZ**, FR, **IE**, **NL**	Multiple attacks from NoName057 and affiliated groups in **IT**, **CZ**, **SK**	Multiple attacks from NoName057 and affiliated groups in **FR**, **EL**, **LU**, **PL**, **SI**, IT, **DK**, AT
6 June	**7 June**	**8 June**	**9 June**
NL & CZ elections day	CZ, IE IT elections day	IT, LV, MT, SK elections day	Elections day in multiple Member States, including DK, EL, FR, LU, AT, PL, SI

Figure 5 Timeline of NoName057 DDoS cyberattacks against EU Member States targets between 7 and 9 June 2024. Source: ENISA based on publicly available sources

93. The findings reported by ENISA are consistent with the public reporting of the main technology companies. Google also reported[101] between 6 June 2024 and 9 June 2024, a higher number of DDoS attacks against users of its anti-DDoS attacks Project Shield[102], including media organisations and civil society users. Based on these reports, Poland received the most attacks, followed by Ireland, and Romania. The largest attacks took place on 9 June 2024.

94. In the framework of the European Cooperation Network on Elections, Bulgaria reported that two cyber-attacks by Russian hacker groups against state private cloud infrastructures were neutralised during election days. The Netherlands indicated that the websites of three political parties were also targeted with cyber-attacks. Ireland reported further attacks, including one on a voting registration website. Czechia reported three cyber-attacks during elections, not targeting election infrastructure.

95. Among the almost 60 political parties surveyed, five reported cyber-incidents targeted at their infrastructure or online presence. One European party reported a DDoS attack against the website of a political candidate during one hour on the night of 6th June, and a similarly heavy attack on the party's own website on the night of 9th June. Another European political party pointed to minor incidents, notably phishing activities targeting the party's staff and a DDoS attack briefly disrupting access to the website for an estimated timeframe of 8 hours. Two parties flagged that the DDoS and phishing activity was not higher during the electoral period than usually. Other DDoS attacks against political parties had been publicly reported[103].

96. In addition to DDoS and phishing, hacking attempts were also reported. One of the political parties surveyed reported that the social media accounts of some of their candidates were subject to unsuccessful hacking attempts. Hacking incidents that were part of information interference operations carried out most likely by foreign actors were also recorded.[104]

97. Additionally, while not related to the European elections, ENISA reported on multiple incidents involving satellite television signal hijacking in the EU, for instance hijacking the transmission of children's programmes to broadcast Russian propaganda.[105]

2. Evolving risks

98. ENISA released a comprehensive report on the cybersecurity threat landscape in 2024.[106] It points to the increasing connections between State-nexus actors and alleged hacktivist activities.

99. It also points to the hybrid nature of information interference operations, including with the use of Artificial Intelligence for operating sites with little human oversight.[107]

100. In addition, the NIS Cooperation Group published[108] a substantial compendium on elections cybersecurity and resilience which gives a comprehensive overview of cybersecurity threats for elections and shortlists a number of cybersecurity good practices for Member States to protect their elections. Notably, this compendiums shows the many risks for the elections, and the wide range of of tactics and techniques, which can be used by attackers who are trying to interfere with the EU's democratic processes and elections.

Endnotes

[1] With gratitude to the services, authorities, networks, civil society and industry contributing with their data and analysis and quoted in this memo, as well as to academics and in particular to James Pamment, for his appreciated advice.

[2] How the Council coordinates the EU response to crises - Consilium (europa.eu)

[3] None of these sources developed a comprehensive picture alone, rather it is the composite picture which is compelling. On occasions, definitions used in the different data sources are close, but are not identical, and data sets are not fully comparable

[4] Reports Archive Archive - Transparency Centre (disinfocode.eu)

[5] Dashboard - DSA Transparency Database (europa.eu)

[6] COM/2020/790 final – 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, EUR-Lex - 52020DC0790 - EN - EUR-Lex (europa.eu)

[7] Joint press release (europa.eu)

[8] https://commission.europa.eu/document/download/c797a16d-f2f6-4540-baf8-a05e8bcb33df_en

[9] European Board for Digital Services publishes post-election report on the EU elections | Shaping Europe's digital future (europa.eu)

[10] Dashboard - DSA Transparency Database (europa.eu)

[11] Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes | Shaping Europe's digital future (europa.eu)

12 In particular, Commitment 37 and Measure 37.2.

13 https://edmo.eu/thematic-areas/elections/european-elections/edmo-taskforce-on-2024-european-elections/

[14] EDMO final report, Final-Report-—EDMO-TF-EU24.pdf (cedmohub.eu) pp. 2 - 4.

