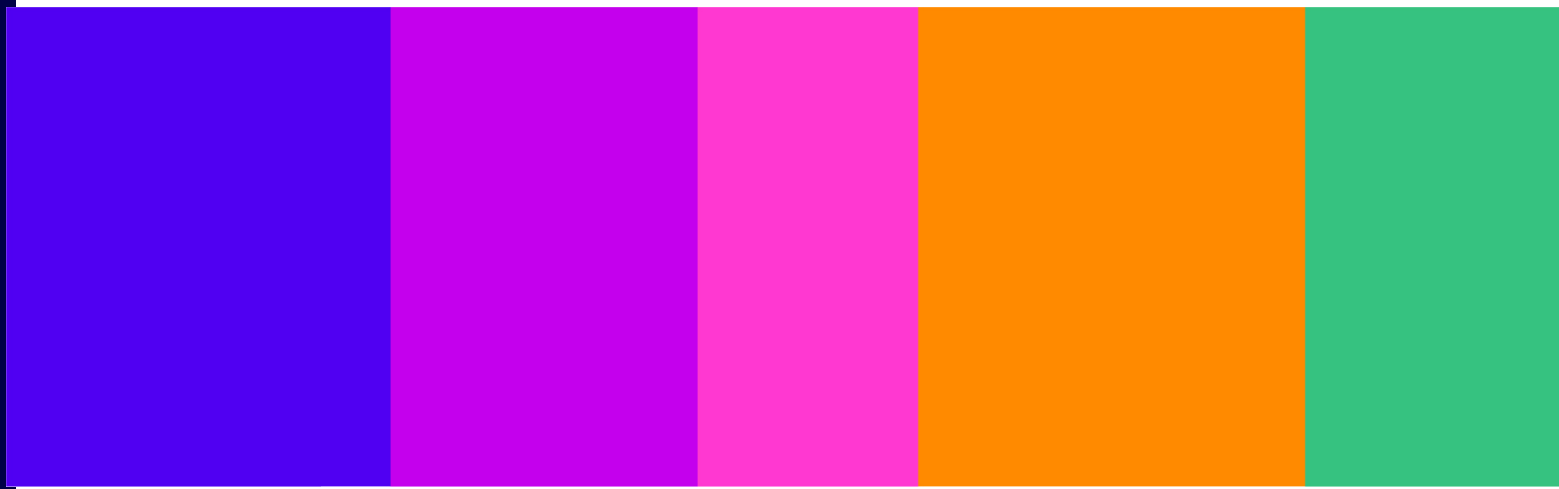


A literature review on online information- based threats to elections

Literature review

Published: 13 October 2026



Contents

Section

Summary	3
Introduction	4
Taxonomy and literature review	8
Annex	33

Summary

This review aims to provide an overview of literature examining online information-based threats to elections. It focuses on intentionally deceptive or abusive behaviours that might inform the work of the Online Information Advisory Committee. The literature examined highlighted a wide range of research on this topic, which we organised into four categories.

Information manipulation. Some literature explored information manipulation covering suspected intent to shape perceptions, narratives or understanding with fake or manipulated content. There are several examples of information that has been fabricated or altered in an attempt to influence elections. Some sources highlighted that these include the creation of fake or impersonated news outlets, false or misleading claims, the impersonation of real people, or fake personas that do not represent real people. According to the literature, AI-produced content from LLMs appears to be an emerging factor in information manipulation.

Ecosystem manipulation, involving efforts to shape discoverability, delivery, or apparent provenance of information. This review surfaced literature which provided evidence for attempts at the manipulation of platform features and functions, including search engine and algorithmic manipulation, LLM grooming, exploitation of data voids, and information saturation tactics. Some of the sources highlighted evidence for automation and fake accounts, and other coordinated inauthentic activity. Other sources highlighted evidence for tactics that obscure the provenance of information, including astroturfing, inauthentic websites, the use of proxies, information laundering, and synthetic or false personas.

Marketing manipulation, involving attempts to shape electoral outcomes through illicit or opaque funding or manipulation of advertising. According to the literature, there is emerging evidence that AI is starting to feature in elections, in terms of voter targeting and campaign planning. Some of the sources highlighted other techniques that include the use of influencers and endorsements while inauthentic advertising, 'dark PR', and information laundering have also been observed. These might be used to circumvent restrictions on election campaign spending limits.

