



Weapon and poison? Framing disinformation in European Commission Speeches, 2016–2024

Eliana Fattorini, Alberto Acerbi, Massimiano Bucchi & Enzo Loner

To cite this article: Eliana Fattorini, Alberto Acerbi, Massimiano Bucchi & Enzo Loner (16 Sep 2026): Weapon and poison? Framing disinformation in European Commission Speeches, 2016–2024, *Information, Communication & Society*, DOI: [10.1080/1369118X.2026.2733507](https://doi.org/10.1080/1369118X.2026.2733507)

To link to this article: <https://doi.org/10.1080/1369118X.2026.2733507>



View supplementary material [↗](#)



Published online: 16 Sep 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)



Weapon and poison? Framing disinformation in European Commission Speeches, 2016–2024

Eliana Fattorini , Alberto Acerbi , Massimiano Bucchi  and Enzo Loner 

Department of Sociology and Social Research, University of Trento, Trento, Italy

ABSTRACT

Drawing on 238 speeches delivered by European Commission (EC) presidents, vice-presidents, and commissioners (2016–mid-2024), this paper examines how the EC narrates ‘disinformation’. Using topic modelling, text-community detection, and qualitative content analysis, we show a generally self-absolving and fatalistic framing. Disinformation is considered the root cause of unwanted behaviours and events, naturalized as a technological inevitability given citizen gullibility. Moreover, responsibility for the spread of disinformation is externalized to hostile States, ‘bad actors’, and digital platforms. Battlefield and contagion metaphors (‘fight/weapon’; ‘poison/infodemic’) underpin a discursive policy repertoire focused on platform governance, detection/takedown, and media-literacy ‘vaccines’, positioning citizens as vulnerable subjects. Temporal analysis traces shifts from Russia-centred attributions to a broadened cast (China, Lukashenko) and, by 2023–2024, AI-enabled amplification. We argue that this framing narrows problem definitions and answers, imposing top-down solutions instead of supporting democratic dialogue. A better balance would combine fair platform rules with transparency, media pluralism, and participatory channels that treat citizens as interlocutors, so policies are shaped by informed dialogue rather than by presumptions of actors being misinformed.

ARTICLE HISTORY

Received 17 October 2025

Accepted 7 September 2026

KEYWORDS

Disinformation; European commission; framing; disinformation narratives; communication

Introduction

According to the latest results of the World Economic Forum Global Risks Perception Survey 2024–2025, the issue of ‘misinformation and disinformation’ has been identified as the most serious risk that societies could face in the next two years and the fifth main potential threat in the next ten years (World Economic Forum, 2025). Data from the cross-national survey conducted by Pew Research Center (Poushter et al., 2025) shows that the spread of false information online is considered the most pressing threat by respondents (72%). International organizations, governments, scholars, media, and citizens have been increasingly concerned in recent years by the spread of so-called ‘fake news’ (Gelfert, 2018) – especially through social media (Altay & Acerbi, 2023) –, thus

CONTACT Eliana Fattorini  eliana.fattorini@unitn.it  Department of Sociology and Social Research (University of Trento), via Verdi 26, 38122 Trento  <https://www.linkedin.com/in/elianafattorini/>

 Supplemental data for this article can be accessed online at <https://doi.org/10.1080/1369118X.2026.2733507>.

© 2026 Informa UK Limited, trading as Taylor & Francis Group

creating ‘a seemingly endless supply of guides, frameworks, and approaches to ‘combatting’ the problem’ (Eadon & Wood, 2024, p. 7).

Conceptually, misinformation and disinformation are usually distinguished by intentionality (Lecheler & Egelhofer, 2022): misinformation refers to false or misleading information shared without necessarily intending to deceive, whereas disinformation implies deliberate attempts to mislead, manipulate, or secure strategic advantage. While this distinction is analytically important, it is often difficult to apply empirically, since intent is not always observable and the same content may circulate across actors and contexts with changing purposes. This paper therefore does not treat the two concepts as theoretically interchangeable. Rather, it focuses on ‘disinformation’ because this is the category adopted by the European Commission in the policy initiatives and speeches examined here, and because we analyse how this institutional category is framed, mobilized, and connected to responsibility, threat, and democratic governance.

The proliferation of false and misleading information online has become a dominant concern in contemporary public and political discourse, frequently framed as an existential threat to democracy, public health, and social cohesion. This widespread anxiety often posits that exposure to false or misleading content on digital platforms has a profound and direct influence on individuals’ beliefs, attitudes, and behaviours, leading to irrational decisions and societal fragmentation. However, a growing body of research challenges the extent of these presumed effects, suggesting that the prevalence of misinformation might be overstated, as well as the public’s susceptibility to it, so that its direct impact on behavioural or political outcomes is less pervasive than often assumed (Altay & Acerbi, 2023; Budak et al., 2024). Taking this into consideration, scholars have referred to the exaggerated attention to the amount and effects of online falsehoods as part of a broader ‘techlash’ (Hoffmann, 2023), or within the sociological concept of ‘moral panic’ (Carlson, 2018).

Beyond the empirical debate concerning its effects, the concept of ‘misinformation’ itself has long been a contested terrain, often instrumentalized for political ends (Radnitz, 2025). Critics argue that the heightened focus on online falsehoods can serve as a convenient scapegoat, deflecting attention from underlying structural issues, political grievances, or policy failures. In this framing, concerns about misinformation can be strategically employed by political actors to discredit opponents, delegitimize inconvenient narratives, or justify measures that may, in turn, impinge on freedom of expression or media pluralism. Such weaponization of the ‘misinformation crisis’ narrative highlights a complex interplay between genuine societal concerns and the strategic deployment of the concept in contemporary political struggles (Jungherr and Schroeder, 2021).

Recent scholarship (Kuo & Marwick, 2021) has further conceptualized disinformation as a discursive and political construct through which institutions delineate symbolic boundaries between legitimate and illegitimate knowledge claims. Studies in the European context show that labels such as ‘fake news’, ‘misinformation’, and ‘post-truth’ often function less as neutral descriptors than as boundary-making devices that construct disinformation as a public threat while legitimizing specific forms of intervention (Egelhofer et al., 2020; Farkas, 2023). From a securitization perspective, framing disinformation as a threat to democracy may authorize exceptional regulatory or governance measures (Monsees, 2020, 2023). Other contributions highlight how invocations of ‘post-truth’ can operate as anti-populist or depoliticizing devices within struggles over

authority and truth (Farkas & Schou, 2019; Galanopoulos & Stavrakakis, 2022). In the EU context specifically, Casero-Ripollés et al. (2023) identify a structural tension between geopolitical framings of disinformation as an external threat and regulatory framings that construct it as an internal platform-governance challenge.

In their work on misinformation – understood as ‘an umbrella term encompassing all forms of false or misleading information regardless of the intent behind it’ – Altay et al. (2023, p. 2) presented six misconceptions about misinformation widely used in both the media and scientific research: (1) misinformation is essentially a social media problem; (2) the Internet is pervaded by misinformation; (3) misinformation spreads faster than reliable information; (4) people are easily misguided by misinformation on the Internet; (5) there are a significant number of people who are misinformed; (6) misinformation has a significant impact on how people behave. These misconceptions are often communicated through the use of metaphors, and political authorities can strategically deploy metaphorical framing to define disinformation and mobilize support for interventions (Boeynaems et al., 2017). Disinformation is frequently conceptualized and communicated through metaphors, which play a critical role in shaping how the phenomenon is understood and addressed across academic, policy, and media contexts (Deignan, 2016). In their study, Eadon and Wood (2024) identify two dominant metaphorical framings – i.e., embodied health and environmental health – that structure the discourse surrounding misinformation and disinformation. These metaphors help translate the abstract complexity of mis- and disinformation phenomena into more tangible and emotionally resonant domains, such as disease (‘infodemic’¹, ‘virality’) and ecological crisis (‘information pollution’, ‘digital wildfire’). According to the authors, while metaphor offers cognitive clarity and rhetorical force, its uncritical use can oversimplify, obscure nuance, and embed normative assumptions about danger, urgency, and appropriate responses. In doing so, metaphors not only diagnose disinformation as a major societal threat but also legitimize specific interventions while foreclosing deeper interrogation of the phenomenon’s roots and variability. As such, metaphor is not merely descriptive but constitutive, shaping both the perception of disinformation and the range of viable responses to it (Lakoff & Johnson, 1980).

Over the years, the European Commission (EC) has addressed the issue of disinformation by developing several initiatives and tools. Among the most relevant legislative ones are the 2018 Code of Practice on Disinformation² – i.e., an agreement signed, voluntarily, by the main digital platforms for adopting self-regulatory measures to fight disinformation – and its above-mentioned strengthening in 2022³ – which is part of the broader European Democracy Action Plan, adopted in 2020.⁴

Analysing EC speeches is important because they are not merely ceremonial or descriptive texts. They are public-facing acts of institutional meaning-making through which the Commission defines policy problems, assigns responsibility, legitimizes intervention, and signals priorities to member states, platforms, journalists, civil society, and citizens. This is especially relevant in the field of disinformation, where the EC has acquired an increasingly central role in shaping European information governance through instruments such as the Code of Practice on Disinformation (2018; revised 2022), the European Democracy Action Plan (2020), the establishment of the European Digital Media Observatory (2020), and the Digital Services Act (2022).

Although the Commission is not a media regulator in the traditional national sense, its initiatives influence the conditions under which platforms moderate content, journalists and fact-checkers are enrolled in counter-disinformation infrastructures, and democratic communication is institutionally framed. For this reason, examining how the EC publicly defines and narrates disinformation is relevant not only for understanding EU policy communication, but also for assessing the legitimacy, assumptions, and democratic implications of emerging information-governance regimes.

