European Digital Media Observatory

TASK FORCE ON THE 2024 EUROPEAN PARLIAMENT ELÉCTIONS

Systemic vulnerabilities, MIL, disinformation threats: Preliminary Risk Assessment ahead of the 2024 European elections

REPORT

EDITED BY **ENZO PANIZIO**

The European Digital Media Observatory's Task Force on the 2024 European Parliament Elections

In January 2023, the European Digital Media Observatory (EDMO) established a Task Force ahead of the 2024 European elections, in order to monitor and counter any attempts to condition and undermine public confidence in the democratic process. The aim is to provide useful information and tools in the effort to promote an honest European debate in the run-up to the elections.

The composition of the Task Force is designed to provide comprehensive geographic coverage of the European Union and to build upon the multidisciplinary approach of EDMO and its coverage of the whole Union through its national and regional Hubs.

It brings together experts from different professional backgrounds in academia, the media ecosystem, fact-checking and MIL. It consists of one chair, one secretary, one representative from each Hub and three members of the EDMO Advisory Council, plus one MIL expert.

Its current members are:

Giovanni Zagni | Pagella Politica/Facta.news – EDMO Executive Board, IDMO (Chair)
Louise Carnapete-Rinieri | European University Institute – EDMO (Secretary)
Alina Bârgăoanu | SNSPA Bucharest – EDMO Advisory Council
Stamos Archontis | FactReview – MedDMO
Kian Badrnejad | dpa – GADMO
Eileen Culloty | Dublin City University – EDMO Ireland Hub
Guy De Pauw | Textgain – BENEDMO
Victor Ebekwumonye | Sciences Po Paris – DE FACTO
Radovan Geist | EURACTIV Slovakia – EDMO AC
Emma Goodman | European University Institute – EDMO
Ivana Grkeš | University of Dubrovnik – ADMO
Pablo Hernández Escayola | Maldita.es – IBERIFIER
Péter Krekó | Political Capital – HDMO
Ruslana Margova | GATE Institute Sofia University – BROD
Giacomo Mazzone | Eurovisioni – EDMO AC
Bert Pieters | Mediawijs – BELUX
Gianni Riotta | Luiss Data Lab – IDMO
Mikko Salo | Faktabaari – NORDIS
Michal Šenk | Charles University – CEDMO
Andra Siibak | University of Tartu – BECID

More information about the Task Force and its activities are available on the EDMO's website.

Executive summary

As the 2024 European Parliament elections approach, this Risk Assessment report is aimed at analyzing the **interconnected landscape of systemic vulnerabilities and specific electoral risks**, which together with the pervasive challenge of disinformation pose significant threats to electoral integrity and public discourse across the European Union. This report highlights the critical nature of these challenges in shaping public opinion, voter behavior and, ultimately, the democratic discourse across Europe.

Based on existing research, documents and operative frameworks, as well as the evaluations of the EDMO Task Force on European Elections, the findings spotlight the risks related to the structural weaknesses within the media ecosystem, non-compliance with campaign regulations (especially online), specific risks related to the upcoming elections and the perils of dissemination of disinformation, through recurring narratives and new techniques. In addition, cyber threats to voting infrastructure pose a direct danger to the security and authenticity of election results, as well as a potential hook for disinformation campaigns aimed at suggesting election rigging.

Based on the assessments contained in the report, and drawing to similar analyses conducted by others, the following table summarizes an evaluation of the level of risk associated with each issue.

Specific Risk	Risk level
Common disinformation narratives about the EU elections	HIGH
Cyber threats and technological infrastructure	HIGH
Coordinated operations to amplify disinformation	HIGH
Disinformation techniques: AI-generated disinformation	MEDIUM-HIGH
Unfair conduct by political actors	MEDIUM-HIGH
Low MIL levels	MEDIUM
Declining trust in media	MEDIUM
Ineffectiveness of campaign rules, especially online	MEDIUM
Physical threats to candidates, activists, and other actors	MEDIUM
Lack of inclusion and accessibility	MEDIUM -LOW
Exogenous crises	LOW
Issues with counting/voting procedures	LOW

A critical concern is the role of **AI-generated content**, including deepfakes, which poses an unprecedented challenge by potentially misleading voters on a large scale and exacerbating the manipulation of electoral debates. Although the deployment of the new disinformation techniques using AI tools seems not pervasive so far, its effectiveness could be enhanced by realistic-looking false content, including videos of political figures or candidates. Moreover, the analysis identifies coordinated campaigns, both foreign and domestic, exploiting these vulnerabilities to amplify false narratives, undermining trust in democratic institutions and processes.

Moreover, since the EU elections are held on a national base, specific disinformation trends are unique to each EU member state, driven by national contexts but reflecting broader global concerns such as geopolitical tensions, economic uncertainties, and social issues. These narratives not only fuel polarization but also risk bolstering anti-EU sentiment and delegitimizing the electoral process through unfounded allegations of voter fraud and manipulation. This report only considers the risks related to the disinformation narratives that are most common to all EU countries. A comprehensive overview of the disinformation narratives affecting the various national elections held in EU and Council of Europe member countries in 2023 can be found in the *Report on Disinformation narratives during the 2023 elections in Europe*, the first output of the Task Force.

This report contains the pre-election assessments of the EDMO Task Force the 2024 European Parliament Elections.

Its main editor is Enzo Panizio, with contributions by Giovanni Zagni, Tommaso Canetta, Emma Goodman and the final review by the members of the Task Force. Graphic design by Renata Leopardi.

Index

Introduction

The main purpose of this document is to provide a brief overview of the main risks to the integrity and fairness of the European public debate in the run-up to the European elections, given the vulnerabilities of the media ecosystem and other structural factors, with a particular focus on the threats posed by disinformation.

The document aims to shed light on the intricate web of challenges that could skew public perception and debate, influencing voter behavior and potentially undermining the electoral outcome. The issues considered are various and they do not only concern the media landscape, but in each case their analysis is focused on communication incidents and how disinformation can exploit them.

This document is structured in an initial executive summary, with a summary table and a table with color-coded risks based on the likeliness of their occurrence, and three main parts. The first part focuses on systemic risks of the media ecosystem; the second one examines specific risks within the context of the European elections; and the third narrows down to threats directly related to disinformation. Each part is divided into smaller sections, one for each highlighted risk. The textual part will discuss the main issues related to the topic covered as well as list the work of the entities monitoring activities, recent research on the various issues and the authorities tasked with monitoring or mitigating the related risks.

PART I Systemic/Structural/ Environmental Risks

The impact of election-related problems and disinformation incidents that may occur in the run-up to the European Parliament elections can be enhanced by the vulnerabilities of the media ecosystem. Some characteristics of the media ecosystem could be exploited by malicious actors in order to maximize efforts to influence the public debate and thus the awareness of the choice that European citizens will make in June 2024. Those actors can be external, e.g. foreign actors pursuing their strategic interests (promoting foreign policy stances, undermining the European public discourse, and so on) or internal, e.g. groups interested in exploiting social polarization for economic or political gains.

This section will focus on a brief presentation of the main risks related to the general structure of the current information environment, such as media regulation, media and information literacy (MIL) levels, trust in media by the European citizens, and communication crises following the emergence of exogenous crises. Those are elements that weaken the resilience of the media landscape and make it vulnerable to interference and disinformation campaigns.

Section 1 Media regulation – HIGH-MEDIUM RISKS

The European Union is making significant efforts to develop a regulatory framework to ensure media freedom and pluralism while protecting the integrity of the media landscape. The proposed *European Media Freedom Act* (EMFA) aims to establish new rules to safeguard editorial independence, protect journalistic sources, and increase transparency in media ownership, among other measures. The *Digital Services Act* (DSA), on the other hand, was approved with the aim to create a safer digital space, where users' rights are protected and online platforms are held accountable, introducing stringent measures for transparency, especially in advertising, content moderation, and algorithmic processes.

At the same time, the 2018 revision of the *Audiovisual Media Services Directive* (AVMSD) – designed to harmonize national laws on all audiovisual media, aiming to protect minors, preserve cultural diversity, and ensure media pluralism – was updated to include online platforms and social media, reflecting the changing media consumption patterns. The *Digital Markets Act* (DMA) complements the broader regulatory framework designed to promote a safer and more competitive digital space. In particular, it addresses the

dominance of large online platforms, or "gatekeepers", to ensure that they do not impose unfair terms on businesses and consumers. Finally, to address the potential flood of AI-generated disinformation, the recently approved *Artificial Intelligence Act* (AI Act) appears relevant, since it requires, among other measures, AI-generated content to be watermarked to make it easily recognizable.

However, while the positive effects of these laws may take years to fully materialize, some of the original motives for their approval are urgent and could be relevant factors in the context of the EU elections.