Participant manipulation, including aims to change participation in elections rather than beliefs. The evidence surfaced in this review mostly concerned interference with voters, or with election candidates or officials. Some sources highlight that there is evidence that voters can be affected by narratives aimed to suppress their activity, and emerging evidence that LLMs can be politically persuasive. The literature also discusses cognitive warfare in the context of elections, where the suspected aim is less to influence voter choice, and more to induce disengagement from the democratic process. According to the literature, there is evidence that participants in elections can be subject to the actions of 'trolls' and harassment, with women being especially targeted. In the context of the literature, deepfakes, including non-consensual intimate image abuse (NCII), can also be used to intimidate or otherwise interfere with participation. Other threats that were identified in the review include doxxing and SLAPPs.

All findings in this document should be contextualised in the scope of this review, the limitations highlighted in the methodology section, and the gaps in evidence. The review also reflects literature examined, so may not reflect evidence of emerging risks or those where there is less available literature.

Introduction

This literature review aims to provide an overview of literature examining online information-based threats to elections. It will inform the work of the Online Information Advisory Committee ('the Committee'), as well as others to whom it may be of interest. The Committee's function is set out by the Online Safety Act.

The Committee requested that the literature review focus on information-based threats to elections and cover the following topics:

- a) What tactics, techniques and procedures relating to information-based threats to elections have been examined by relevant literature?¹
- b) What is a useful taxonomy to present these tactics, techniques and procedures?

To address these topics, we have structured the literature review into three overarching sections:

- a) Introduction, including scope, methodology, and limitations.
- b) Taxonomy & literature review, split into four categories with key findings from the review.
- c) Other themes identified in the literature review and cross-cutting points based on it.

The review does not offer a comprehensive assessment of all information-based threats to elections, an independent assessment of their impact, or whether they can accurately be described as a threat. Much of this is contested within the large body of existing literature itself. Some of these might amount to protected speech, and might not even be considered harmful by themselves. Instead, the review summarises identified relevant literature and should be considered in this context. The literature examined points to four broad categories of threat: information manipulation, ecosystem manipulation, marketing manipulation, and participant manipulation. These categories are intended as a practical organising framework rather than a hierarchy of risk, because the evidence base varies in depth, quality and proximity to the UK election context.

Methodology

In carrying out this review, the Committee requested that we give consideration to:

- a) Where possible, a focus on literature reporting on intentionally deceptive or abusive behaviours that could pose an online information-based threat which are relevant to the Committee's questions, and not simply 'mistakes'.² This includes disinformation which can be defined as information that is false and deliberately created to harm a person, social group, organisation or country. This largely excludes most misinformation, which

¹ 'Tactics, techniques and procedures' is language often used by organisations working to identify and respond to 'foreign information manipulation and interference'. In the context of 'foreign information manipulation and interference', the European External Action Service defines them as 'patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. "Tactics" are the operational goals that threat actors are trying to accomplish. "Techniques" are actions through which they try to accomplish them. "Procedures" are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.' European External Action Service, 2026. [4th EEAS Report on Foreign Information Manipulation and Interference Threats](#). We have used this framing to organise information in this review, though not all come from a 'threat actor'.

² Further information on this can be found in the scope section.

can be defined as information that is false, but not created with the intention of causing harm, although some studies related to misinformation may be included when especially pertinent to the research focus.³

- b) Include harms that are relevant to a UK election context, for example by examining literature that has focussed on the UK or other countries with a similar Parliamentary model and/or similar limits on campaign expenditure.
- c) The current relevance of harms examined, by focussing on literature examining the past five years including where these may occur in future elections.
- d) Where possible, a focus on literature that examines more than one online service to increase the breadth and applicability of any findings.

Scope

Initial scoping showed that there is a large body of research that is potentially relevant to this review.⁴ To answer the Committee's questions with its methodological considerations in mind, and to deliver the review in a timely manner, we further focussed the literature review to largely exclude certain types of literature listed below. We made exceptions where they may be the only example in the literature and were relevant to the review.