This paper argues that, across presidential and commissioners' speeches from 2016 to 2024, the EC has developed a narrative on disinformation that is at once self-absolving and fatalistic. It is self-absolving in two ways. First, the effect of disinformation on citizens is considered the cause of events and behaviours considered as negative, such as vaccine hesitancy or the result of the Brexit referendum. Second, responsibility is consistently shifted outward – towards foreign adversaries and 'big digital platforms' – while citizens are predominantly depicted as passive victims in need of protection or education. At the same time, it is fatalistic, since disinformation is frequently presented as an unavoidable by-product of digital infrastructures – 'everywhere online', travelling faster than truth – which reinforces a platform-deterministic view and legitimizes exceptional, security-oriented measures to 'fight' an ongoing threat to democracy. This dual framing is sustained through three recurring elements: (i) misconceptions, most notably the idea that social media themselves create and spread disinformation; (ii) metaphorical framings such as battlefields, contagion, or environmental hazards; and (iii) a democracy discourse that stresses electoral integrity and civic vulnerability, while leaving largely unexamined the role of institutional accountability within the EU itself.

Following the European Democracy Action Plan, we use the EC's operational definition of disinformation as 'false or misleading content that is spread to deceive or secure economic or political gain and which may cause public harm', excluding 'misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary'.⁵ This operational choice does not imply that misinformation and disinformation are conceptually identical. Rather, it reflects the empirical focus of the paper: the EC's own public discourse is organized around 'disinformation' as the privileged policy category through which online manipulation, foreign interference, platform accountability, and democratic vulnerability are addressed. At the same time, public and scholarly usage often treats 'disinformation', 'misinformation', 'fake news', and 'conspiracy theories' interchangeably (Eadon & Wood, 2024; Khan et al., 2022). In practice, authorities commonly adopt 'disinformation' as a catch-all for the online manipulative practices they prioritize, a usage reflected in the EC's 2022 Strengthened Code, which also subsumes 'misinformation, disinformation, information influence operations and foreign interference in the information space' (European Commission, 2022, p. 1; see also Pielemeier, 2020). The boundary between mis- and disinformation further blurs when generative AI is involved in news production (Schäfer, 2023; Vogler et al., 2023). For analytic clarity and corpus construction, we therefore adopt 'disinformation' as our single keyword, while examining how the EC's discourse draws on broader misconceptions and metaphors that also circulate in the literature on misinformation, fake news, and information disorder. Moreover, we use the term 'discourse' to refer to the broader, recurring structure of meaning through which the EC frames disinformation across the corpus, rather than to individual speeches. Individual speeches are therefore treated as

situated textual instances that reproduce, negotiate, or occasionally complicate this broader institutional discourse. Accordingly, when referring to single texts, we use the term ‘speech’.

Empirically, we combine topic modelling, text-community detection, and qualitative content analysis on 238 EC speeches (2016–mid-2024). The first research question is exploratory and identifies the dominant narratives articulated across the corpus. The second focuses on two sensitizing framings suggested by the literature and by the EU policy context – platform determinism and securitization – and examines how they are sustained through metaphors and actor attributions. The third question then considers how these narratives and framings construct the relationship between disinformation and democracy. We ask: (1) What dominant narratives about disinformation are articulated across EC leadership speeches, and how do they contribute to a broader institutional discourse on disinformation? (2) To what extent, and through which metaphors and actor attributions, do these narratives sustain platform-deterministic and security framings? (3) How is the relationship between disinformation and democracy constructed, and what implications follow from this framing?

Data & methods

This work analysed a corpus of 238 speeches retrieved from the European Commission’s official speech archive (Press Corner) that include the keyword ‘disinformation’, delivered by European Commission officials occupying 60 role entries between 1 January 2016 and 30 June 2024: 2 Presidents, 5 Executive Vice-Presidents, 10 Vice-Presidents, and 43 Commissioners (see [Table 1](#) in the Supplementary Material). The EC’s official speeches were manually downloaded from the EU website⁶ and compiled into a document corpus managed through the R software (R Core Team, 2024). Because the corpus was built from the Press Corner archive, relevant speeches published in other official EU repositories (e.g., European External Action Service – EEAS) are not captured by this data collection procedure.

We selected an eight-and-a-half-year timeframe to provide a longitudinal overview of the main events that brought the issue of disinformation into the public debate and to the attention of international institutions during the Juncker (from 1 November 2014 to 30 November 2019) and von der Leyen presidencies (from 1 December 2019 to 30 November 2024). We focused on this timeframe because, in the selected period, five main events have led to the rise of the disinformation issue as a matter of public and political concern: (1) the United Kingdom’s process of exiting the European Union (also known as ‘Brexit’) which occurred between 2016 and 2020; (2) the United States presidential campaign in 2016; (3) the onset of the Covid-19 pandemic in 2020; (4) the outbreak of war between Russia and Ukraine in 2022; (5) the launch of Open AI’s chatbot ChatGPT in late 2022. The analysis of the speeches employed a mixed-method approach, connecting the quantitative analysis of the EC speeches to the qualitative inquiry.

A substantial share of the speeches – and therefore of the quoted material – comes from Věra Jourová, who served as Vice-President for Values and Transparency during much of the period analysed, with responsibilities closely related to disinformation, media freedom, and democratic integrity.

Table 1. Coding frame used in qualitative content analysis.

Main code	Sub-code	Source of category	Operational definition	Examples/indicators
Disinformation misconceptions	Pervades the Internet	Deductive: Altay et al. (2023)	Disinformation is described as widespread, omnipresent, or pervasive online.	'everywhere online'; 'pervades the internet'
	People are easily misguided	Deductive: Altay et al. (2023)	Citizens or users are represented as vulnerable to manipulation or easily misled by false information.	'manipulate'; 'mislead'; 'confuse their choices'
	Many people are misinformed	Deductive: Altay et al. (2023)	Disinformation is described as affecting large numbers of people or publics.	'many people'; 'large-scale'; 'massive'
	Impact on people's behaviours	Deductive: Altay et al. (2023)	Disinformation is presented as shaping concrete actions, such as voting, refusing vaccination, or ignoring health advice.	'led people to'; 'influence'; 'manipulate elections'
	Faster than reliable information	Deductive: Altay et al. (2023)	False information is described as spreading more quickly than truthful or reliable information.	'flies quicker than the truth'; 'spreads fast'
	A social media problem	Deductive: Altay et al. (2023)	Disinformation is primarily attributed to social media platforms, digital platforms, or online infrastructures.	'social networks'; 'online platforms'; 'algorithms'
Disinformation metaphors	Battlefield-related: combat/attack	Inductive	Disinformation or responses to it are framed through offensive, adversarial, conflictual, or weaponized language.	'fight'; 'combat'; 'attack'; 'weapon'; 'war'; 'warfare'; 'threat'; contextually 'tackle' ¹³
	Battlefield-related: defence	Inductive	Responses to disinformation are framed through protection, defence, security, shielding, or resilience against an external threat.	'defend'; 'protect'; 'shield'; 'security'; 'resilience'
	Environmental health	Deductive: Eadon and Wood (2024)	Disinformation is framed as pollution, contamination, wildfire, or an environmental hazard.	'pollution'; 'wildfire'; 'toxic'; 'contaminated'
	Embodied health	Deductive: Eadon and Wood (2024)	Disinformation is framed through disease, contagion, immunity, vaccines, antibodies, or bodily health.	'infodemic'; 'virus'; 'vaccine'; 'antibodies'; 'poison'
Disinformation actors	Private interests/companies	Inductive	Responsibility is attributed to private companies, economic actors, or platform business models.	platforms; companies; private interests
	Undefined others/other	Inductive	Responsibility is attributed to generic, unspecified, or diffuse actors.	'bad actors'; 'those who spread disinformation'
	EU actors/countries	Inductive	Responsibility is attributed to actors located within the EU or to EU countries.	EU-internal actors; member states
	Political actors	Inductive	Responsibility is attributed to parties, politicians, campaigns, or politically motivated actors.	political campaigns; populists; extremists
	Bots/AI/fake accounts	Inductive	Responsibility is attributed to automated accounts, fake profiles, AI systems, or deepfakes.	'bots'; 'fake accounts'; 'AI'; 'deepfakes'

(Continued)

Table 1. Continued.

Main code	Sub-code	Source of category	Operational definition	Examples/indicators
	Foreign actors	Inductive	Responsibility is attributed to foreign adversaries, foreign governments, or external interference actors.	'foreign actors'; 'foreign interference'; 'Kremlin'
	Countries	Inductive	Responsibility is attributed to countries as geopolitical actors.	Russia; China; Belarus

Text-community detection

Text-community detection (Bedi & Sharma, 2016; Fortunato, 2010) was performed on a word co-occurrence network constructed from the speeches and analysed using the igraph package (Csárdi et al., 2024), with communities identified through the Leiden algorithm (Traag et al., 2019). Community detection was chosen to fulfil a distinct analytical role, rather than to directly support interpretative semantic mapping. While semantic network analysis is commonly used to map and interpret relationships between concepts or actors – often with the aim of identifying discursive frames – our objective at this stage was not to derive frames directly from network structures. Instead, we employ community detection on a word co-occurrence network as an exploratory, data-driven technique to identify clusters of frequently co-occurring terms, i.e., recurrent lexical fields within the corpus. These clusters provide a structural overview of how disinformation is discussed, without imposing a priori interpretative semantic categories. In this sense, community detection complements topic modelling by offering a network-based representation of lexical proximity and serves primarily to guide the subsequent qualitative content analysis, in which framing processes are interpreted in context. This approach enables an analytical distinction between the identification of lexical structures and the interpretation of discursive frames, the latter being carried out inductively in the qualitative phase. The procedure yields clusters of frequently co-occurring terms ('word communities') that summarize recurrent lexical fields; we report these communities (with their salient terms) as a descriptive complement to topic modelling and to guide the selection of excerpts for qualitative analysis.