For this section, we find relevant the analysis conducted by the European University Institute's (EUI) Centre for Media Pluralism and Media Freedom (CMPF). Therefore, the following text is based on the assessments of the Media Pluralism Monitor, the flagship project of the CMPF. – The *Media Pluralism Monitor 2023* (MPM) reports an overall **HIGH RISK** of excessive concentration of media ownership in the EU, damaging the pluralism and the independence of large parts of the European information industry. The lack of market plurality is significant in the sector and it is combined with an average **MEDIUM** – but increasing – **RISK** of scarce editorial autonomy from owners, advertisers and interest groups (with "deficiencies when it comes to the separation between newsrooms' commercial and editorial activities"), also leading to various concerns about the conflicts of interest affecting media coverage. The situation appears slightly better in the case of political independence but the overall risk is also rated by the MPM as MEDIUM. And so is the risk of political influence on the public service media, but in fourteen countries the risk of political control on both funding and governance of public broadcasters is reported to be **high**. The MPM also highlights journalistic standards that are not always excellent in various countries.

In general, the document reports, "While conditions vary from state to state, on average, the indicators on Editorial autonomy, the Political independence of the media, and the Independence of public service media demonstrate an increased risk rate, in the upper medium risk band. The three indicators are intertwined, as they illustrate the conditions and media systems in which political influences penetrate significantly into media ownership, the management of the PSM, and undermine editorial autonomy."

The concerning situation of the so-called "strategic lawsuits against public participation" (SLAPPs) is also worth mentioning. SLAPPs are spurious legal actions used by powerful entities to intimidate and silence journalists, NGOs, and independent observers by burdening them with the cost and hassle of legal defense. The risk that this strategy could be used during the European elections campaign is evaluated as **MEDIUM** by the MPM.

As reported by the European Parliament and research activities on the phenomenon, the number of SLAPPs appeared in constant growth in recent years, although it is not currently possible to determine the exact scale of the problem. The European Parliament has recently approved a law against SLAPPs, which partially fills the normative vacuum created by the lack of national regulation of the problem in all EU member States.

Stakeholders involved (outside media):

- National Governments and Parliaments;
- Media & Communication Public Authorities; Civil society

Monitoring Tools:

- European University Institute, *Media Pluralism Monitor 2023*;
- EU Commission, *2023 Rule of Law Report*;
- Coalition against Slapps in Europe, *SLAPPs: A Threat to Democracy Continues to Grow*.

Monitoring Entities:

- European Regulators Group for Audiovisual Media Services (ERGA)
- European University Institute (EUI)

Section 2 Media and Information Literacy (MIL) levels and challenges – MEDIUM RISK

Media literacy, meaning the skills to access, critically understand, and interact with media, directly influences democratic engagement. Media literacy skills are therefore particularly relevant around elections, when citizens need to make important decisions while being bombarded with information, especially online. This is even more critical in the upcoming elections, when the capabilities of generative AI are being put to the test. It is easier than ever before to create disinformation, and stopping it at source or via intermediaries is becoming ever more challenging.

The *Media Pluralism Monitor 2023* found that Europe-wide, the risk associated with the indicator media literacy is **MEDIUM**, with 50% for EU member states and 53% for all the countries studied. The monitoring tool offered by EUI points out huge differences between the various countries analyzed. The European Media Literacy Index 2023 from the Open Society Institute Sofia ranks 41 European countries in their potential for resilience to disinformation using several indicators, such as the quality of education, media freedom, trust in society, and the usage of new tools of participation. It found significant variations across Europe, and that countries in south Eastern Europe tended to be far more vulnerable to disinformation.

Therefore, in the context of the upcoming 2024 European elections, media literacy emerges as a pivotal skill, essential for navigating election-related information and combating disinformation, particularly with the rise of generative AI.

Key risks going into the 2024 elections:

Lack of knowledge around (likely low) media literacy levels. Based on the available evidence, it is not possible to assume that MIL levels around Europe are sufficient to withstand sophisticated disinformation campaigns, particularly given the challenges posed by generative AI.

Lack of evidence of the most effective strategies to increase media literacy. The lack of consistent evaluation means that it is hard to know the best approaches to increasing media literacy among the public, particularly when it comes to reaching and educating adults (and even more so when it comes to vulnerable groups). Many existing media literacy initiatives are targeted at children (partly because they are relatively easy to reach while in formal schooling) while clearly it is essential to reach adults when it comes to disinformation around elections (in Austria, Belgium, Germany and Malta the voting age is 16, in Greece it is 17, and in all other member states it is 18).

Election-specific issues. European politics is not the most straightforward topic, and the way people assess the accuracy of political news is particularly complex.

There are various rules around election campaigning which vary from country to country – such as those regarding the role of public service media, or political advertising on social media - and it is important that the public understand these and how they might impact the coverage they see. In such scenarios, deepfakes and other generated content could be particularly disruptive, highlighting the environment's lack of resilience against a flood of false information generated using AI tools.

A more detailed analysis of these issues is provided by Emma Goodman, MIL expert member of the Task Force, in Appendix B.

Stakeholders involved (outside media):

- Citizenship; Universities

Monitoring Tools:

- EUI, *Media Pluralism Monitor 2023*
- Open Society Institute Sofia (OSIS), *The Media Literacy Index 2023*

Monitoring Entities:

- ERGA
- EUI

Existing frameworks:

- UNESCO, *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2*

Section 3 Declining trust in media – MEDIUM RISK

Declining trust in mainstream media, coupled with the tendency to conspiratorial thinking observed in recent years, poses significant challenges, leading the public towards alternative, often less reliable information channels. This trend is particularly concerning during electoral periods, as it can have a significant impact on voters' perceptions and decision-making processes, leading to a more polarized and less informed electorate.

However, the available data does not show a critical situation. The risk that this combination of factors could disrupt the public debates leading up to the elections and directly influence the outcome of the vote appears to be **MEDIUM**. More subtle and plausible disinformation narratives, rather than purely imaginative conspiracy theories, appear more likely to have a direct impact on the election campaign.

According to Eurobarometer's *Media & News Survey 2023*, while trust in traditional media (such as TV, radio, and newspapers) and their use by the public slightly decrease, news consumption on social media grows fast. Although still behind and far from television (the most trusted medium overall), it is closing in on radio and the print press and is likely to overtake them soon.

"Compared to Parliament's Media and News survey 2022, there is an increase of 11 percentage points in the overall share of respondents who use social media platforms to access news", the press release of the survey reports, further adding how "37% of respondents follow influencers or content creators on social media platforms. This percentage varies widely among the different age-groups. 79% of young Europeans (aged between 15 and 24) follow influencers or content creators, while only 14% of those aged +55 do so".

Stakeholders involved (outside media): Citizenship

Monitoring Tools:

Eurobarometer, *Media & News Survey 2023*

EU Commission, *The state of democracy*

Monitoring Entities:

Eurobarometer

European Federation of Journalists

Section 4 Exogenous crises - LOW RISK

Catastrophic events not directly caused or controllable by human activities – such as the advent of natural disasters, war or pandemics – could pose significant threats to both the general population and political candidates' campaigns. The risk of their occurrence ahead of June 6-9 appears **LOW** at the moment this report is published, but these events still have the potential to shift public focus, potentially overshadowing election-related discussions.

As seen in the case of the Covid-19 pandemic, the Russian invasion of Ukraine, and the war between Israel and Hamas, disinformation follows the information environment's tendency to concentrate on crises, leading to massive campaigns of false stories. If a similar crisis occurs in the context of European elections, this focus might result in further polarization of public debate and obscure critical discussions about the elections. Disinformation strategies during these times can create confusion and misinformation, steering the public dialogue and attention away from substantive election issues and towards fabricated narratives, thereby influencing voter perception and behavior in a critical period.

Stakeholders involved (outside media):

- Governments; NGOs

Monitoring Tools:

- International crisis group, *Report & Brief*

PART II Specific risks related to the electoral process and campaign

In addition to the risks posed by a vulnerable media ecosystem, there are specific risks that may arise on the eve of an important election. These include issues related to compliance with the rules governing the electoral campaign, the inclusion of all citizens in the electoral process, cyber-attacks on strategic technological infrastructures, and physical attacks in the context of the electoral campaign.

Section 1 Inadequate campaign rules, especially online - MEDIUM RISK

The risks concerning the campaign rules in the run-up to the European Elections appear to be **MEDIUM**, in particular regarding the difficult balance between freedom of speech and electoral integrity, especially in the online sphere. Given the existence of significant regulatory differences between EU Member Countries, the scenario appears fragmented and critical in many cases. A recent report, titled "Political Online Campaigns in Central Europe: Wild and Waiting for the Regulation" and co-authored by several NGOs, highlighted the lack of consistent regulation and transparency in online political advertising within the Visegrád region, for example.