[15] ec.europa.eu

[16] According to EDMO: 'In Portugal, for example, a doctored image was circulated purporting to show Ursula von der Leyen, EU Commission president, being arrested in the European Parliament. In Hungary, the photo of an information panel on a public toilet – explaining it was built thanks to EU funds – was circulated claiming that the toilet itself cost 268 million Hungarian forints to build (in fact, the cost of the whole project), suggesting that money was being stolen or that EU procedures are absurd.' ec.europa.eu/newsroom/edmo/newsletter-archives/53146

[17] EUROPEAN DIGITAL MEDIA OBSERVATORY - Disinfo Bulletin – Issue n. 45 (europa.eu)

[18] EDMO final report, Final-Report-—EDMO-TF-EU24.pdf (cedmohub.eu), p. 1

[19] Structural Indicators - Transparency Centre (disinfocode.eu)

[20] Internal analysis by the Text and Datamining Unit at the European Commission's Joint Research Centre

[21] 'Unverified sources', i.e. websites that were indicated by independent fact checkers and other experts as frequently spreading mis/disinformation. The corpus of websites observed includes sources from 36 countries covering 24 languages. For methodological details, see https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0291423

[22] See detailed reports from the Code of Practice on Disinformation ELECTIONS 2024 - Transparency Centre (disinfocode.eu) and other specific reports from online platforms in response to the Commission's DSA guidelines on elections, e.g. https://transparency.meta.com/sr/european-parliament-report-2024

[23] EDMO final report, Final-Report-—EDMO-TF-EU24.pdf (cedmohub.eu), pp. 24-25

[24] Misinformation is defined in the terms and conditions of the respective services. A general definition is offered by the European Democracy Action Plan, as 'false or misleading content shared without harmful intent though the effects can still be harmful, e.g. when people share false information with friends and family in good faith'

[25] Based on data reported by companies in their transparency reports under the Code of Practice on Disinformation Reports Archive Archive - Transparency Centre (disinfocode.eu)

[26] From 7 May to 23 June 2024

[27] For a benchmark of scale, Meta removed in the EU around 15.1 million pieces of content in total on Facebook, and 1.58 million on Instagram, over the same period as reported in the database of statement of reasons maintained by the Commission Dashboard - DSA Transparency Database (europa.eu)

[28] See Meta's 2024 European Parliament Post-Elections Report, https://transparency.meta.com/sr/european-parliament-report-2024

[29] During the 4 weeks preceding the vote

[30] TikTok removed in total 83 million pieces of content over the same period of time, all violations of their terms of service combined, and reported having removed 346,810 pieces of content that were linked to

negative effects on civic discourse or elections; see Dashboard - DSA Transparency Database (europa.eu)

[31] Platform response to disinformation on EU Election 2024 - Maldita.es - Periodismo para que no te la cuelen

[32] Study conducted by Trustlab to test the structural indicators of the Code of Practice on disinformation. Code of Practice 2 - Supplementary Report [Designed] - 2024 (disinfocode.eu) The study performed three tests during the electoral period of the European and the French elections.

[33] Discoverability refers to the percentage of content returned from searching disinformation keywords. It captures how easily a platform surfaces misinformation or disinformation content to a user searching for sensitive topics.

[34] *Ibidem,* Code of Practice 2 - Supplementary Report [Designed] - 2024 (disinfocode.eu)

[35] Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections | Shaping Europe's digital future (europa.eu)

[36]https://transparency.meta.com/sr/european-parliament-report-2024 ; EP Post election report

[37] Analyzing TikTok's 'Others Searched For' Feature (aiforensics.org)

[38] For example, European Parliament Elections, 6-9 June 2024: Statement of Preliminary Findings and Conclusions | OSCE
https://appf.europa.eu/cmsdata/287771/Special%20report%20on%20the%202024%20European%20elections.pdf

[39] Out of 59 parties responding to the survey

[40] COM/2020/790 final – 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, EUR-Lex - 52020DC0790 - EN - EUR-Lex (europa.eu)

[41] Report Stratcom activities 2021.pdf (europa.eu)

[42] How the Council coordinates the EU response to crises - Consilium (europa.eu)

[43] See, for example, media reports of the incident Hackers publish fake story about Ukrainians attempting to assassinate Slovak president (therecord.media)

[44] Ghostwriter has been a long-running campaign originating from Belarus and Russia. It has primarily targeted Ukraine and NATO countries through a combination of influence operations and cyber intrusions. Their activities have often involved stealing the credentials of legitimate actors such as journalists and producing content using their identities. They often sought to amplify content using additional compromised news platforms, with the aim of triggering reactions from prominent public figures and institutions. See, for example: https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf

[45]https://www.irozhlas.cz/zpravy-domov/ceske-noviny-ctk-web-server-hackeri-hackersky-utok-pellegrini-atentat_2404231223_ako; https://therecord.media/hackers-breach-news-website-false-article-slovakia-assassination; https://wyborcza.pl/7,75398,31021873,falszywa-depesza-o-mobilizacji-kto-na-niej-korzysta-by-podgrzac.html

[46] https://www.justice.gov/opa/media/1366261/dl

[47] Doppelganger is a major Kremlin-linked operation ran by SDA and affiliates that aims to undermine support for Ukraine and has been active since at least 2022. The operation unfolded over several channels. See, for example, Google reports on suspensions of Doppelganger links from Google News TAG Bulletin: Q1 2024 (blog.google), or OpenAI reports on suspension of misuse of ChatGPT Disrupting deceptive uses of AI by covert influence operations | OpenAI.

The operation made clones of legitimate websites to spread disinformation, including news sites, government websites, and a variety of other pro-Russian and anti-Ukrainian platforms. See https://www.disinfo.eu/doppelganger-operation/

Content was often amplified through fake personas on social media, as well as paid advertisements.[47] Doppelganger also created its own news media brands which purport to be independent.

[48] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

[49] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

[50] Fool Me Once: Russian Influence Operation Doppelganger Continues on X and Facebook - Alliance4Europe %

[51] https://www.qurium.org/alerts/russian-disinformation-against-zelenskyy-exposed-on-times-square-billboard/; https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf

[52] https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts/; https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf

[53] Operation Overload (checkfirst.network)

[54] Portal Kombat refers to around 200 news portals that relay and amplify content from Pro-Kremlin social media accounts, Russian news agencies, and official institutions. It provides part of the infrastructure to circumvent EU sanctions against Russian state media. The content mainly focuses on perceptions of the Russian invasion of Ukraine. This includes the production of localised Pravda news portals, automation of content publishing, significant localisation of content, and search engine optimisation. See https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

55 https://edmo.eu/publications/russian-disinformation-network-pravda-grew-bigger-in-the-eu-even-after-its-uncovering

[56] https://www.theguardian.com/world/article/2024/jun/02/revealed-russian-legal-defence-foundation-pravfond-europe

[57] Telegram: Contact @rybar_in_english

[58] BAY, S. Hybrid CoE Research Report 12: 'Countering hybrid threats to elections: From updating legislation to establishing collaboration networks', March 2024 Hybrid CoE Research Report 12: Countering hybrid threats to elections: From updating legislation to establishing collaboration networks - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

[59] The NIS Cooperation Group's *Compendium on Elections Cybersecurity and Resilience* also identified disinformation and Artificial Intelligence as threats, covered in more detail in other chapters of this analysis Safeguarding EU elections amidst cybersecurity challenges — ENISA (europa.eu)

[60] https://www.politico.eu/article/european-parliament-fines-mep-tatjana-zdanoka-accused-spying-russia/; https://denikn.cz/1388809/european-politicians-on-putins-payroll-russians-attempted-to-influence-european-elections-from-prague/?cst=f5e5df7bfaed79f079589fd852aae9630777e0c682b484a0836d56d390b2e654; https://www.politico.eu/article/belgium-germany-police-mep-maximilian-krah-china-espionage-alternative-for-germany-afd/

[61] https://www.europarl.europa.eu/pdfs/news/expert/2024/4/press_release/20240419IPR20542/20240419IPR20542_en.pdf

[62] See, in particular, the Commission guidelines on elections, where clear expectations are set for labelling generative AI. Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes | Shaping Europe's digital future (europa.eu)

63 EUR-Lex - 52024XC03014 - EN - EUR-Lex (europa.eu)

64 Commission sends requests for information on generative AI risks to 6 Very Large Online Platforms and 2 Very Large Online Search Engines under the Digital Services Act | Shaping Europe's digital future (europa.eu)

[65] Commitments - AI Elections Accord

[66] EDMO final report, Final-Report-–-EDMO-TF-EU24.pdf (cedmohub.eu),

[67] See p. 4 of EP Post-Elections Report_Meta_September 2024

[68] https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf

[69] https://www.reuters.com/technology/few-ai-deepfakes-identified-eu-elections-microsoft-president-says-2024-06-03/

[70] Affidavit, https://www.justice.gov/opa/media/1366261/dl p.52

[71] Influence and cyber operations: an update, October 2024 (openai.com)