Topic modelling

Topic modelling (Murakami et al., 2017) with the packages ldatuning (Nikita, 2020), topicmodels (Grün & Hornik, 2024), and lda (Chang, 2024) was carried out to identify the overarching themes that emerged from the data. We preprocessed the speech transcripts by converting them to lowercase, removing common English and domain-specific stopwords (e.g., 'europe', 'european', 'euro'), eliminating punctuation and numbers, stemming words to their root form, and stripping excess whitespace. We determined the optimal number of topics using two metrics (Cao et al., 2009; Deveaud et al., 2014), converging on 11 topics (see Supplementary Material, Figure 1). We used Latent Dirichlet Allocation (Blei et al., 2003) to extract underlying themes within the speeches. Topic-word distributions were used to identify the 11 themes that were manually labelled (see Table 2).

Table 2. Topic model.

<i>Topic</i>	<i>Label</i>	<i>Terms</i>
1	Hybrid threats	secur cyber threat attack state cybersecur terrorist cooper crimin member
2	Disinformation as a threat to democracy	disinform elect platform inform onlin polit code manipul transpar respons
3	Digital technologies and online disinformation	digit technolog data market innov servic tech onlin protect internet
4	Ambiguous	can time world need just want one chang peopl know
5	Global security and investments	global world secur china invest chang industri suppli depend econom
6	Disinformation in health	educ health vaccin support pandem programm area covid need learn
7	Empowering and engaging citizens	citizen confer democraci futur engag commiss union institut societi panel
8	Supporting free and independent media communication	democraci media freedom rule disinform support journalist law independ plan
9	EU and migration	union peopl border fight migrat past valu right life must
10	EC's initiatives	commiss will state work need also implement propos member progress
11	Russian-Ukrainian conflict	ukrain russia support war countri financi energi russian region reform

Qualitative content analysis

The qualitative examination was conducted using MAXQDA (version 24.8; VERBI Software, 2021). We used qualitative content analysis as a systematic and interpretive procedure for describing selected aspects of meaning in qualitative data through the construction and application of a coding frame (Schreier, 2012, 2014). In this study, qualitative content analysis was not understood as a merely preliminary inductive step. Rather, it was used as a distinct qualitative method aimed at identifying recurrent meanings, categories, and narrative patterns in context. The coding frame was developed and applied following the eight-step process outlined by Schreier (2012): deciding on the research question; selecting the material; building the coding frame; segmenting the material; trial coding; evaluating and modifying the coding frame; conducting the main analysis; and presenting and interpreting the findings.

The coding frame (Table 1) combined concept-driven and data-driven categories. Concept-driven categories were derived from existing literature on disinformation misconceptions and metaphorical framings, while data-driven categories were developed to capture recurrent actor attributions and battlefield-related expressions emerging from the corpus. The qualitative content analysis therefore served to interpret how disinformation was narratively constructed in the speeches and how specific misconceptions, metaphors, and actors were articulated. Specifically, the code ‘disinformation misconceptions’ was constructed deductively and operationalizes the six misconceptions identified by Altay and Acerbi (2023). The code ‘disinformation metaphors’ was likewise constructed deductively, drawing on the literature on metaphorical framings of misinformation and disinformation: ‘battlefield-related’ metaphors were identified inductively through recurrent linguistic patterns in the corpus, while ‘health-related’ metaphors (‘environmental’ and ‘embodied health’) follow the typology proposed by Eadon and Wood (2024). The code ‘disinformation actors’ was developed inductively, based on how responsibility for spreading disinformation is attributed in the speeches. Actor categories include institutional and non-institutional, human and non-human entities, such as ‘foreign actors’,

‘EU actors’, ‘countries’, ‘political actors’, ‘private interests or companies’, ‘bots/AI/fake accounts’, and ‘undefined or generic others’. References to ordinary users or citizens were not coded as actors, as they are not described in the speeches as agents responsible for spreading disinformation. The actor labels used in the qualitative coding correspond to those reported in Figure 4 to ensure consistency between qualitative and quantitative analyses. Coding categories were not treated as mutually exclusive: a given excerpt could be coded simultaneously for multiple actors (e.g., platforms and foreign states), multiple misconceptions, and/or multiple metaphors, reflecting the layered nature of the discourse.

As the qualitative coding was conducted by a single coder, intracoding stability was assessed through a second round of coding of the full dataset, carried out 20 days after the first. Agreement between the two coding rounds was evaluated using MAXQDA’s default kappa coefficient, which follows the Brennan and Prediger (1981) free-marginal chance-correction approach. The resulting intra-coder stability was $\kappa = 0.95$, indicating a high level of consistency in code application.

Results

Word communities & bi-grams

The speeches were first studied using a community detection analysis, which made it possible to draw an initial static picture of the themes touched upon by the European Commissioners in their communication. This analysis informed the subsequent part of the research, highlighting the macro cores on which the Commission focused its attention.

As communities can be represented as networks, their observation allows an overall idea of how disinformation was defined and discussed (Figure 1).

A first community (Figure 1, centre, to the right) focuses on five words: ‘disinformation’, ‘online’, ‘platform’, ‘digital’, and ‘media’. It also includes other terms, including ‘technology’, ‘data’, ‘market’, ‘rule’, ‘skill’, ‘education’ and ‘freedom’. These words suggest that the threat of disinformation is associated with online communication, especially through digital social networks, but also that possible solutions focus on the need to enforce rules and raise the population’s skills and digital education level.

A second community of words (Figure 1, bottom) links terms that include the EU and its institutions, first and foremost the Commission, with the member states and their citizens. The network also refers to Ukraine, ‘security’, and other words, including ‘threat’, ‘people’, ‘citizen’, ‘democracy’, but also ‘cooperation’, ‘support’ and ‘future’. Therefore, the network calls for united efforts and cooperation to tackle the challenges of disinformation.

Finally, a last, extensive community (Figure 1, towards the left) is centred around the word ‘European’. Other terms refer either to the consequences that disinformation can have at a political level (‘national’, ‘election’, ‘democracy’, ‘political’), or a social level (‘society’, ‘war’, ‘global’), or to the need to face the threat (‘action’, ‘conference’, ‘challenge’, ‘build’, ‘policy’).

However, the three networks are not separate from each other. In particular, some words such as ‘EU’, ‘disinformation’, ‘European’, ‘people’, ‘democracy’, and ‘digital’

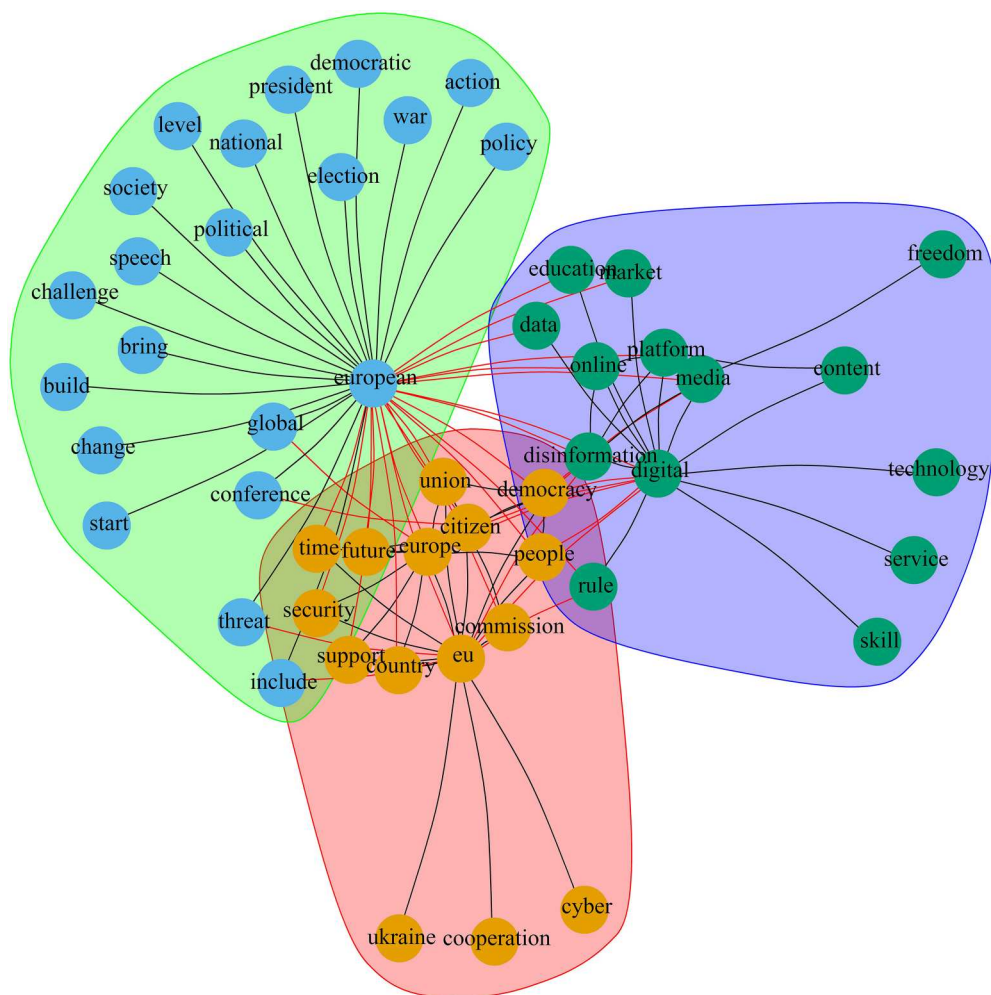


Figure 1. Word communities Leiden method (n = 238 Speeches).

connect the communities, helping to reinforce the idea that the themes are intertwined.

As expected, the analysis of the most frequently used bigrams, i.e., words that follow one after the other in the speeches, confirmed that the responsibility for spreading disinformation is linked to the Internet and digital technologies (bigrams ‘online platforms’, ‘digital services’, ‘social media’, ‘digital world’, ‘artificial intelligence’, [Figure 2](#)). However, an important finding of this analysis is that speeches on disinformation delivered by EC presidents, vice-presidents, and commissioners also touch upon some of the fundamental issues addressed by the EU, namely the social consequences and how to counteract their negative effects. It is no coincidence that the most frequent bigram is ‘civil society’ (141 times). However, ‘fundamental rights’, ‘media freedom’, ‘European democracy’, and ‘human rights’ are also mentioned, as well as worldwide problems, such as ‘COVID-19’ and ‘climate change’. Finally, there is evidence of the measures taken by the EU, as it results from the ‘action plan’, ‘data protection’ and ‘services act’ bigrams.