The fact that existing legal frameworks in several countries do not adequately address the complexities of digital campaigning, particularly concerning social media platforms, could lead to mis/disinformation incidents and unregulated campaigning practices. Among the most concerning issues are those related to compliance with laws on equal treatment and equal time allocated to the various political candidates in traditional media (e.g. the Italian law on so-called "*par condicio*", "equal conditions") and the respect of the election silence period, especially online. Moreover, if the fast labeling of false content spread on social media platforms seems crucial to not harm the voters' ability to make informed decisions during the European elections, the possibility that propaganda and false content circulate in the hours before election day is very likely, which would reduce the intervention

of institutions, fact-checking and mitigating measures by large online platforms. More troubling, if a falsehood spreads online shortly before voting, traditional media may be limited by electoral silence, potentially leading to the scenario where many more people are exposed to the false content than those reached by its debunking.

Stakeholders involved (outside media):

- Social media platforms; Politicians; Electoral Bodies; Regulatory Authorities (ERGA)

Monitoring Tools:

- Election-Watch.EU, *Pre-election assessment mission report*
- Election-Watch.EU, *Election Assessment Mission Final Report 2019*

Monitoring Entities:

- Association of Electoral Commissions
- Election-Watch.EU
- European Platform for Democratic Elections
- European Elections Monitoring Center
- Freedom House

Existing frameworks:

- International Institute for Democracy and Electoral Assistance, *Online Political Advertising Rules in Europe and Selected*
- International Institute for Democracy and Electoral Assistance, *Countries Globally*
- Stanford Internet Observatory, International Republican Institute, National Democratic Institute, *Combating Information Manipulation: A Playbook for Elections and Beyond*

Section 2 Lack of inclusion and accessibility - MEDIUM-LOW RISK

Another important aspect of such an important election is the inclusion of all citizens, whatever their specific needs may be. This encompasses enabling minorities and individuals with disabilities to engage in political life, vote, and run as candidates, safeguarding the right to a secret ballot and facilitating voting assistance. The related risk ahead of the upcoming elections appears **MEDIUM-LOW**: not gravely concerning, but still relevant. Although the adoption of the UN Convention on the Rights of Persons with Disabilities and its ratification by all the EU Member States has set a positive trend for inclusion, several challenges such as inaccessible voting environments, inadequate information, revocation of legal capacity, and discrimination based on disability continue to hinder the political participation of these persons. The European Economic and Social Committee (EESC) reported that approximately 400,000 persons with disabilities were unable to exercise their right to vote in the 2019 European Parliament elections.

This involves ensuring that all voters can obtain reliable and accessible information about candidates, policies, and voting procedures, which is fundamental for a functioning democracy. Efforts to address these challenges include implementing accessible digital platforms, providing materials in multiple formats – such as Braille, large print, and easy-to-understand language – and enhancing the training of election staff to assist all voters, including those with disabilities. Furthermore, ensuring that election-related websites and digital tools comply with international accessibility standards is essential for inclusive political engagement.

Stakeholders involved (outside media): National Electoral Commissions; NGOs and associations.

Monitoring Tools:

Election-Watch.EU, *Inclusive elections? The case of persons with disabilities in the European Union*

Inclusion Europe, *Inclusion indicators*

Monitoring Entities:

Election-Watch.EU

Inclusion Europe

Existing frameworks:

EU Parliament, *Political participation of people with disabilities in the EU*

Council of Europe, *Recommendations from the Council of Europe to European governments How to make sure people with disabilities can take part in political and public life*

EU Commission, *Union of Equality: Strategy for the Rights of Persons with Disabilities 2021-2030*

Section 3 Cyber threats and technological infrastructure - HIGH RISK

Technological infrastructure – encompassing traditional media, online media platforms and institutional systems – is susceptible to cyber-attacks, with a HIGH risk of their occurrence during the EU elections, as it happened in 2019. These attacks not only threaten the security of electoral data but also undermine public confidence in the State's ability to protect its democratic processes. The rise in foreign information manipulation and interference, as reported by the European External Action Service (EEAS), highlights the evolving landscape of cyber threats targeting electoral systems with malicious actors likely trying to push mistrust in elections and instigating people to abstention or invalidate voting. Particularly concerning are episodes of cyberespionage and so-called "hacktivism" from foreign actors.

In the context of the upcoming EU elections, ensuring the integrity and security of the electoral process is paramount. This includes safeguarding against the likely attempts to manipulate electoral data, unauthorized access to sensitive information, and the spread of disinformation, aside from likely cyber-attacks on electoral infrastructure. The perception of such infrastructure as weak could increase people's distrust in institutions and in the election administration itself, with critical consequences for participation, informed choice, and confidence in the proper conduct of elections.

Stakeholders involved (outside media):

- National Intelligence agencies; ICT firm; Online Platforms

Monitoring Tools:

- Computer Emergency Response Team for the EU institutions, bodies and agencies (EU CERT), *Monthly Briefs*
- EU CERT, *Threat Landscape Report - The 10 Years Edition*
- European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*
- EEAS, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*

Monitoring Entities:

- EEAS
- EU CERT
- European Union Agency for Cybersecurity (ENISA)

Existing frameworks:

- ENISA, *National Cybersecurity Assessment Framework (NCAF) Tool*
- MITRE corporation, *MITRE ATT&CK®*

Section 4 Physical threats to candidates, activists, and other actors - MEDIUM RISK

The assault on Capitol Hill in the United States and the attack on the Brazilian Congress are two of the most important recent examples of how disinformation and verbal violence can turn into attacks on the highest democratic institutions. The situation in the EU differs from those scenarios due to various socio-political factors and a generally stronger trust in electoral systems. However, while widespread violent reactions are less common in the context of European elections, a very serious episode of localized violence occurred with the attempted assassination of the Slovak prime minister Robert Fico. The scale of this case is smaller than what happened in the US and Brazil, as the Slovakian authorities defined the shooter as "lone wolf", but it is equally significant in terms of the role that disinformation can play in similar episodes.

Shortly after the shooting, several disinformation narratives emerged, alleging that the main opposition party, Ukraine or NATO were tied tho the violent act and prompting fears about the outbreak of violence in the bitterly polarized country. The Slovak interior minister, Matus Sutaj Estok, stated: "We are on the doorstep of a civil war. The assassination attempt on the prime minister is a confirmation of that".

The risk of a generalized outbreak of violence affecting the upcoming elections does not seem high, but after the attempted assassination of Fico, the general climate is certainly more susceptible and we rate the risk as MEDIUM.

More in general, the evolving digital landscape and the spread of mis/disinformation could contribute to a charged atmosphere, potentially leading to unexpected challenges, like attacks on politicians or candidates, especially women. Such incidents can significantly impact the electoral process by instilling fear, discouraging voter turnout, and undermining the overall perception of election integrity. Moreover, journalists, independent fact-checkers, and legal professionals, vital to the democratic process, could become targets for intimidation or violence, impacting the electoral discourse and information flow, as the increasing number of harassment cases testifies.

While the EU's strong democratic institutions and legal frameworks generally provide a buffer, the risks associated with political polarization and misinformation could escalate tensions, especially in the case of crucial elections. Historical and recent events have shown that even well-established democracies are not immune to the threats posed by disgruntled factions or radicalized individuals.

Stakeholders involved (outside media):

- Governments; law enforcement.

Monitoring Tools:

- International crisis group, *Report & Brief*
- Reporters without borders, *Reports*

Monitoring Entities:

- United Nations (UN)
- Reporters without borders

Existing frameworks:

- UN, *Preventing and Mitigating Election related Violence*

Section 5 Counting issues - LOW RISK

While the EU has generally maintained robust mechanisms to ensure the accuracy of election results, possible errors or tampering in vote counting pose a potential risk to the integrity of the European elections. At the moment the associated risk appears LOW. However, it is important to note that similar incidents, while in themselves having a debilitating effect on public opinion, could even lead to massive disinformation campaigns aimed at undermining the legitimacy of the election results, fostering distrust among the electorate and potentially inciting political unrest.

As we will see in Part III, dedicated to disinformation threats, disinformation narratives about the electoral process itself have been very common during recent national elections across Europe. These narratives often attempt to discredit the fairness of the competition and suggest the existence of conspiracies to invalidate the citizens' choices. In this sense, a relevant case occurred in Serbia, where during the recent parliamentary elections in December 2023, the electoral process was denounced as not entirely fair by international organizations. Amid accusations of excessive control over the national media environment, members of the ruling party, as well as pro-government media, raised concerns about alleged possible fraud and even violent actions by the opposition during the campaign. Instead, after the vote, when opposition parties and independent observers raised reasonable doubts about the legitimacy and fairness of the elections, the Prime Minister and members of the ruling party claimed that they were "the fairest elections ever".

The Serbian case is particular because of the high concentration of state-controlled media. If these incidents occur during elections in EU countries, on the contrary, it is reasonable to assume that they could boost the effectiveness of disinformers' efforts to spread distrust towards democratic institutions and elected representatives.