- Misinformation, in which there is no apparent intent for deception or abuse. This might include mistakes or bias. However, the key in distinguishing between disinformation and misinformation is the intent of the user. Intentional falsehoods are considered disinformation while unintentional falsehoods are considered misinformation. Identifying whether falsehoods are intentional is difficult and sometimes impossible. Therefore, some studies related to misinformation may be included when especially pertinent to the research focus.⁵
- Disinformation or malinformation⁶ that does not directly relate to elections or democracy.
- Behaviours or media that would likely be out of scope of the work of the Online Information Advisory Committee, for example activity without an online element.
- Studies of countries that do not have a comparable parliamentary system to the UK or that do not have broadly comparable campaign spending limits.
- Studies of financing, regulation, or discussing the legality of foreign interference.
- Studies of the psychological processes exploited for information disorder.
- Studies of public or individual susceptibility to information disorder.
- Studies of mitigations and responses to information disorder.

Searching for relevant literature

To conduct a thorough and focussed literature review, the review used a structured search strategy that focussed on results that were in the English language and accessible for the purpose of this

³ Definitions derived from Wardle & Derekshsan, 2017. [Information Disorder](#).

⁴ For a discussion on one area that has relevance related to misinformation and disinformation, see Scantamburlo & Zollo, 2026. [A Scoping Review of Misinformation Research: Definitions, Conceptualizations, and Measurement Approaches](#).

⁵ Definitions derived from Wardle & Derekshsan, 2017. [Information Disorder](#).

⁶ First Draft (Claire Wardle), 2020. [Understanding Information disorder](#). Malinformation can be defined as 'genuine information that is shared with an intent to cause harm'

review. It began with Boolean queries on Google Scholar filtered to only include sources from 2019 onwards, so as to focus on the most recent research. Supplementary research included:

- Searching with general web search tools (Google, and DuckDuckGo) using query terms similar to the main Boolean query.
- Searching with Google Scholar and general web search for specific deceptive or abusive behaviours.
- Reviewing the research repositories of relevant NGOs, journals, and research labs.
- Following relevant citations in reviewed documents.

Sources returned from the searches were filtered and prioritised as set out in the Annex.

All papers and websites were accessed in April and May 2026. LLMs were not used significantly in the production of this report although initial queries were used to generate a longlist of deceptive or abusive behaviours to further inform the search terminology.

Limitations

In carrying out the review, we identified several research gaps and challenges which contributed the limitations of this literature review. These include that:

- Definitions of terminology are inconsistent across the literature examined. In particular, the definitions of misinformation and disinformation are contested and used differently in different contexts.
- Some information-based threats to elections are not in scope of this review, such as where they occur offline.⁷
- Only studies in English were included, excluding other research likely to be of value. Some potentially valuable papers were not open access and so could not be fully considered.
- The review focussed on identifying a breadth of information-based threats rather than depth on each kind. These are illustrated in this review by examples, and this may not give a direct sense of prevalence or representativeness.
- It is difficult to assess the extent of impact of different techniques and threats, and most studies did not attempt to do so. The review did not identify much longitudinal evidence which examines threats and their effects over time. It also found limited evidence on the direct effects of online information-based threats on voting or other behaviours. The dynamic two-way interaction between individuals and information, and its causal effect on belief formation and behaviour, is poorly understood and remains under-studied. This means this review cannot robustly produce a hierarchy of threats. Some of the literature examined self-reported experiences of harms which we have included.
- This is a fast-moving area of research, with multiple new studies being published even as this work was being completed. Many of these relate to elections that occurred around the world from 2024 to 2026 for which academic research is still being conducted and published. Analysis on these elections has typically been in the form of media and anecdotal reporting rather than peer-reviewed quantitative or qualitative research. There is also chance that as yet unpublished research on those elections may alter the picture.

⁷ Offline threats can also be significant in nature, for example over one third of harassment incidents documented in the lead up to Irish elections in 2024 included both an on- and offline element. Institute for Strategic Dialogue, 2024. [Political violence, harassment, intimidation & threats during Ireland's 2024 general election campaign](#).

- There were some data source challenges in the review, as described in a recent European Commission Joint Research Centre study:⁸ Researchers often find it difficult to access data from online services, some are concerned that collaborations or funding arrangements may lead to undue industry influence, and historically, certain services have provided greater data access potentially skewing our understanding of how harms manifest online as they only represent a portion of all online content. Ofcom has documented and discussed some of these concerns in its Researchers' access to information from regulated services report, laid in Parliament in July 2025.⁹
- In focussing on creating a taxonomy, we have not considered the role of different actors behind them. Some of the literature examined risks through the lens of particular actors, such as risks of foreign interference, though it can be argued that many risks can emerge from any actor with sufficient knowledge.
- There is limited research on private messaging and communication services online, which users may engage with and trust in different ways than other service types. There may be potential for influence here which is not captured in more commonly researched areas like social media services.