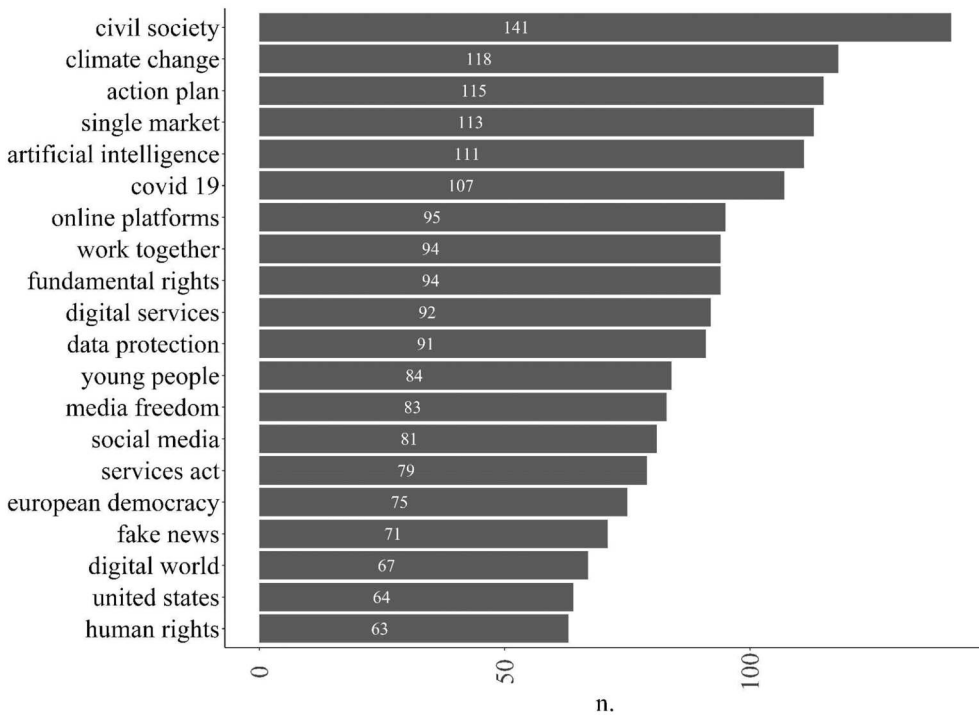


Figure 2. Most frequently used bigrams (n = 238 Speeches).

Topic modelling

We first identified and labelled the 11 topics (see [Table 2](#)). Most of the topics identified consider disinformation as a problem pervading the Internet, for example, this results from the terms associated with topic 1 (Hybrid threats, 8.4% of tokens), topic 2 (Disinformation as a threat to fair elections, 8.8% of tokens), topic 3 (Digital technologies and online disinformation, 10.1% of tokens) and topic 5 (Global security and investments, 11.0% of tokens). Terms connected with these topics are, among others, ‘cybersecur’, ‘cyber’, ‘onlin’, ‘Internet’, ‘digit’, ‘technolog’, which clearly refer to the Internet and related technologies.

Topic 8 (Disinformation, information, and democracy, 8.0% of tokens) and (again) topic 2 (Disinformation as a threat to fair elections, 8.8% of tokens) evaluate disinformation as a social media problem. The terms associated with these topics also show that they are mainly concerned with the influence of disinformation on the regularity of political elections, thus undermining democracy, on the one hand, and the freedom and independence of information on the other.

Topic 7 (Empowering and engaging citizens, 7.8% of tokens), 6 (Disinformation in health, 6.2% of tokens), and 4 (Disinformation changes the people, 13.4% of tokens) focus on the impact of disinformation on people’s behaviour. Examples of terms related to these topics are ‘citizen’, ‘people’, ‘change’, ‘learn’, and ‘engag’.

Topics 2 (Disinformation as a threat to fair elections, 8.8% of the tokens) and 6 (Disinformation in health, 6.2% of the tokens) also point out the problem that people are easily misguided.

It is also worth considering that the EU Commissioners used metaphors in their narrative rhetoric to describe disinformation. For example, topic 1 (Hybrid threats, 8.4% of tokens), topic 8 (Disinformation, information, and democracy, 8.0% of tokens), topic 9 (EU and migration, 6.3% of tokens), topic 10 (EC's measures, 11.1% of tokens) and topic 11 (Russian-Ukrainian conflict, 7.9% of tokens) frequently included battlefield (combat/defence) metaphors. Some terms linked to these topics are 'fight', 'war', 'support', 'threat', and 'attack'.

Topic 6 (Disinformation in health, 7.2% of tokens) instead included health-related metaphors with terms such as 'vaccin', 'pandem', and 'covid'.

We focused on the temporal evolution of the 11 topics by analysing their proportion across speeches over different years, focusing on trends since 2018, as in the previous years, an insufficient number of speeches was present (2 speeches in 2016 and 5 in 2017). Each speech was associated with a single topic with the highest probability. Mentions of disinformation are present in speeches that concern the current political events, and their temporal dynamic closely follows their developments (see [Figure 3](#)). Initially (2018), disinformation is associated with technology-specific topics (topics 1, 2, and 3 characterize more than 70% of the speeches). In 2020, speeches were dominated by the 'health and vaccination' theme (topic 6), in correspondence with the onset of the COVID pandemic. Again, from 2022, the Russia-Ukraine war (topic 11) starts to be linked to mentions in the speeches.

Finally, the manually coded categories were considered in relation to the topic-modelling results in order to examine how specific actors, misconceptions, and metaphors appeared across speeches associated with different topics. This step connected the computational mapping of the corpus with the qualitative interpretation of narrative patterns. For each of the 11 topics, we examined the distribution of coded references to actors ([Figure 4](#)), misconceptions ([Figure 5](#)), and metaphors ([Figure 6](#)) in the speeches associated with that topic. [Figures 4–6](#) represent the proportion of speeches (to which a given topic is associated) that contains a specific metaphor, misconception, or actor. Because

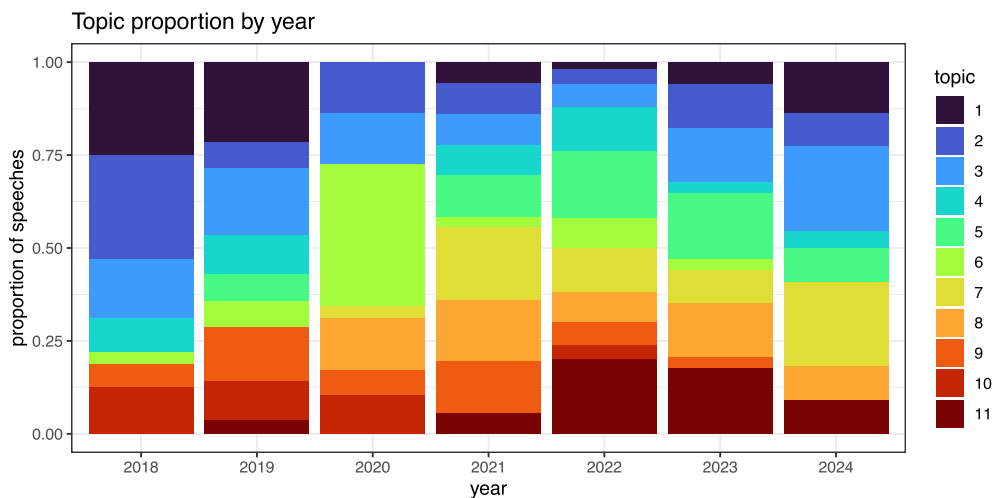


Figure 3. Longitudinal distribution of the 11 topics in the European Commission speeches (N = 238).

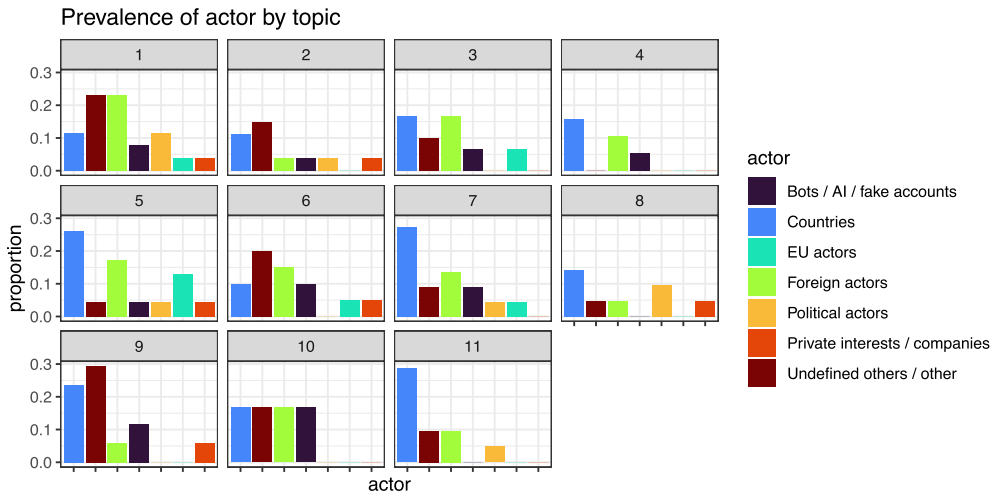


Figure 4. Proportion of actors linked to disinformation mentioned in the European Commission's speeches across topics.