Monitoring Entities:

- National Electoral Commissions
- European Parliament

PART III Mis/disinformation-related risks

Disinformation is the number one global issue of concern, according to the Global Risks Report 2024 by the World Economic Forum. In the "short term" (i.e. 2 years) mis/disinformation is what respondents are most concerned about, placing it at the top of the list. And, in the long term, AI-generated misinformation is the second most worrisome risk, after extreme weather events. 2024 is widely described as the biggest election year in history, with billions of people casting their vote at a crucial historical moment, post-pandemic and amidst rising global tensions over ongoing wars.

In this context, the risk of false content spreaded to polarize public opinion and influence the outcome of the vote appears to be very high. Therefore, this section is dedicated to outlining the main disinformation threats to the fairness and integrity of the public debate, such as the evolution of false narratives, new disinformation techniques that can be exploited in the context of elections (mainly generative AI), and coordinated operations to influence public opinion. Countering this type of threat is the mission of EDMO, whose work is dedicated to monitoring the evolution of new vehiculated messages and informing public opinion about their presence, prominence, and evolution.

Section 1 Common disinformation narratives about the EU elections - HIGH RISK

Disinformation trends follow public discourse. When an issue is central to media coverage and political debate, disinformation will likely focus very soon on that same issue. Thus, as the European Parliament elections approach, it is reasonable to predict that a number of false stories will pop up during the European election campaign, posing a HIGH RISK of the related debate being polluted by false information. As EU elections are held on a national basis, false and misleading content is likely to focus most on local issues being debated in the various national campaigns. Each country has its own particularities, but common trends have been observed by EDMO over the past year. In particular, the spread of anti-EU disinformation and disinformation about the electoral process itself (in countries where elections were held in 2023) were common to all EU member states.

Our analysis of disinformation during national elections in EU and Council of Europe member states found that all campaigns (or post-electoral periods) were affected by

false stories alleging irregularities in the electoral process. Such false narratives typically focus on alleged voter fraud, illegal vote manipulation, faults in electronic or postal voting, abnormal voter registration practices, or foreign influence and interference. The clear goal is to portray the elections as invalid and, as a consequence, the elected representatives as illegitimate. A threat that is likely to be replicated in the context of EU elections, creating a climate of skepticism and confusion. In Germany, in particular, various false stories questioning the fairness of the EU electoral process have already been detected.

Moreover, thanks to almost a year of constant monitoring in its fact-checking briefs, EDMO has observed that, in fact, presenting EU institutions as anti-democratic and against citizens is a common and recurring disinformation narrative. In recent months, exploiting the relevance of farmers' protests, anti-EU narratives have again been widely circulated, with long-running false stories about EU institutions forcing citizens to eat insects and allowing the sale of lab-grown meat within its borders, while in the past EU institutions have been accused by false stories of being unreasonable and authoritarian in imposing countermeasures to climate change or wars, for example.

Other topics that indirectly involve the EU have been among the main targets of disinformation in recent months, such as EU countries' support for Ukraine (e.g. arms, money, reception of Ukrainian refugees), while national governments have been accused of introducing unfair laws because of EU policies. For example, measures against climate change (those part of the so-called European Green Deal, but also conspiracy theories), alleged support for indiscriminate immigration or Islamist organizations, and pandemic-related issues.

These narratives, as well as new ones, could escalate as the EU campaign enters its decisive phase.

Monitoring Tools:

- EDMO, *Fact-checking Briefs* and *Investigations*
- EDMO, Outputs of the EDMO Task Force on EU elections

Monitoring Entities:

- EDMO Task Force on EU elections
- EDMO National Hubs.

Existing frameworks:

- DISARM Foundation, *DISARM Framework*
- Digital Forensic Research Lab, *Dichotomies of Disinformation*

Section 2 Disinformation techniques: AI-generated disinformation – MEDIUM-HIGH RISK

Aside from the most common and well-known disinformation techniques – such as the recaptioning of old and out-of-context content, the exploitation of current events, and the impersonification of reliable news outlets, for example – new techniques are likely to be used by disinformers to affect the public debate ahead of the elections, in particular content generated through artificial intelligence (AI).

Technological progress in the field has been fast in the last few years, and their usage by disinformation has increased. Even if the traditional techniques are more likely to be massively exploited, AI-generated disinformation, although low in numbers, could represent a serious concern, especially because of the growing number of technologies capable of generating content that is very hard for users to identify as not real. AI technology is already affecting election campaigns and it could be used to boost Euroskepticism in the context of the European parliament elections.

The risk of the use of AI-generated content being used to disinform in the European campaign appears **MEDIUM-HIGH**. In a recent article, the EDMO Task Force on EU elections has outlined the main concerns on this topic in the run-up to the elections. Currently, AI tools can generate content in various formats, which can be used to spread disinformation: images, text, audio or deepfake videos (using generated audio as well), while totally generated videos are still quite unrealistic. Of these, deepfake videos (many false stories using them have recently been identified in several EU countries) and generated audio are the most worrying. Completely fabricated audio recordings are cheaper and particularly difficult to detect and debunk (even by experts), and can easily clone the voices of politicians and candidates.

A very significant case occurred in Slovakia, where an alleged phone conversation between a prominent political leader and a journalist discussing election rigging was circulated a few days before the presidential election of 2023 – but it was likely AI-generated. Given the difficulty of addressing this type of false content and the lack of time when it appears close to election day, it could be difficult to limit citizens' exposure to false content potentially influencing their choice.

***Monitoring Tools**:*

- EDMO, *Fact-checking Briefs* and *Investigations*
- EDMO, *Outputs of the EDMO Task Force on EU elections*
- EU CERT, *Monthly Briefs*

***Monitoring Entities**:*

- EDMO Task Force on EU elections
- EDMO National Hubs
- EU CERT
- EEAS

***Existing frameworks**:*

- Kalina Bontcheva, Symeon Papadopoulous, others, *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities*
- Knight First Amendment Institute, Columbia University, *How to Prepare for the Deluge of Generative AI on Social Media*
- EU CERT, *Security Guidance 23-002 - Potential impact and risks of Generative AI in EUIBAs*

Section 3 Coordinated operations to amplify disinformation – HIGH RISK

The spread of false information could be boosted by coordinated operations and networks to magnify the circulation of false content, especially on social media platforms. In the context of EU elections, coordinated operations, both from foreign or domestic actors, present a **HIGH RISK**. These operations aim to manipulate the flow of information, shaping public discourse on key (and often polarizing) electoral topics, often using bots, artificial intelligence and sophisticated algorithms to enhance their reach and believability. A recent investigation by *The Journal factcheck*, a fact-chacking organization of the EDMO network, highlighted how social media suspected of being part of a broader influence operation, spread misinformation and attacked poltiticians, journalists and news outlets, in an attempt to amplify divisive narratives and distort public opinion. At the same time, another recent research by CEDMO, the regional EDMO hub covering Central European countries, shows that 1/3 of voters in the four Visegrad Group countries (Poland, the Czech Republic, Slovakia, and Hungary) are aware of foreign interference attempts and perceive its threat. However, in Slovakia, people are more afraid of interference from the US or the EU, rather than Russia.

Tactics include the establishment of dedicated communication channels and social media accounts during the preparation phase, aimed at building legitimacy and setting the narrative agenda. These platforms serve as launchpads for the targeted dissemination of manipulated content, leveraging existing networks to maximize reach and impact. A notable strategy involves discrediting established media outlets, pushing audiences towards alternative and less credible sources. The overarching risk is the erosion of public trust in mainstream media and official channels, increasing reliance on unverified sources and potentially skewing public perception and electoral outcomes, weakening the infosphere and improving the effectiveness of disinformation campaigns.

Monitoring Tools:

- EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*
- EEAS, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*

Monitoring Entities:

- EEAS
- EU CERT

Existing frameworks:

- EU Commission, *Digital Services Act – Application of the risk management framework to Russian disinformation campaigns*
- EU DisinfoLab, Towards an impact-risk index of disinformation: measuring the virality of a single hoax

Section 4 Unfair conduct by political actors - MEDIUM-HIGH RISK

Finally, another risk potentially affecting the political debate around the European elections is linked to possible unfair conducts by national politicians themselves or other relevant political actors. This issue appears to be growing and highly dangerous in the context of important elections. The associated risk ahead of June seems **MEDIUM-HIGH**, encompassing several concerning behaviors.

Political incivility can facilitate the dissemination of disinformation by polarizing public opinion and undermining trust in credible information sources. When political discourse becomes hostile or disrespectful, it can create an environment where factual accuracy is overshadowed by emotional responses. This division can lead individuals to seek out information that aligns with their views, regardless of its truthfulness, further entrenching disinformation. Moreover, incivility can distract from substantive debate, making it easier for false narratives to spread unchallenged.

Moreover, when politicians spread false or inaccurate messages via mainstream channels they reach a vast audience. This extensive reach can overwhelm fact-checking efforts since the original false information might penetrate more deeply into the public consciousness than subsequent corrections. Thus, people exposed to the mis/disinformation may never encounter or recognize the related fact-checking articles, maintaining their exposure to falsehoods without access to corrective truths, which perpetuates the cycle of mis/disinformation.