[72] Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale | Recorded Future

[73] https://dfrlab.org/2024/06/11/far-right-parties-employed-generative-ai-ahead-of-european-parliament-elections/

[74] https://alliance4europe.substack.com/p/salvinis-electoral-campaign-uses

[75] https://aiforensics.org/uploads/Report_Artificial_Elections_81d14977e9.pdf

[76] https://dfrlab.org/2024/06/11/far-right-parties-employed-generative-ai-ahead-of-european-parliament-elections/

[77] https://www.euractiv.com/section/artificial-intelligence/news/viral-deepfake-videos-of-le-pen-family-reminder-that-content-moderation-is-still-not-up-to-par-ahead-of-eu-elections/; https://www.bfmtv.com/tech/actualites/reseaux-sociaux/deepfakes-de-la-famille-le-pen-les-comptes-tiktok-ont-finalement-ete-fermes_AV-202404150301.html

[78] in the questionnaire shared with European political parties as well as with national parties

[79] https://democracy-reporting.org/en/office/global/publications/chatbot-audit

[80] Chatbots: Don't Bother Asking AI About the EU Elections (correctiv.org)

[81] https://aiforensics.org/work/chatbots-moderation

[82] https://democracy-reporting.org/en/office/global/publications/follow-up-study-on-electoral-disinformation-by-chatbots

[83] DSA Election Readiness - Roundtable with Platforms, Search Engines, and Digital Service Coordinators | Shaping Europe's digital future (europa.eu)
[84] Reporting under the Code of Practice on Disinformation, Reports Archive Archive - Transparency Centre (disinfocode.eu)
[85] Progress update under the voluntary Munich Tech Accord, Progress Update - AI Elections Accord
[86] Notably the standard prepared by the Coalition for Content Provenance and Authenticity used by several signatories to label AI-generated content and supported by Adobe and other companies
[87] See Microsoft's report under the Code of practice on disinformation, available at Reports Archive Archive - Transparency Centre (disinfocode.eu)
[88] Disrupting deceptive uses of AI by covert influence operations | OpenAI
[89] See Google's report under the Code of practice on disinformation, available at Reports Archive Archive - Transparency Centre (disinfocode.eu)
[90] Fredheim, F., & Pamment, J., 'Assessing the risks and opportunities pose by AI-enhanced influence operations on social media' in *Place Branding and Public Diplomacy*, 2024
[91] See, Chesney, B., & Citron, D. (2019). *Deep fakes: A looming challenge for privacy, democracy, and national security*. California Law Review 107, 1753. https://doi.org/10.15779/z38rv0d15j and, Safeguarding Elections in the Digital Age: Assessing Evolving Electoral Risks and their Mitigation for Online Electoral Integrity - ISD (isdglobal.org)
[92] C/2024/3014, Communication from the Commission – Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065 (europa.eu)
[93] Commission sends requests for information to YouTube, Snapchat, and TikTok on recommender systems under the Digital Services Act | Shaping Europe's digital future (europa.eu)
[94] See point 39 of the Guidelines Communication from the Commission – Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065 (europa.eu)
[95] See NIS Cooperation Group, *Compendium on Elections Cybersecurity and Resilience*, 2024, pp. 11-12
[96] ENISA Threat Landscape 2024 — ENISA (europa.eu)
[97] EU cybersecurity exercise: foster cooperation, secure free and fair EU elections — ENISA (europa.eu) and table-top exercise within the European Cooperation Network on Elections in November 2023.
[98] EU cybersecurity exercise: foster cooperation, secure free and fair EU elections — ENISA (europa.eu) and table-top exercise within the European Cooperation Network on Elections in November 2023.
[99] INTERNATIONAL ELECTION OBSERVATION (osce.org)
[100] https://www.radware.com/blog/security/2024/06/uncovering-the-hacktivist-cyberattacks-targeting-the-eu-election/
[101] Report under the Code of practice against disinformation, p. 287
[102] Project Shield
[103] Germany's Christian Democratic party hit by 'serious' cyberattack | Reuters
[104] See *Supra,* p.8 on the hacking incidents against the Czech and the Polish news agencies, or operations leg by Doppelganger.
[105] See BabyTV hacked again: little ones watch Russian propaganda for fifteen minutes (nos.nl)
[106] ENISA Threat Landscape 2024 — ENISA (europa.eu)
[107] Citing Tracking AI-enabled Misinformation: Over 1050 'Unreliable AI-Generated News' Websites (and Counting), Plus the Top False Narratives Generated by Artificial Intelligence Tools - NewsGuard (newsguardtech.com)
[108] Safeguarding EU elections amidst cybersecurity challenges — ENISA (europa.eu)