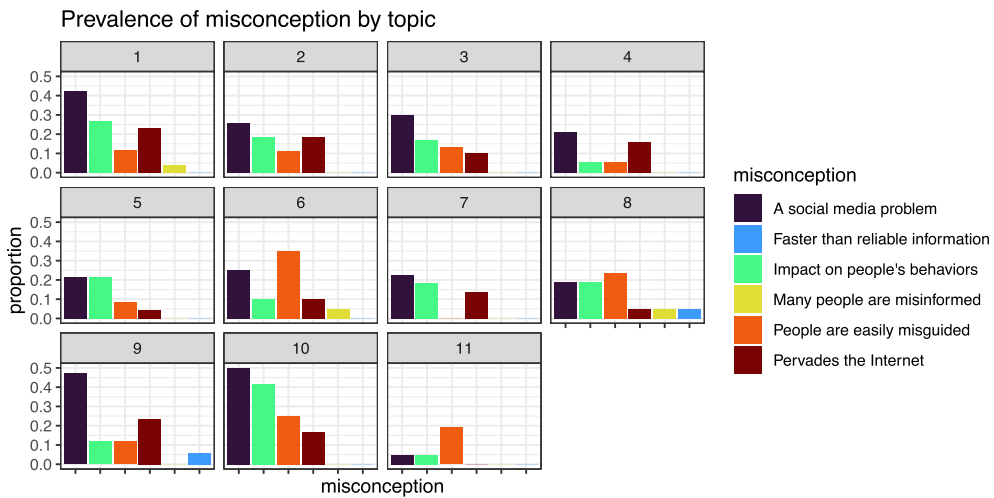


Figure 5. Proportion of misconceptions related to disinformation emerging from the European Commission's speeches across topics.

these codes are not mutually exclusive, these figures should be read as distributions of coded references rather than as a partition of the corpus into exclusive categories. Interesting aspects emerge from this integration. For example, while the idea that disinformation is mostly a social media problem appears across all topics, the misconception that people are easily misguided is especially prominent in speeches about health and vaccination (see Figure 5, Topic 6). Figure 6 disaggregates the broader battlefield metaphor into two subcategories: 'combat/attack' and 'defence'. The 'combat/attack' subcategory is the most frequent across topics, especially in Topic 11, related to the Russia–Ukraine war, and Topic 8, related to democracy and free and independent media communication.

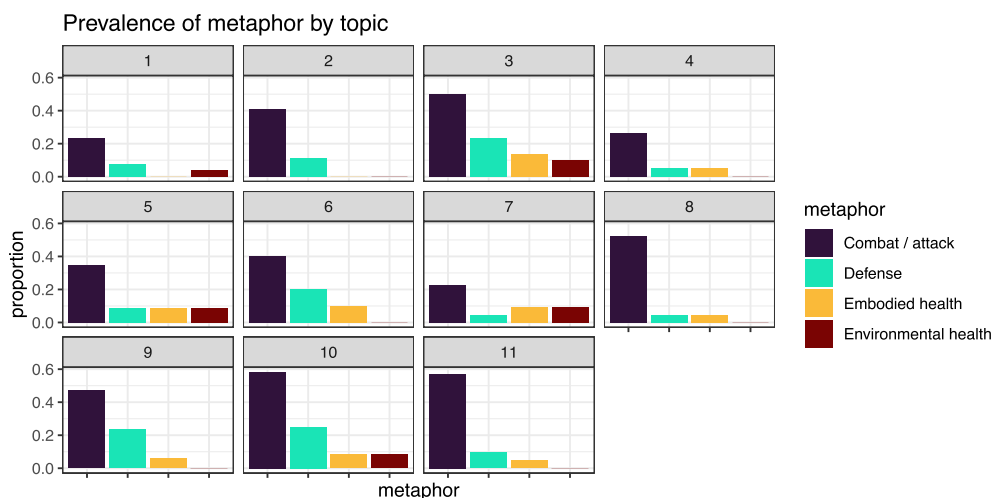


Figure 6. Proportion of metaphors used to talk about disinformation in the European Commission's speeches across topics.

Qualitative content analysis

Building on the topic modelling results, the qualitative analysis situates these framings within the political and temporal contexts in which the speeches were delivered, including the COVID-19 pandemic, electoral cycles, and the Russian invasion of Ukraine, whenever such contexts are analytically relevant to interpreting the narrative. In line with the topic modelling results – particularly Topics 1, 2, 3, 6, and 7, which emphasize hybrid threats, electoral integrity and democracy, digital technologies, health, and citizen engagement – the qualitative analysis examines how these themes are narratively constructed and linked to metaphors, actors, and responsibility attribution.

Qualitative content analysis revealed a multilayered intertwining of misconceptions, metaphors, and actors. Three features recur: (i) a securitizing tendency that externalizes agency by casting disinformation as a hybrid threat (i.e., a threat arising from a blend of cyber, information, diplomatic, and economic pressures) driven by hostile states or 'bad actors'; (ii) a platform-deterministic framing (i.e., platform design and algorithms as the primary causal driver of disinformation) that treats social media as the main source and amplifier of falsehoods; and (iii) a democracy discourse depicting citizens as vulnerable and in need of institutional protection, particularly via media-literacy 'vaccines'.

Consistent with this securitized framing, speeches portray disinformation as an instrument of information warfare – invoked through the language of 'hybrid' conflict:

I remember starting in my current role a year ago and reading an article by Eric Schmidt and Jared Cohen which began with the following, rather sobering, opening: "All future wars will begin as cyberwars. Cyberattacks and online disinformation campaigns will define the next generation of conflict, and they will unfold silently, invisibly and relatively inexpensively." That for me sums up the 'Hybrid Challenge'. (2017-06-09_JulianKing_5659-NUM-4, p. 1)

This securitizing framing corresponds to Topic 1 ('Hybrid threats') identified in the topic modelling, which clusters disinformation with security, conflict, and geopolitical competition. The dominant metaphor is that of the battlefield: disinformation is

frequently described through the language of fighting, attacks, defence, weapons, threats, and war, and is cast as an instrument wielded by state and non-state actors. In some cases, verbs such as ‘tackle’ also contribute to this framing when embedded in a security-oriented context emphasizing coordinated action or protection from threats. During COVID-19, the trope shifts to poison, fuelling an infodemic; following Russia’s 2022 invasion of Ukraine, it returns to explicit weaponization:

And what we see now while in the pandemic the disinformation served as a poison; now in war, it is used as a weapon against us. (2022-10-05_VeraJourova_2983–NUM-149, p. 2)

But this is not the only virus that is causing problems. The coronavirus pandemic has been accompanied by a massive infodemic. (2020-10-06_JosepBorrellFontelles_1036–NUM-76, p. 1)

This externalization of agency is self-absolving; temporally, attribution patterns evolve as follows: in 2016–2019 speeches, responsibility is placed primarily on foreign governments – above all, Russia – alongside ‘foreign adversaries’, bots, and diffuse ‘bad actors’, with politically driven disinformation (e.g., targeted online advertising) also flagged. From 2020, the cast widens to include China and the Lukashenko regime,⁷ although Russia remains the modal referent. By 2023–2024, attention shifts to technological force multipliers – AI and generative AI (including deepfakes) – as amplifiers of cross-border campaigns. Although noted less frequently, some speeches also acknowledge EU-internal sources, underscoring that disinformation ‘knows no borders’ (2021-24-06_VeraJourova_7648–NUM-115, p. 1).

The Kremlin fights with bombs in Ukraine, but with words everywhere else, including in the EU. (2023-26-09_VeraJourova_4645–NUM-201, p. 2)

‘We see how AI, including deepfakes, can be used today to amplify disinformation – I call it disinformation on steroids’. (2024-21-03_VeraJourova_1647–NUM-228, p. 2)

A hybrid threat with different actors involved constitutes a complex issue requiring a ‘more nuanced’ (2019-11-04_VeraJourova_2119–NUM-52, p. 2), ‘whole-of-society’ (2023-26-09_VeraJourova_4645–NUM-201, p. 1), ‘holistic approach’ involving several strategies and actors, as indicated by EC Commissioner Věra Jourová:

To counter disinformation, we need a holistic approach: 1. we need to equip authorities and improve cooperation among them in the EU 2. we need to beef up our cooperation with international partners, including NATO. Disinformation is part of the hybrid threats, so this is a security issue as well. 3. we need to engage civil society 4. we need to support free and independent media, resilient and critical citizens. To sum up, we all need to get better in detecting, analysing and exposing disinformation. (2020-04-06_VeraJourova_1000–NUM-75, p. 2)

This passage is one of the clearest instances in which the EC explicitly acknowledges the complexity of disinformation and the plurality of actors and strategies involved. However, while the rhetoric emphasizes a ‘holistic’ and ‘whole-of-society’ approach, the enumeration of concrete actions remains strongly structured around security cooperation, platform-centred detection and exposure, and citizen-focused resilience and media literacy. Institutional self-reflection on endogenous drivers – such as political communication practices, trust dynamics, or structural features of the media system – remains largely implicit rather than developed as a distinct line of intervention.

This recognition of complexity is consistently accompanied by the claim that such an approach is necessary and unavoidable. As highlighted by EC President Ursula von der Leyen,⁸ disinformation is not a merely politically related issue but ‘a societal one’ because it makes it ‘impossible to distinguish’ what is true (2022-22-09_UrsulavonderLeyen_5723–NUM-163, p. 4). Despite the recognition that disinformation campaigns were a problem also before the advent of the internet, speeches tend to normalize a technologically driven spread of disinformation as ‘everywhere online’ (2021-25-05_UrsulavonderLeyen_2671–NUM-108, p. 1) – which underwrites exceptional, security-oriented remedies.