Monitoring Entities:

- Body of European Regulators for Electronic Communication
- European Network Against Racism

Existing frameworks:

- EU Commission, *EU Code of Conduct on Countering Illegal Hate Speech Online*

Conclusion

As it approaches the 2024 European Parliament elections, Europe faces a complex landscape of challenges that threaten the integrity and fairness of the electoral process. From systemic vulnerabilities within the media ecosystem to sophisticated disinformation campaigns, these challenges demand concerted efforts from all involved stakeholders and a whole society approach to safeguard democratic integrity.

Since the European elections are still essentially 27 national elections, the scenario is aggravated by the differences between the various countries. For example, in the varying degrees of weakness of the national media landscape and the effectiveness of countermeasures against each national peculiarity.

The findings of this report illustrate significant concerns that span systemic issues, election-specific vulnerabilities, and disinformation threats. Systemic challenges such as media regulation deficiencies and gaps in media and information literacy (MIL) underscore deeper issues within the European information environment that could amplify election-related risks. While systemic fragility requires an overall, structured, long-term strategy, the exposed specific risks of the upcoming elections – including cyber threats, physical attacks, and inadequate campaign regulations, especially in the digital sphere – must be addressed with swift and targeted solutions.

Moreover, the rise of AI-generated disinformation and coordinated operations to manipulate public discourse creates a high-risk environment for mis/disinformation to flourish. By distorting the electoral debate, such techniques aim to undermine trust in democratic institutions and processes. The deployment of false narratives, particularly those – that will likely resurface – targeting the EU and the various national electoral processes, underscores the urgency of addressing disinformation head-on, with responsive fact-checking and collaborative efforts by traditional media and social media platforms. To counter these multifaceted threats, a comprehensive strategy is indeed necessary, and informing the citizens of the menaces they are exposed to appears crucial.

As the election draws near, ensuring the resilience of the entire European democratic process is paramount. This entails not only protecting against immediate threats but also fortifying the foundations of European democracy against future challenges. To safeguard the democratic integrity of the European Union in times of growing international tensions and conflicts is crucial that informed and fair electoral outcomes prevail.

Appendix A: An overview of the main existing frameworks for assessing/countering disinformation

This section provides an organized list of existing frameworks for detecting and countering disinformation incidents that may be useful in the context of the elections. The list includes frameworks on a variety of topics (from cybersecurity to legal issues), but all are somehow related to disinformation.

DISARM – A Framework for Analysis of Disinformation Campaigns

by DISARM Foundation, started in 2017

links: DISARM Framework, Disarm Framework Explorer , DISARM Foundation · GitHub , Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'

DISinformation Analysis & Risk Management is an open source framework for countering disinformation by sharing data and coordinating effective action. It is an analysis that schematizes, step by step, the behaviors of those who carry out disinformation campaigns and the countermeasures to be carried out to depower them. Therefore, DISARM is structured into two main components: the Red Team Framework, which lists the TTPs (Tactics, Techniques and Procedures) of disinformation creators by tactic stage, and the Blue Team Framework, which lists the TTPs of disinformation responders by tactic stage. For each stage, there are various procedures to be followed (sometimes complementary, sometimes alternative), which in turn list various procedures as appropriate.

Red team (**examples**, one for each stage): Determine Target Audiences, Discredit Credible Sources, Map Target Audience Information Environment, Respond to Breaking News Event or Active Crisis, Generate information pollution, Create inauthentic websites, Compromise legitimate accounts, Leverage Echo Chambers/Filter Bubbles, create fake Online polls, Conduct Pump Priming, Deliver Ads, Bots Amplify via Automated Forwarding and Reposting, Harass People Based on Identities, Conduct Crowdfunding Campaigns, Continue to Amplify, Assess Effectiveness, etc…

Blue team (**examples**, one for each stage): Repair broken social connections, Media literacy. Games to identify fake news, Educate high profile influencers on best practices, Reduce political targeting, Real-time updates to fact-checking database, Redirect searches away from disinformation or extremist content, Open dialogue about design of platforms to produce different outcomes, Use humorous counter-narratives, Prebunking, Seize and analyse botnet servers, Verification of project before posting fund requests. etc…

All these TTPs, strategies, and metatechniques are structured on the basis of many disinformation incidents and data sets. The definitions and procedures described in the framework provide a set of common concepts and language that are also the reference and basis for other documents, such as those of the EEAS and ENISA.

Foreign Information Manipulation and Interference concept developed

by the EEAS

Links: Beyond Disinformation - What is FIMI? | EEAS , Tackling disinformation: Information on the work of the EEAS Strategic Communication division and its task forces (SG.STRAT.2), an interesting overview FIMI: TOWARDS A EUROPEAN REDEFINITION OF FOREIGN INTERFERENCE

The FIMI definition offered by the EEAS is: *"FIMI is a mostly non-illegal 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. Not all disinformation is FIMI, and not all FIMI is disinformation"*. FIMI refers to information manipulation at the intersection of disinformation, influence operations, and cybersecurity. The growing popularity of the term is leading to a refocusing on behaviors and methods, the incorporation of cyber threat intelligence terminology, and a holistic, whole-of-society approach. It promotes collective understanding and response to such threats, with the goal of moving from a descriptive effort to an actionable operational framework to effectively counter disinformation.

2nd EEAS Report on FIMI threats

by the EEAS, January 2024

Link: 2nd EEAS Report on Foreign Information Manipulation and Interference Threats

The *2ndEEAS Report on FIMI Threats* explicitly addresses the delicate scenario of FIMI occurring before, during and after the upcoming European Parliament elections. The possible identified FIMI threats are: **Information Consumption**; **Citizens' Ability to Vote**; **Candidates and Political Parties**; **Trust in Democracy**; **and Election-Related Infrastructure**. Each possible menace is analyzed in its respective **objectives**, **methods** and **risks**. EEAS hypothesizes on a chronological basis which threat can be more plausible in a time frame that ranges from the early pre-electoral period until after the electoral count. Months before the election, information consumption and citizens' ability to vote could be the main focus of FIMI actors, while getting closer to the opening of the polls the targeting of political parties/candidates. Fostering distrust in democracy can gain more importance in the FIMI strategy, while the threat toward election-related infrastructure represents a constant risk, according to the report.

The first phase of **identification and preparation** is set months before the election and analyzes the possible scenario triggered by FIMI. The second step, **detection**, asks each stakeholder to carefully analyze - with the ABCDE framework - the FIMI elements; the third phase of **reactive responses** employs the correct countermeasure for each identified FIMI attack; the last moment is the **integration phase** in which the insights are shared across the stakeholders and new knowledge is advanced. A set of responses is presented in the final table of the Report, highlighting an optimized countermeasure for each type of risk. According to the general FIMI response framework, "responses

to FIMI need to take place at different levels and be adapted to the type of attack."

Indeed, drawing from the "Kill Chain perspective" the responses deconstruct the attack in each of its phases, providing different types of action along the development of a FIMI.

Therefore, the response framework is divided into 3 phases:

> **Cross-domain analysis**: the analysis must be carried out through different lenses, ranging from open source intelligence, and other IT data methodologies, as well as more humanistic analytical practices (public opinion…).
>
> **Adapted counter-measures**: it represents the arsenal of possible and suitable countermeasures, and it splits the phases of a FIMI in the pre-incident moment (when preventive measures are necessary) and the mid-incident moment (when the response can be to **ignore**, to **contain**, to **minimize** or to **react** to the threat).
>
> **Mechanisms for Collective Response**: in distributing opportunities to address FIMI, various stakeholders with distinct competencies play a role. Mechanisms for collective response delineate the necessary actions during incidents, guaranteeing timely and coordinated efforts by informing and preparing all relevant stakeholders. These systems employ structured procedures, guiding stakeholders in reporting, receiving, and responding to FIMI incidents.

The framework provides the analysis of 750 FIMI attacks recorded in one year. The main results are that "FIMI targeting is diverse and also affects nonpolitical individuals". For instance, some identified targets are the main governmental institutions, but also discriminated communities (e.g. LGBTIQ+), different political individuals, and popular celebrities. Moreover, the analysis affirms that FIMI attacks are often **event-driven**, since real cases offer a fertile ground for the proliferation of distorted narratives drawing from them, and FIMI strategy carefully employs a **cross-platform approach** to optimize its goal. Finally, the report points out that the advent of generative AI seems to be still in its embryonic stage, and is probably more beneficial for "defenders than attackers".

1st EEAS Report on FIMI threats

by the EEAS, February 2023

Link: 1st EEAS Report on Foreign Information Manipulation and Interference Threats

It is the first of its kind and can be seen as a pilot project. It applies a novel framework developed by the EEAS, based on best case practices of the FIMI defender community,

to a first sample of 100 FIMI incidents detected and analyzed between October and December 2022. The main findings of the report, based on the samples used, are:

- Russia's full-scale invasion of Ukraine dominates observed FIMI activity. Ukraine and its representatives have been the direct target of 33 incidents. In 60 out of 100 incidents, supporting the invasion was the main motivation behind the attack.