I wouldn’t go so far as to call it the oldest profession, but the manipulation of information to interfere with public opinion has certainly been around for centuries. What is different today, however, are the digital tools which make mis- and disinformation easier, cheaper and more impactful on society. (2018-05-12_JulianKing_4129–NUM-40, p. 1)⁹

Accordingly, speeches call for ending the ‘digital Wild West’ (2020-07-07_VeraJourova_2817–NUM-80, p. 1), a space where disinformation and data-misuse actors (e.g., Cambridge Analytica) can operate; environmental-health metaphors reinforce this shift, as the internet ‘is to online disinformation what wind is to wildfire. It spreads it fast and wide, so the damage is difficult to contain’ (2022-22-06_VeraJourova_4005–NUM-158, p. 2). At the same time, disinformation is presented as an almost inevitable by-product of digital infrastructures, which naturalizes a platform-deterministic view and narrows remedies to platform governance. This platform-deterministic narrative corresponds to Topic 3 (‘Digital technologies and online disinformation’) identified in the topic modelling, which clusters references to platforms, algorithms, and digital infrastructures in discussions of disinformation. From 2018 onward, speeches increasingly call to ‘take action’, with the Code of Practice (voluntary; strengthened in 2022) framed as a first step and the Digital Services Act (DSA) and the Digital Markets Act (DMA) as a co-/re-regulatory accountability regime – while insisting that platforms ‘need to do more’ (2020-10-06_VeraJourova_1033–NUM-77, p. 1). The prescribed remedy thus targets platforms rather than institutional communication or accountability practices, aligning the policy response with the self-absolving diagnosis. The DSA and the DMA are two of the main measures of the EC ‘rulebook’ (2022-07-02_VeraJourova_851–NUM-137, p. 2) for digital platforms ‘to become more accountable’, adopting a ‘co-regulatory scheme to ensure transparency, regulatory oversight and accountability of online platforms’ (2021-10-06_VeraJourova_7594–NUM-111, p. 3).

Social media platforms are perceived as amplifiers of disinformation because of their algorithms and profit-oriented practices – with disinformation becoming a ‘multi-million Euro weapon of mass manipulation’ (2023-23-10_VeraJourova_5252–NUM-209, p. 2) —, and spreading faster than reliable information:

Lying sells better and flies quicker than the truth, which makes it a special challenge. (2020-04-06_VeraJourova_1000–NUM-75, p. 2)

Remembering the anniversary of the Capitol Hill events,¹⁰ EC Commissioner Thierry Breton explicitly points the finger at the responsibility of social media for having favoured – and benefited from – the spread of disinformation:

What we experienced was the culmination of years of uncontrolled hate speech, incitement to violence, disinformation and destabilisation strategies spread on social networks without

restraint and from which these platforms have – it must be admitted – largely profited. It has become clear to all that the absence of rules and democratic control over the decisions of a handful of large platforms, which have now become systemic public spaces, is no longer tolerable. (2022-19-01_ThierryBreton_431–NUM-134, p. 1)

This centres responsibility on platforms' governance and business models, while pushing institutional communication and political accountability into the background.

According to EU Commissioner Vytenis Andriukaitis,¹¹ referring to the drop in immunization against poliomyelitis in Pakistan and the increase in disease infections, (social) media also contributed to spreading vaccine-related disinformation, highlighting the direct impact of this disinformation and fake news on vaccination decisions.

Two million Pakistani households have refused immunisations for children since April, following television and social media reports about adverse reactions to a vaccination drive. In many ways, this is a perfect example of the massive dangers posed by myths, disinformation, vaccine hesitancy and fear. (2019-12-09_VytenisAndriukaitis_7246–NUM-62, p. 1)

Disinformation that led people to ignore official health advice and engage in risky behaviour. (2020-03-07_MargretheVestager_2810–NUM-79, p. 1 - 2)

In these framings, vaccine refusal is predominantly narrated through the lens of disinformation exposure, with other possible explanatory factors – such as trust in institutions, health-system performance, or historical and socio-cultural contexts – remaining largely implicit. This does not preclude the relevance or interaction of such factors, but it highlights how responsibility is discursively relocated toward information flows and away from endogenous institutional or systemic dynamics. These excerpts also show that disinformation is perceived – and addressed as – having a non-negligible impact on directing people's behaviours in their daily lives. The main fields in which online disinformation is believed to have a greater (negative) impact are health and politics – especially related to voting (e.g., Brexit and EU elections). This framing reflects the prominence of Topic 2 ('Disinformation as a threat to fair elections') and Topic 6 ('Disinformation in health') in the topic modelling, which respectively foreground electoral integrity and public health as particularly vulnerable domains.

Lastly, with less than 3 months to go until the European elections, it is our duty to ensure that our citizens can cast their ballot without interference and without disinformation to confuse their choices. (2019-07-03_DimitrisAvramopoulos_6959–NUM-43, p. 2)¹²

A myriad of data analytics and communication firms work daily with our data to try to figure out the best way to convince us to buy something or vote for someone or not to vote at all. (2021-25-11_VeraJourova_6309–NUM-130, p. 1)

Domestic political discontent is thus reframed as an interference problem to be filtered out, relocating causality from institutional performance to exposure to disinformation.

The US presidential elections, Brexit referendum and the Cambridge Analytica case helped us realise that modern technology can be used by private or foreign interests to take advantage of our digital presence and to manipulate our elections. (2018-25-09_Dubravka-Suica_5883–NUM-21, p. 2)

By foregrounding ‘modern technology’ and foreign and/or private interests, this framing shifts explanatory weight away from party strategies or policy choices and onto externalized, technologically mediated causes.

In this landscape, EU citizens are often seen as defenseless actors affected by and at the mercy of disinformation, who can be easily misguided by it, and in need of (institutional) help to navigate the Internet pitfalls. Hence, promoting initiatives aimed at increasing citizens’ media literacy and their empowerment online. This strand of the discourse closely resonates with Topic 7 (‘Empowering and engaging citizens’) identified in the topic modelling, which emphasizes citizen engagement, education, and resilience in response to disinformation. Across the speeches, this institutional effort to ‘educate’ citizens is presented as needed, also based on the results of the Eurobarometer survey on democracy, which highlighted that 73% of EU citizens are worried about disinformation online in the pre-election period. Especially starting in 2020, EC Commissioners increasingly promoted media and digital literacy initiatives for the broader population and young citizens – e.g., through the Digital Education Action Plan.

The European Commission supports projects to strengthen media literacy and combat disinformation through the Creative Europe program and through the European Digital Media Observatory (EDMO). We also encourage media literacy through education and training: the Directive on audiovisual media services. (2023-31-05_DubravkaSuica_3475–NUM-194, p. 1)

Education is presented as playing a fundamental role in fighting the disinformation phenomenon: educational programmes (also) aimed at developing citizens’ critical thinking, which is presented as ‘a ‘vaccine’ against the infodemic that we have experienced during the height of the COVID-19 pandemic’. (2021-11-10_Dubravka-Suica_7838–NUM-122, p. 1) Education and digital literacy increase societal resilience, considered ‘the best vaccine against a virus of disinformation’ (2024-31-05_VeraJourova_3041–NUM-236, p. 3), ‘the best antibodies for the virus of disinformation’ (2023-26-10_VeraJourova_5353–NUM-211, p. 2).

Finally, it is interesting to note that in a 2018 speech by EC Commissioner Věra Jourová, the disinformation issue seems to be reframed in less alarmist terms. A more cautious framing that, nonetheless, seems to have been at least partly abandoned over the considered time.

Many in the so called political mainstream blame the rise of nationalism and populism on fake news or Russian bots. But if any of us in this room believes that it is only because of the bots that people switched their votes from the pro-EU liberal forces to nationalists, then we have a much bigger problem than I thought. We have to recognise the danger coming from disinformation. Disinformation can create divisions and relativise the values that are dear to all of us. At the same time, we have to admit that it’s not the bots that caused the financial crisis, it’s not because of fake news that the living conditions in Greece have deteriorated or that youth unemployment in Spain is still above 40%. (2018-09-11_VeraJourova_4050–NUM-29, p. 2)

Overall, while occasional voices acknowledged the limits of attributing political outcomes to ‘bots’ or ‘fake news’, these reflexive moments remained marginal. The dominant storyline remained self-absolving – locating the problem in foreign actors and digital platforms – and fatalistic – portraying disinformation as structurally embedded

in today's online environment. This framing both legitimized the Commission's security-oriented and regulatory agenda and positioned citizens primarily as recipients of protection and education, with comparatively less emphasis on their role as active political participants in shaping democratic resilience.

Discussion

The analysis of the European Commission leadership's speeches reveals a rhetorical use of the narrative of disinformation that foregrounds it as a central explanatory frame for undesirable behaviours and their outcomes. On the one hand, speeches tend to externalize the sources of disinformation and, on the other hand, to naturalize its spread as a technological inevitability. This pattern should be read in relation to the specific discursive context examined here: speeches in which disinformation is explicitly invoked as a policy problem, rather than as a comprehensive account of EU institutional communication across all policy domains. Indeed, this narrative is used as a flexible resource to project onto other, external actors, or gullible citizens (Altay & Acerbi, 2023), the responsibility and blame for events like the Brexit vote and other political crises or electoral results considered negative, thereby undermining self-criticism and related acceptance of institutional failures. This narrative also serves the purpose of identifying external enemies (e.g., digital platforms, Russian hackers ...) while strengthening internal cohesion, in a classical 'us vs. them' argument. This alignment is self-absolving – displacing scrutiny from EU institutional performance, media systems, and policy choices – and fatalistic – presenting disinformation as an ambient condition of the digital environment rather than a contingent, socially mediated phenomenon. While these framings intensify during moments of crisis – such as the COVID-19 pandemic or geopolitical conflict – their recurrence across different policy domains and time periods suggests a relatively stable narrative repertoire rather than a purely situational rhetoric.

For example, objections to vaccinations by some citizens are mainly attributed to downstream effects of (social) media falsehoods, and contentious electoral outcomes are narrated as products of external manipulation rather than of party strategies, institutional communication, or policy performance. The fatalistic register is likewise visible in claims that disinformation is 'everywhere online' and moves 'faster than truth', often reinforced by environmental- and health-related metaphors that naturalize diffusion. These framings thus tend to relocate causality to platforms and foreign actors and away from EU institutions and 'domestic' media systems.

These patterns resonate with scholarship that conceptualizes disinformation as a discursive construct through which political institutions delineate threats and legitimize intervention (Egelhofer et al., 2020; Farkas, 2023). In particular, the combination of externalization and platform-centred remedies echoes the tension identified in EU discourse between geopolitical framings of disinformation as an external security threat and regulatory framings targeting digital infrastructures (Casero-Ripollés et al., 2023), while our analysis further specifies the self-absolving and fatalistic logic that structures this narrative. The findings also resonate with Boudana and Segev's (2026) analysis of mainstream media coverage of fake news, which shows that fake news is commonly framed through questions of causality, responsibility,

and solutions, with political actors and social media platforms occupying central positions in the narrative. While their study focuses on mainstream media rather than institutional EU discourse, the parallel is instructive: in both cases, the framing of false information tends to organize responsibility around identifiable political and platform actors, while shaping public understandings of the problem and of legitimate responses. Our analysis extends this insight to the EU institutional level, showing how similar responsibility attributions are embedded in a broader self-absolving and security-oriented discourse.

It is no coincidence that recurring metaphors to describe disinformation and fight against disinformation draw upon biology and, in particular, immunology: disinformation is a virus, and we need antibodies to fight it. While Topic 7 ('Empowering and engaging citizens') foregrounds empowerment and engagement at the quantitative level, the qualitative analysis shows that this empowerment is predominantly framed in pedagogical and immunological terms, reinforcing a view of citizens as recipients of protection rather than as political interlocutors. Notably, even when the EC explicitly invokes a 'whole-of-society' or 'holistic' approach, these claims tend to translate into an expanded coordination of security, platform governance, and educational measures, rather than into a sustained engagement with institutional accountability or participatory democratic reform. The policy corollary is a securitized and technocratic repertoire: co-/regulating platforms, enhancing detection and takedown, and partnering with civil society for literacy 'vaccines'. While such measures can be warranted and may complement other approaches, the remedial repertoire articulated in the speeches is most consistently framed in terms of platform governance (e.g., co-/regulation, transparency requirements for platforms, takedown/detection) and citizen-focused educational responses (media/digital literacy and resilience). References to broader democratic remedies – such as institutional transparency, responsiveness, media pluralism, or participatory channels – are not incompatible with this agenda, but they are less systematically developed as remedies within the speech framing and are often invoked as general democratic values rather than as institutional accountability commitments. In this way, the solution space narrows to platform rules and content enforcement, with little attention to how institutions communicate, listen, or account for their own performance. In this sense, democracy becomes the fortress to be defended, and citizens the body to be immunized. This framing connects with a longstanding historical tradition in overlapping infectious diseases and foreign dangers or enemies, in which the medical virus is often considered to come from the 'outside' and brought in by foreigners (Boeynaems et al., 2017; Deignan, 2016; Eadon & Wood, 2024; Lakoff & Johnson, 1980). This narrative often includes two sub-narratives and related assumptions: (1) a notion of citizens as weak, unprepared, and easy prey of disinformation; (2) an overlapping of disinformation and social media, with the equation traditional news information = good quality, information on social media = poor quality.

Rebalancing the narrative would entail acknowledging endogenous drivers (such as trust dynamics, efforts to improve the quality of institutional communication, incentive structures in politics and media) alongside exogenous ones, and shifting from platform determinism to a broader account of how messages become credible and mobilizing in specific contexts. Importantly, a democracy-first framing need not presume civic helplessness; it can treat citizens as interlocutors rather than people lacking education – emphasizing participation,

accountability, and institutional learning together with proportionate platform governance. Both the general narrative and sub-narratives appear questionable in the face of several studies and recent literature (Altay & Acerbi, 2023; Budak et al., 2024; Carlson, 2018; Hoffmann, 2023). However, they serve the above-described rhetorical purposes: a justification available and adaptable to different cases and circumstances.

A few limitations should be noted. This study analyses official European Commission leadership speeches that explicitly contain the keyword ‘disinformation’. While this provides a longitudinal and comparable corpus of public framing, it also constrains representativeness in two ways. First, speeches constitute a specific genre of institutional communication – often oriented toward agenda-setting, legitimization, and public positioning – and therefore may not fully reflect internal deliberation, implementation practices, or the full range of policy instruments. Second, restricting the corpus to speeches that explicitly use the term ‘disinformation’ may under-represent adjacent framings expressed through other keywords (e.g., ‘misinformation’, ‘information manipulation’, ‘foreign interference’) or through other communication channels such as press releases, policy documents, and regulatory texts, or speeches hosted in other institutional repositories (such as the European External Action Service – EEAS). Accordingly, our findings are best interpreted as evidence about the EC’s public narrative and rhetorical framing of disinformation in leadership speeches, rather than as a comprehensive account of EU information policy as such. Furthermore, our analysis did not disaggregate systematically by individual Commissioner, partly because a small number of speakers are present in the corpus (see Tables 1 and 2 in the Supplementary Material). Most speeches on disinformation come from Věra Jourová (n = 39), Dubravka Šuica (n = 26), Ursula von der Leyen (n = 26), Julian King (n = 20), Valdis Dombrovskis (n = 15), and Mariya Gabriel (n = 14), suggesting room for future work on speaker-level framing differences. Further research should also examine how audiences perceive and evaluate this narrative: Do citizens accept it as a convincing explanation, and with what cross-group variations? Finally, to what extent do societal actors (media, parties, civic groups) co-produce the narrative because it also offers rhetorical justifications for their own positions?

Our findings show that the Commission’s discourse on disinformation functions as a generally self-absolving and fatalistic narrative: it centres external adversaries and technological infrastructures while backgrounding endogenous accountability. Recognizing this pattern does not deny real cross-border manipulation; rather, it clarifies how framing choices narrow remedies to platform governance and ‘vaccines’, with citizens cast chiefly as subjects in need of protection. Treating disinformation as the *root* cause risks overlooking the social, economic, and institutional conditions that let falsehoods take hold. Effective prevention therefore requires treating both the information problem and its broader social ecology. A more balanced communication approach would retain proportionate platform rules while investing in institutional transparency, media pluralism, and participatory channels that treat citizens as active interlocutors. Reframing along these lines widens the policy horizon beyond digital platform determinism and supports a thicker, more accountable vision of European democracy. This also outlines a way out of fatalism: by centreing credibility, trust, and participation, the field of action widens beyond the assumptions that disinformation is an inevitable by-product of digital infrastructures.

Notes

1. For a critical overview of the origins and diffusion of the ‘infodemic’ metaphor see Simon and Camargo (2023).
2. <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation>.
3. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.
4. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en#countering-disinformation.
5. <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423>.
6. <https://ec.europa.eu/commission/presscorner/home/en>.
7. Since 1994, Belarus is governed by a post-Soviet authoritarian system ruled by Alexander Lukashenko and its government.
8. Ursula Gertrud von der Leyen is a German politician, serving as the 13th president of the European Commission. This is a role that she has held since 2019. She served in the German federal government between 2005 and 2019, holding positions in Angela Merkel’s cabinet, most recently as Federal Minister of Defence.
9. Julian Beresford King is a British diplomat and civil servant who served as the final British European Commissioner for the Security Union from 2016 to 2019 prior to Brexit, having previously served as the British ambassador to Ireland (2009–2011) and France (2016).
10. On 6 January 2021, the United States Capitol — seat of the Congress of the United States — was attacked by a mob of Donald Trump’s supporters in the attempt to self-coup to protest against Trump’s defeat in the 2020 presidential elections.
11. Vytenis Povilas Andriukaitis is a member of the European Parliament from 2024 July, a former WHO Special Envoy for the European region, a former European Commissioner for Health and Food Safety, a heart surgeon, a co-signatory to the 1990 Act of the Re-Establishment of the State of Lithuania.
12. Dimitris Avramopoulos is a Greek politician of the conservative New Democracy party, and former career diplomat. He has served in various high-level cabinet posts, including Minister for Foreign Affairs and Minister for National Defence, and was Mayor of Athens from 1995 to 2002.
13. The term ‘tackle/tackled’ was not treated as inherently battlefield-related. Since the term can also function as a generic policy verb meaning ‘to address’, it was coded as battlefield-related only when its immediate context connected disinformation to threats, attacks, security, coordinated action, or the protection of citizens. In these cases, ‘tackle’ contributed to a broader adversarial or defensive framing rather than being interpreted as a battlefield metaphor in isolation.

Author contributions

CRedit: **Eliana Fattorini**: Conceptualization, Data curation, Formal analysis, Methodology, Visualization, Writing – original draft, Writing – review & editing; **Alberto Acerbi**: Conceptualization, Data curation, Formal analysis, Methodology, Visualization, Writing – original draft, Writing – review & editing; **Massimiano Bucchi**: Conceptualization, Supervision, Writing – original draft, Writing – review & editing; **Enzo Lonner**: Conceptualization, Data curation, Formal analysis, Methodology, Visualization, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Eliana Fattorini, Research Fellow at the Department of Sociology and Social Research at the University of Trento (Italy), where she collaborates on the Science, Technology, and Society – STSTN.

Her work focuses on vaccine hesitancy, science communication, and the broader relationship between science and society [email: eliana.fattorini@unitn.it].

Alberto Acerbi, Associate Professor at the Department of Sociology and Social Research at the University of Trento (Italy). His work is at the interface of psychology, anthropology, and sociology. Particularly, his research interests include cultural evolution and cognitive anthropology [email: alberto.acerbi@unitn.it].

Massimiano Bucchi, Full Professor of Science and Technology in Society and Director of the International Master SCICOMM at the Department of Sociology and Social Research at the University of Trento (Italy). His research interests include Science and Technology in Society, Science Communication, The Public Image of Science and Technology [email: massimiano.bucchi@unitn.it].

Enzo Loner, PhD in Sociology. He works at the Department of Sociology and Social Research of the University of Trento (Italy). His works use quantitative and mixed-mode methods to focus on science and society, political participation and communication, social media and public opinion [email: enzo.loner@unitn.it].