- Diplomatic channels are an integral part of FIMI incidents. Russia's diplomatic channels regularly serve as enablers of FIMI operations.
- Impersonation techniques become more sophisticated. Impersonations of international and trusted organizations and individuals are used by Russian actors particularly to target Ukraine. Print and TV media are most often impersonated, with magazines seeing their entire style copied. (On this topic there is also: *Doppelganger - Media clones serving Russian propaganda*, EU DisinfoLab)
- FIMI actor collusion exists but is limited. Official Russian actors were involved in 88 analyzed FIMI incidents. Chinese actors were involved in 17. In at least 5 cases, both actors engaged jointly.
- FIMI is multilingual. Incidents featured at least 30 languages, 16 of which are EU languages. Russia used a larger variety of languages than Chinese actors but 44% of Russian content targeted Russian-speaking populations, while 36% targeted English-speaking populations.
- FIMI is mostly intended to distract and distort. Russia (42%) and China (56%) mostly intend to direct attention to a different actor or narrative or to shift blame ("distract"). Russia attempts to change the framing and narrative ("distort") relatively more often (35%) than China (18%).
- FIMI remains mostly image and video-based. The cheap and easy production and distribution of image and video material online makes these formats still the most commonly used.

The report is rich with interesting definitions, graphs, and examples related to the various incidents analyzed.

2022 Report on EEAS Activities to Counter FIMI

by the EEAS, February 2023

link: 2022 Report on EEAS Activities to Counter FIMI | EU-HYBNET

The report focuses on the EEAS's efforts to counter FIMI in 2022 and outlines the EEAS's objectives, which are primarily aimed at identifying threats and increasing the resilience of countries exposed to them by developing appropriate policies, common strategies, and tools to respond to the threats. Examples cited are the disinformation strategies of Russia and China, and the weak resilience to this kind of menaces in Western Balkans and MENA, Middle East and North Africa.

In addition to developing a **FIMI toolbox**, the EEAS conducted more than 120 public presentations and workshops, reaching more than 13,000 people. In particular, the EEAS launched 'LEARN', a website available in English, Ukrainian and Russian explaining disinformation tactics and mechanisms. Furthermore, the EUvsDisinfo website, which raises awareness of pro-Kremlin disinformation, attracted 2.7 million visitors in 2022 and reached an estimated 20 million via social media.

Following Russia's invasion of Ukraine, the EEAS has intensified its engagement in the Western Balkans and the MENA region, promoting understanding of EU values, countering disinformation and supporting local studies. Together with EU delegations, the EEAS develops communication strategies and provides resources for long-term strategic communication engagement in these areas.

FIMI and Cybersecurity - Threat landscape

by the EEAS and ENISA, The European Union Agency for Cybersecurity, December 2022

Link: Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape — ENISA

It is an analytical framework, consistent with the ENISA Threat Landscape (ETL) methodology, with the aim of analyzing both FIMI and cybersecurity aspects of disinformation, and how to collectively respond to these phenomena. The report proposes and tests an analytical approach describing FIMI and manipulation of information, as well as the underlying cybersecurity elements, by combining practices from both domains:

• For **cybersecurity**: The open methodological framework2 used by ENISA's annual report on the state of the cybersecurity threat landscape, the ENISA Threat Landscape Reports3

• For **FIMI**: The open-source **DISARM** framework used to capture FIMI/disinformation

By testing the framework on a limited set of events, the report serves as a proof of concept for the interoperability of the frameworks. In addition, it puts forward some preliminary conclusions on the relationship between cybersecurity and FIMI/disinformation:

• **Role of cybersecurity in FIMI/disinformation**. Cybersecurity analysis seems to be particularly important in establishing attribution: among the events analyzed, those that had been attributed relied on a cybersecurity analysis. In addition, cyber-attacks seem to be more prominent at the initial stages of FIMI/disinformation events. This means firstly that specific cyber-attack techniques could act as an indicator of a FIMI/disinformation event and, secondly, that awareness raising is important to limit the development or acquisition of content and the compromise of infrastructure that facilitate dissemination.

• **Importance of structured and seamless incident reporting between the cybersecurity and FIMI/ disinformation community**. Consistency of data and data quality are the main limitation to cross-domain analyses. For example, open-source data about FIMI/disinformation events often cover entire operations encompassing several incidents, whereas a "pure" cybersecurity perspective would tend to focus on single incidents. Also, data about FIMI/disinformation events might not contain sufficient information about its cybersecurity aspects. In both cases, improved incident reporting practices could help.

• **Mutual exchanges between the cybersecurity and the FIMI/disinformation community could benefit the fight against FIMI/disinformation.** Since incident handling and response has been at the core of the cybersecurity community for many years, established cybersecurity practices can help the counter FIMI/disinformation community speeding up analytical maturity. For example, the FIMI community can adopt and adapt standard information formats widely used in the cybersecurity realm, to move beyond information sharing by written reports. Conversely, the FIMI/disinformation community can, in return, inform cybersecurity practitioners on new and emerging motivations, targets and threat vectors.

MITRE ATT&CK - Cybersecurity

by MITRE, started in 2013

Link: MITRE ATT&CK®

"MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. It aims to bring communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge."

The framework is similar to **DISARM**, but focused on cybersecurity. It is a situational map based on recorded behaviors. It shows step by step different strategies and possibilities by analyzing techniques and sub techniques. This is also used as a reference for several cybersecurity documents. Here you will find some helpful resources to get started with ATT&CK. In particular: Sp4rkcon Presentation: Putting MITRE ATT&CK™ into Action with What You Have, Where You Are and a methodology for using ATT&CK to build, test, and refine behavioral-based analytic detection capabilities.

ABCDE Framework

by Carnegie Endowment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework, 2020

Link: The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework

The ABCDE framework is a tool for analyzing influence operations and disinformation. It is structured into **five components**: Actors (who are the key players), Behavior (what are their actions), Content (what messages are being disseminated), Degree (how widespread is the influence), and Effect (what are the outcomes). It helps define terminology, structure analysis, and design countermeasures. Its use includes asking component-specific questions to dissect the influence operation, making it a versatile tool adaptable to different scenarios. The ABCDE framework shapes countermeasures into four key initiatives: democracy-building initiatives, norm-defining initiatives, resilience-building initiatives, and adversary influence efforts.

The Landscape of Hybrid Threats: A Conceptual Model

by European Commission and European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2021

link: The landscape of Hybrid Threats: A Conceptual Model (Public Version)

The conceptual model covers the key elements that form the landscape of Hybrid Threats: **(a)** the actors that apply hybrid mechanisms, **(b)** the phases of a hybrid campaign, **(c)** the tools applied, and **(d)** the domains targeted, in order to achieve the hostile actor's strategic objectives. In addition, it provides arguments about hybridity – what makes a series of activities part of a Hybrid Threat.

The report highlights the complexity of hybrid threats and suggests that addressing them requires a whole-of-government or whole-of-society approach, involving civilian, military, and political actors. It provides a conceptual model to improve understanding of hybrid threats, identify gaps in preparedness, and enable targeted response strategies. The model includes key elements such as the actors involved, the phases of a hybrid campaign, the tools used, and the domains targeted. The report emphasizes the importance of vulnerability assessments, early detection, and a strong evidence base for attributing hybrid threats to specific actors.

In addition, the report points to discrepancies in how hybrid threats are perceived and understood, particularly between Western countries and states such as Russia and China. Finally, the report argues for strategic changes in governance, intelligence sharing, and crisis management mechanisms to effectively counter hybrid threats. It suggests that EU-NATO cooperation in the area of hybrid threats should be continued and strengthened.

Disinformation and electoral campaigns - Legal approach

by Council of Europe, 2019

Link: DISINFORMATION AND ELECTORAL CAMPAIGNS

The document is divided into **two parts**. The first provides an overview of the situation regarding disinformation, both from a political point of view (with data on past electoral campaigns) and from a technical point of view (in particular the use of social networks and their algorithms). The second part is devoted to structuring proposals and recommendations of useful practices to be followed or implemented regarding terminology, the handling of personal data, transparency, with particular attention to the accountability of service providers and their algorithms.

Structured Threat Information eXpression (STIX) framework - cybersecurity

by OASIS Open, started in 2016

STIX (Structured Threat Information eXpression) is a standardized XML programming language for communicating cybersecurity threat information in a common language that can be easily understood by humans and security technologies. It is designed to improve the sharing of all threat-related information, thereby improving security through collaboration. STIX works by providing a common language for describing threat indicators, incidents, and data breaches. It can be used manually or programmed using an XML editor, Python and Java bindings, and Python APIs and utilities. Data is organized into STIX packages and then shared in a variety of ways, including file exchange, APIs, or publishing to a threat intelligence platform. The STIX language is designed to support a number of core use cases.

Combating Information Manipulation: A Playbook for Elections and Beyond

by DNI, IRI and The Stanford Internet Observatory, 2021

link: Combating Information Manipulation: A Playbook for Elections and Beyond

It is a playbook created by the International Republican Institute (IRI), the National Democratic Institute (NDI), and the Stanford Internet Observatory (SIO) to help societies effectively counter efforts to undermine free and fair elections and support democratic processes and rights more broadly.

The playbook outlines the basics of the problem and core elements of a response, and points to trusted resources for a deeper dive into a particular type of intervention or threat. Its approach consists of how to **(1)** identify ongoing information manipulation campaigns, **(2)** develop real-time and near-term responses, and **(3)** build long-term resilience against a range of information manipulation tactics designed to influence or disrupt democratic decision-making.

The playbook's three-part strategy can be helpful in developing rapid and real-time responses, as well as long-term and sustainable approaches to building resilience to maintain the integrity of elections and strengthen democratic processes. It includes interesting case studies on the Mexican and Taiwanese elections.

Dichotomies of Disinformation

By Digital Forensic Research Lab, Atlantic Council, February 2020

Link: GitHub - DFRLab/Dichotomies-of-Disinformation

A comprehensive framework for classifying political disinformation campaigns that addresses the limitations of previous models, such as their inability to distinguish between disinformation, state propaganda, and illicit financial pressure. According to the framework's creators, these models also often exclude non-Western nations and don't address domestic disinformation. The framework was designed to be replicable, extensible, and applicable to a wide range of disinformation campaigns.

The creation process includes case selection based on two criteria: (1) a case must meet their definition of a political disinformation campaign, determined through inter-coder agreement and investigator guidance; (2) a case must come from a reliable secondary source. The final framework includes 76 binary variables, 35 text descriptors, and 40 quantitative variables which classify disinformation campaigns across **six categories**:

Target - The characteristics of the campaign's target, such as its national or supranational characteristics and its political or social strata.

Platforms - The medium through which the disinformation is spread, such as the open web, social media, and messaging services.

Content - The language and subject matter of the disinformation.

Methods - The tactics and narrative techniques used to spread disinformation.

Attribution - The characteristics of the disinformant, such as its national or supranational characteristics, political or social strata, and confidence in the attribution.

Intent - The inferred purpose of the disinformation campaign.

The order of these categories reflects the process the DFRLab uses to identify and evaluate suspicious campaigns. Here is a map of the detected cases.

Towards an impact-risk index of disinformation: measuring the virality and engagement of single hoaxes

by EU DisinfoLab, June 2022

Link: TOWARDS AN IMPACT-RISK INDEX OF DISINFORMATION: MEASURING THE VIRALITY AND ENGAGEMENT OF SINGLE HOAXES

EU DisinfoLab's impact-risk index offers an approach to assess the potential impact of single hoaxes. The method goes through a list of **eight indicators** related to the virality and engagement of a single disinformative content. The indicators are: 1 Engagement on social networks, 2 Exposure on social networks, 3 Content circulation, 4 Diffusion across communities, 5 Media outreach, 6 Type of actor, 7 Appearance in various formats, 8 Call for action and danger of the narrative. The scores from these indicators are translated into a final scale measuring the low, medium, high, or alarming impact-risk.

How to Prepare for the Deluge of Generative AI on Social Media

By Knight First Amendment Institute at Columbia University, June 2023

Link: How to Prepare for the Deluge of Generative AI on Social Media | Knight First Amendment Institute

The essay offers an analysis of the potential challenges and opportunities that generative AI brings to the social media landscape. It contends that the current discourse is overly focused on the threats posed by malicious uses, and overlooks the potential harm that could result from non-malicious but nonetheless questionable practices. The essay first presents a **framework** to analyze malicious uses, distinguishing the benefits to both attackers and defenders.

It then examines a variety of nonmalicious practices that, while not intended to cause harm, may pose significant risks. The paper advocates a balanced approach to evaluating these practices, taking into account both their potential benefits and drawbacks. It also highlights how chatbots could enhance the social media experience, and encourages more in-depth research in this area. Finally, the essay offers actionable recommendations for social media platform providers, civil society, and other key stakeholders to effectively navigate the burgeoning world of generative AI in the social media space.

Appendix B: Media literacy and election disinformation

by Emma Goodman, Media Literacy researcher for EDMO

Disinformation is a highly complex problem and to tackle it requires a multi-faceted effort: only by adopting a combination of approaches at each point in the process of information creation, distribution and consumption do we have any hope of addressing it. Developing citizens' resilience through media literacy education is a proactive approach to tackling disinformation. We are not going to be able to stop all disinformation reaching citizens, and we are not going to change their minds with fact checks or debunking if citizens don't understand why they should trust these, how the wider media ecosystem works and why everything they read might not be true. Citizens need to understand how and why they are being targeted by disinformation in order to resist it, and how to find and identify trustworthy information.

Media literacy is a complex, intertwined set of skills and competences. According to the Media Literacy Expert Group chaired by the European Commission, media literacy includes all technical, cognitive, social, civic and creative capacities that allow citizens to access the media, to have a critical understanding of it and to interact with it.

Media literacy education can take many formats – for example, it could be teaching children in schools to create their own news stories or to understand how algorithms function, or demonstrating fact checking processes to adults, or 'pre-bunking' common misconceptions via online videos, a nationwide behaviour-change campaign, or providing digital nudges to encourage users to think about the provenance of what they are reading on social media platforms.

A 2016 mapping project carried out by the European Audiovisual Observatory identified five categories of skills addressed by the projects:

1. Creativity
2. Critical thinking
3. Intercultural dialogue
4. Media use
5. Participation and interaction

LSE's Rapid Evidence Assessment (REA) on Online Misinformation and Media Literacy for Ofcom found that research shows that three types of media literacy skills have consistently been found to be effective in critically engaging with misinformation:

- critical thinking, including asking questions about where information comes from
- evaluation strategies, including a reflective approach to one's status as an audience

member

- knowledge of the operation of news and media industries.

Research in the UK has also found links between low levels of news literacy and a lack of trust in journalism, while other scholars have suggested that by promoting critical thinking skills, media literacy training can help to combat political polarization.

Media literacy skills are therefore particularly relevant around elections, when citizens need to make important decisions while being bombarded with information online, and even more so around these coming elections, when the capabilities of generative AI are being put to the test. It is easier than ever before to create disinformation, and stopping it at source or via intermediaries is becoming ever more challenging.

Media literacy in EU-level policy

Responsibility for promotion of media literacy lies with Member States, while the European Commission's role is to foster collaboration and facilitate progress (EDMO's work is included here).

The Audiovisual Media Services Directive includes requirements for Member States to promote measures that develop media literacy skills, and obligations for video-sharing platforms to provide effective media literacy measures and tools. Member States must report to the Commission periodically outlining their measures to promote and develop media literacy skills. The 2020-22 reports show that reporting is not yet consistent across Member States, despite following the Commission's guidelines.

Under Commitment 17 of the 2022 **Code of Practice on Disinformation**, signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with an aim of including vulnerable groups.

The current status of media literacy in Europe

Our awareness of the status of media literacy in Europe at this crucial point is hindered by a lack of research on media literacy levels, and a lack of clarity about what works. There is no consensus on how to measure media literacy skills, or even how to define media literacy. The research that does exist, however, does not offer a particularly optimistic picture.

The Media Pluralism Monitor (MPM), a tool developed by the EUI's Centre for Media Pluralism and Media Freedom, found in its 2023 edition that Europe-wide, the risk associated with the indicator media literacy is 'medium', with 50% for EU member states and 53% for all the countries studied. Out of the countries covered by the monitor - EU27 plus Albania, Montenegro, Republic of North Macedonia, Serbia and Turkey – 9 were classified as low risk for media literacy (although 4 of these are very close to the medium risk threshold), 12 were medium risk, and 11 were classified as high risk.

The MPM highlighted various challenges that affect the provision of media literacy education across the continent. "In most countries, there is at least a rudimentary media literacy policy," the report states, "However, such policies are often either fragmented or poorly implemented." Only five countries were identified as having a comprehensive and up-to-date media literacy policy: Belgium, Finland, France, Sweden and The Netherlands.

The MPM found that media literacy was usually included in the mandatory school curriculum, but even when this was the case, conducting media literacy activities remained problematic in most of the countries studied. "One of the main issues consists of providing adequate training to the teachers," the report specified, with 28 countries that scored in the medium-risk band in relation to teachers' training and one country (Turkey) at high risk.

Outside formal education, media literacy activities tend to be targeted towards a young and urban public, the report found. Only three countries studied by the MPM scored a low risk in relation to the existence of media literacy activities targeting vulnerable groups: Sweden, Denmark and The Netherlands.