ORCID

Eliana Fattorini  <http://orcid.org/0000-0002-9758-7578>

Alberto Acerbi  <http://orcid.org/0000-0001-5827-8003>

Massimiano Bucchi  <http://orcid.org/0000-0003-3005-9639>

Enzo Loner  <http://orcid.org/0000-0002-5195-3376>

References

- Altay, S., & Acerbi, A. (2023). People believe misinformation is a threat because they assume others are gullible. *New Media & Society*, 26(11), 6440–6461. <https://doi.org/10.1177/14614448231153379>
- Altay, S., Berriche, M., & Acerbi, A. (2023). Misinformation on misinformation: Conceptual and methodological challenges. *Social Media + Society*, 9(1), 1–13. <https://doi.org/10.1177/20563051221150412>
- Bedi, P., & Sharma, C. (2016). Community detection in social networks. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 6(3), 115–135. <https://doi.org/10.1002/widm.1178>
- Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet allocation. *Journal of Machine Learning Research*, 3, 993–1022. <https://doi.org/10.7551/mitpress/1120.003.0082>
- Boeynaems, A., Burgers, C., Konijn, E. A., & Steen, G. J. (2017). The effects of metaphorical framing on political persuasion: A systematic literature review. *Metaphor and Symbol*, 32(2), 118–134. <https://doi.org/10.1080/10926488.2017.1297623>
- Boudana, S., & Segev, E. (2026). Fake News makes the news: Definitions and framing of fake news in mainstream media. *Journalism Practice*, 20(2), 679–698. <https://doi.org/10.1080/17512786.2024.2379898>
- Brennan, R. L., & Prediger, D. J. (1981). Coefficient kappa: Some uses, misuses, and alternatives. *Educational and Psychological Measurement*, 41(3), 687–699. <https://doi.org/10.1177/001316448104100307>
- Budak, C., Nyhan, B., Rothschild, D. M., Thorson, E., & Watts, D. J. (2024). Misunderstanding the harms of online misinformation. *Nature*, 630, 45–53. <https://doi.org/10.1038/s41586-024-07417-w>
- Cao, J., Xia, T., Li, J., Zhang, Y., & Tang, S. (2009). A density-based method for adaptive LDA model selection. *Neurocomputing: An International Journal*, 72(7-9), 1775–1781. <https://doi.org/10.1016/j.neucom.2008.06.011>
- Carlson, M. (2018). Fake news as an informational moral panic: The symbolic deviancy of social media during the 2016 US presidential election. *Information, Communication & Society*, 23(3), 374–388. <https://doi.org/10.1080/1369118X.2018.1505934>

- Casero-Ripollés, A., Tuñón, J., & Bouza-García, L. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications*, 10(1), 657. <https://doi.org/10.1057/s41599-023-02179-8>
- Chang, J. (2024). *_lda: Collapsed Gibbs sampling methods for topic models_*. R package version 1.5.2, <https://CRAN.R-project.org/package=lda>.
- Csárdi, G., Nepusz, T., Traag, V., Horvát, S., Zanini, F., Noom, D., & Müller, K. (2024). *igraph: Network Analysis and Visualization in R*. <https://doi.org/10.5281/zenodo.7682609>, R package version 2.0.3, <https://CRAN.R-project.org/package=igraph>.
- Deignan, A. H. (2016). From linguistic to conceptual metaphors. In E. Semino & Z. Demjen (Eds.), *The Routledge handbook of metaphor and language*. *Routledge handbooks in linguistics* (pp. 120–134). Routledge.
- Deveaud, R., SanJuan, E., & Bellot, P. (2014). Accurate and effective latent concept modeling for ad hoc information retrieval. *Document numérique*, 17(1), 61–84. <https://stm.cairn.info/revue-document-numerique-2014-1-page-61?lang=en>.
- Eadon, Y. M., & Wood, S. E. (2024). Combating contamination and contagion: Embodied and environmental metaphors of misinformation. *Convergence: The International Journal of Research into New Media Technologies*, 31(2), 500–520. <https://doi.org/10.1177/13548565241255347>
- Egelhofer, J. L., Aldering, L., Eberl, J., Galyga, S., & Lecheler, S. (2020). From novelty to normalization? How journalists use the term “Fake News” in their reporting. *Journalism Studies*, 21(10), 1323–1343. <https://doi.org/10.1080/1461670X.2020.1745667>
- European Commission. (2022). 2022 strengthened code of practice on disinformation. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.
- Farkas, J. (2023). News on fake news: Logics of media discourses on disinformation. *Journal of Language and Politics*, 22(1), 1–21. <https://doi.org/10.1075/jlp.22020.far>
- Farkas, J., & Schou, J. (2019). *Post-truth, fake news and democracy: Mapping the politics of falsehood*. Routledge.
- Fortunato, S. (2010). Community detection in graphs. *Physics Reports*, 486(3-5), 75–174.
- Galanopoulos, A., & Stavarakakis, Y. (2022). Populism, anti-populism and post-truth. In M. Oswald (Ed.), *The Palgrave handbook of populism* (pp. 407–420). Springer International Publishing. https://doi.org/10.1007/978-3-030-80803-7_25
- Gelfert, A. (2018). Fake news: A definition. *Informal Logic*, 38(1), 84–117. <https://doi.org/10.22329/il.v38i1.5068>
- Grün, B., & Hornik, K. (2024). *_topicmodels: Topic Models_*. R package version 0.2-17, <<https://CRAN.R-project.org/package=topicmodels>>.
- Hoffmann, C. P. (2023). The role of moral panics in media transformation: An examination of the ‘tech-lash.’ In A. Godulla & S. Böhm (Eds.), *Digital disruption and media transformation: How technological innovation shapes the future of communication* (pp. 41–54). Springer International Publishing.
- Jungherr, A., & Schroeder, R. (2021). Disinformation and the structural transformations of the public arena: Addressing the actual challenges to democracy. *Social Media + Society*, 7(1), 1–13. <https://doi.org/10.1177/2056305121988928>
- Khan, A., Brohman, K., & Addas, S. (2022). The anatomy of ‘fake news’: Studying false messages as digital objects. *Journal of Information Technology*, 37(2), 122–143. <https://doi.org/10.1177/02683962211037693>
- Kuo, R., & Marwick, A. (2021). Critical disinformation studies: History, power, and politics. *Harvard Kennedy School Misinformation Review*, 2(4), 1–12. <https://doi.org/10.17615/2e3z-m450>
- Lakoff, G., & Johnson, M. (1980). The metaphorical structure of the human conceptual system. *Cognitive Science*, 4(2), 195–208. https://doi.org/10.1207/s15516709cog0402_4
- Lecheler, S., & Egelhofer, J. L. (2022). Disinformation, misinformation, and fake news: Understanding the supply side. In J. Strömbäck, Å Wikforss, K. Glüer, T. Lindholm, & H. Oscarsson (Eds.), *Knowledge resistance in high-choice information environments* (pp. 69–87). Routledge.
- Monsees, L. (2020). A war against truth’—Understanding the fake news controversy. *Critical Studies on Security*, 8(2), 116–129. <https://doi.org/10.1080/21624887.2020.1763708>

- Monsees, L. (2023). Information disorder, fake news and the future of democracy. *Globalizations*, 20(1), 153–168. <https://doi.org/10.1080/14747731.2021.1927470>
- Murakami, A., Thompson, P., Hunston, S., & Vajn, D. (2017). ‘What is this corpus about?’: Using topic modelling to explore a specialised corpus. *Corpora*, 12(2), 243–277.
- Nikita, M. (2020). *_ldatuning: Tuning of the Latent Dirichlet Allocation Models Parameters_*. R package version 1.0.2, <<https://CRAN.R-project.org/package=ldatuning>>.
- Pielemeier, J. (2020). Disentangling disinformation: What makes regulating disinformation so difficult? *Utah Law Review*, 4, 917–940.
- Poushter, J., Fagan, M., Smerkovich, M., & Prozorovsky, A. (2025). *International opinion on global threats*. Pew Research Center. Available at https://www.pewresearch.org/wp-content/uploads/sites/20/2025/08/pg_2025.08.19_global-threats_reporta.pdf.
- Radnitz, S. (2025). Contesting authority to adjudicate misinformation. *Perspectives on Politics*, 1–23.
- R Core Team. (2024). *_R: A Language and environment for statistical computing_*. R Foundation for Statistical Computing. <https://www.R-project.org/>.
- Schäfer, M. S. (2023). The notorious GPT: Science communication in the age of artificial intelligence. *Journal of Science Communication*, 22(02), Y02. <https://doi.org/10.22323/2.22020402>
- Schreier, M. (2012). *Qualitative content analysis in practice*. SAGE Publications Ltd. <https://doi.org/10.4135/9781529682571>
- Schreier, M. (2014). Qualitative content analysis. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 170–183). SAGE Publications, Inc. <https://doi.org/10.4135/9781446282243.n12>
- Simon, F. M., & Camargo, C. Q. (2023). Autopsy of a metaphor: The origins, use and blind spots of the ‘infodemic’. *New Media & Society*, 25(8), 2219–2240. <https://doi.org/10.1177/14614448211031908>
- Traag, V. A., Waltman, L., & Van Eck, N. J. (2019). From Louvain to Leiden: Guaranteeing well-connected communities. *Scientific Reports*, 9(1), 5233. <https://doi.org/10.1038/s41598-019-41695-z>
- VERBI Software. (2021). MAXQDA 2022 [computer software]. Berlin, Germany: VERBI Software. Available from maxqda.com.
- Vogler, D., Eisenegger, M., Fürst, S., Udriș, L., Ryffel, Q., Rivière, M., & Schäfer, M. S. (2023). Artificial intelligence in news production: Perception and acceptance among the Swiss population. *Yearbook Quality of the Media Study*, 1–11.
- World Economic Forum. (2025). Global Risks Report 2024. Insight report, 20th edition. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.