These findings were echoed by recent LSE research which looked at challenges to media literacy provision in several European countries (Belgium, Finland, France, Ireland, Netherlands, Sweden), as well as in the UK and elsewhere. The research identified common challenges for media literacy providers across countries including lack of coordination at a national level and within the sector, difficulties reaching adults outside formal education and vulnerable groups in particular, struggles to secure long term funding in the absence of long-term structural policy, tensions in how media literacy is defined, and a constant race to keep up with the evolving technological landscape.

This research and that of others has also highlighted the lack of consistent evaluation of projects in the sector as a significant problem, as it is harder to ascertain what works in terms of increasing skills.

The European Media Literacy Index 2023 from the Open Society Institute Sofia, which ranks 41 European countries in their potential for resilience to disinformation using several indicators - the quality of education, media freedom, trust in society, and the usage of new tools of participation – found significant variations across Europe, and that countries in south Eastern Europe tended to be far more vulnerable to disinformation.

An Ipsos Mori survey from March 2021 (conducted for Google) found that just 9% of those surveyed from 11 European countries have participated in training about how to use online tools to distinguish between true and false information, but 58% are interested in doing so. Two-thirds of those surveyed believed it would be appropriate for a tech company to provide training to users to improve their ability to critically understand online information.

Key risks going into the 2024 elections

Based on the above, we can identify several risks related the public's resilience to disinformation in the 2024 European elections.

- ***Lack of knowledge around (likely low) media literacy levels***

  We don't have a full picture of media literacy levels across the EU, but based on the available evidence, we cannot assume that they are sufficient to withstand sophisticated disinformation campaigns, particularly given the challenges posed by generative AI. We need more research into media literacy levels.

- ***Lack of evidence of the most effective strategies to increase media literacy***

The lack of consistent evaluation means that it is hard to know the best approaches to increasing media literacy among the public, particularly when it comes to reaching and educating adults (and even more so when it comes to vulnerable groups). Many existing media literacy initiatives are targeted at children (partly because they are relatively easy to reach while in formal schooling) while clearly it is essential to reach adults when it comes to disinformation around elections (in Austria, Belgium, Germany and Malta the voting age is 16, in Greece it is 17, and in all other member states it is 18).

- ***Election-specific issues***

European politics is not the most straightforward topic, and the way people assess the accuracy of political news is particularly complex.

There are various rules around election campaigning which vary from country to country – such as those regarding the role of public service media, or political advertising on social media - and it is important that the public understand these and how they might impact the coverage they see.

'Deepfakes' that put words into politicians' mouths can be of particular concern in election periods – we need the public to be alert to this.

Appendix C: The summary table of the Risk Assessment

The following table provides a shcematich summary of the issues addressed in the text of the report, including related monitoring tools, entities and existing frameworks.

	Description	Stakeholders involved (outside media)	Monitoring Tools/ Reports	Monitoring Entities	Existing Frameworks
Systemic / Structural / Environmental Risks					
Media regulation	Complex factors – such as conflicts of interest, concentration of ownership, SLAPPs and the lack of autonomy of broadcasters – that weaken the resilience of the media landscape and make it vulnerable to threats.	National governments / Parliaments; Media & Communication Public Authorities;	Media Pluralism Monitor 2023 - EUI 2023 Rule of Law Report - EU Commission SLAPPS: A THREAT TO DEMOCRACY CONTINUES TO GROW - Coalition against Slapps in Europe	ERGA; EUI	
MIL levels	Media literacy, encompassing the skills to access, critically understand, and interact with media, directly influences a population's democratic engagement.	Citizenship, Universities	Media Pluralism Monitor 2023 - EUI The Media Literacy Index 2023 - OSIS	EUI; ERGA	A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2 - UNESCO
Trust in media and institutions	Declining trust in mainstream media poses significant challenges, leading the public towards alternative, often less reliable information channels.	Citizenship	Media & News Survey 2023 - Eurobarometer The state of democracy - EU Commission	Eurobarometer, EFJ	
Exogenous crisis	Catastrophic events (e.g. pandemic, natural catastrophe, war) are an important threat to both citizens and candidates. They can divert public attention and be exploited by new disinformation narratives that could permeate the debate.	Governments, NGOs	Report & Brief - International Crisis Group		

Specific risks related to the electoral process and campaign					
Campaign rules	Political advertising / Media and Platforms compliance with laws on "par condicio" and electoral silence / Labeling	Social media platforms, Politicians, Electoral Bodies, Regulatory Authorities (ERGA)	PRE-ELECTION ASSESSMENT MISSION REPORT - Election-Watch.EU Election Assessment Mission Final Report 2019 - Election-Watch.EU	Association of Electoral Commission, Election-Watch.EU EPDE, EEMC, Freedom House Election-Watch.EU EPDE; EEMC, Freedom House	Online Political Advertising Rules in Europe and Selected Countries Globally - International Institute for Democracy and Electoral Assistance Combating Information Manipulation: A Playbook for Elections and Beyond - Stanford Internet Observatory, International Republican Institute, National Democratic Institute
Inclusion/ Accessibility	Risks related to the accessibility for people with disabilities of electoral information and absence of physical barriers for casting the ballot.	National Electoral Commissions; Minority and Disability NGO/ Association	The Global State of Democracy 2023: The New Checks and Balances - Global State of Democracy Initiative Inclusive elections? The case of persons with disabilities in the European Union - Election-Watch.EU Inclusion indicators - Inclusion Europe	Election-Watch.EU	Political participation of people with disabilities in the EU - EU Parliament Recommendations from the Council of Europe to European governments How to make sure people with disabilities can take part in political and public life - Council of Europe Union of Equality: Strategy for the Rights of Persons with Disabilities 2021-2030 - EU Commission

Cyber attacks	Technological infrastructure (media, Institutions…) can be highly sensitive to cyber attacks, which can increase the feeling of weakness that citizens perceive of their State.	National Intelligence agencies; ICT firm; Platforms	Monthly Briefs - EU CERT Threat Landscape Report - The 10 Years Edition - EU CERT 1st EEAS Report on Foreign Information Manipulation and Interference Threats - EEAS 2nd EEAS Report on Foreign Information Manipulation and Interference Threats - EEAS	EEAS; EU CERT; ENISA;	National Cybersecurity Assessment Framework (NCAF) Tool - ENISA MITRE ATT&CK® - MITRE corporation
Physical Threats	Violent reactions before, during and after elections can negatively impact the way citizens approach to the polls (eg. Capitol Hill, Ecuador). These risks can also be aimed at journalists (mainstream and independent, as well as fact-checkers), politicians (who are running for elections or not), jurists (lawyers, judges and magistrates) for intimidation.	Governments, law enforcement	Report & Brief - International Crisis Group Reports - Reportes without borders	United nations	Preventing and Mitigating Election related Violence - UN
Counting issues	Risks related to errors or tampering with counts, and how disinformation can exploit them. [Case study idea: Serbian elections.]	National Electoral Commissions; European Parliament			

Mis-/disinformation risks					
Disinformation narratives	Based on the findings of the EDMO Monthly Briefs, how can disinformation narratives affect the campaign and evolve in its context? Focus on content: anti-EU disinformation and disinformation related to the electoral process itself		EDMO Fact-checking Briefs and investigations	EDMO TF + Hubs	DISARM Framework - DISARM Foundation Dichotomies of Disinformation - Digital Forensic Research Lab
Disinformation techniques	The risks associated with the use of AI tools to produce false stories, deep fakes, and fabricated content about the election and campaigning parties. AI-generated disinformation (false stories using generated images, videos, deep fakes of politicians, etc.)	-	EDMO Fact-checking Briefs EU CERT		Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities - Kalina Bontcheva, Symeon Papadopoulous, others How to Prepare for the Deluge of Generative AI on Social Media - Knight First Amendment Institute, Columbia University Security Guidance 23-002 - Potential impact and risks of Generative AI in EUIBAs - EU CERT
Coordinated Operations (Foreign Influence / Domestic Actors)	Coordinated behaviors by foreign countries and malicious groups can amplify the impact of online mis-disinformation and its influence on public opinion.		1st EEAS Report on Foreign Information Manipulation and Interference Threats - EEAS 2nd EEAS Report on Foreign Information Manipulation and Interference Threats - EEAS	EDMO TF; EEAS	Digital Services Act – Application of the risk management framework to Russian disinformation campaigns - EU Commission TOWARDS AN IMPACT-RISK INDEX OF DISINFORMATION: MEASURING THE VIRALITY AND ENGAGEMENT OF SINGLE HOAXES - EU DisinfoLab
Unfair conduct by political actors	The risk that politicians or other political actors use hate speech or spread mis/disinformation through mainstream channels (debates, interviews, TV programs), with large dissemination of false stories and claims.			Body of European Regulators for Electronic Communications ENAR	EU Code of Conduct on Countering Illegal Hate Speech Online - EU Commission