⁸ Scharfbillig et al, European Commission Joint Research Centre, 2026. [Fractured Reality: How democracy can win the global struggle over the information space](#).

⁹ Ofcom, 2025. [Researchers' access to information from regulated services](#). Section 5, Barriers to sharing information.

Taxonomy and literature review

A taxonomy of online information-based threats to elections

We have organised the examined literature into a taxonomy that describes information-based threats that may be relevant to the scope of this review (Table 1). The limitations set out in the previous section should be considered when reading the taxonomy.

This part of the document is structured into three main sections:

- The taxonomy of online information-based threats to elections in short, table form. All information in the taxonomy is drawn from literature in later sections.
- Deeper dives into the literature on the four categories of online information-based threats¹⁰: information manipulation, ecosystem manipulation, marketing manipulation, and participant manipulation. For each category, there are techniques setting out how this can manifest and examples surfaced in the literature review.
- Additional information surfaced in the literature review that does not map neatly onto the taxonomy. This includes research and studies that suggested additional information-based threats but lacked evidence; report on experiences of online information; and question the claims made in other research, in particular on the impact of information-based threats.

Table 1: Literature-derived categorisation of information threats

Category	Technique	Examples
Information manipulation	Fabricating or manipulating specific content	The use of inauthentic content to spread disinformation
		The use of misleading claims to spread disinformation
		The use of deepfakes to impersonate people such as politicians and voters
		The use of manipulated statistics such as misleading crime data
		The manipulation of opinion polls and fake survey platforms
		The use of false or misleading information to attempt to undermine confidence in electoral processes such as vote counting or trust in elections more broadly

¹⁰ There are many other taxonomies for information threats. For example, see Enestrom et al, 2024. [Proposing a practical taxonomy of misinformation for intervention design](#); James Pamment, Carnegie Endowment for International Peace, 2020. [The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework](#); DISARM Foundation. [DISARM Red Framework](#); Terp & Breuer, 2022. [DISARM: a Framework for Analysis of Disinformation Campaigns](#).

Category	Technique	Examples
	Manipulating the conditions in which fabricated or manipulated content circulates	Setting the agenda through narratives to shape what audiences think about
		The use of discourse to delegitimise the media
		The use of conspiracy theories to influence perceptions
		The use of polarising language to amplify difference, increase message receptivity and drive engagement
		The use of covert incitement, such as dog whistle tactics, which use subtle messages or dysphemism which do not breach laws of service guidelines
		The use of affective mobilisation / 'rage bait', to provoke maximum outrage and engagement
Ecosystem manipulation	Manipulating platform affordances	The use of search engine and algorithmic manipulation to amplify information threats
		Attempting to 'poison' ¹¹ LLMs to influence data outputs
		Attempting to exploit data voids to fill them with false narratives before accurate information is available
		Information (over)saturation used to obscure critical narratives
		Exploiting echo chambers to reinforce opinions
	Obscuring provenance	Astroturfing to disguise content provenance and falsely portray spontaneous, organic support for a view or individual
		The use of inauthentic websites to amplify information threats and make them appear more credible
		The use of proxies to complicate provenance and attribution, increase reach to diverse audiences and help overcome cultural and linguistic barriers
		The use of information laundering to mask the provenance and to influence how it spreads and how it is received by audiences
		The use of automation and fake accounts, such as to impersonate high-profile individuals or amplify engagement
		The use of synthetic accounts to spread disinformation

¹¹ The term 'poison' is set out in more detail on pages 12 and 19.

Category	Technique	Examples
	Technical disruption	The use of hacking and ransomware to disrupt communications and create public confusion
Marketing manipulation	Increasing reach	The use of microtargeting to influence and mobilise groups with tailored narratives
		The use of influencers and endorsements to disseminate disinformation to their networks
	Circumventing restrictions	The use of inauthentic advertising to drive engagement while obscuring provenance
		The use of 'dark PR' to promote narratives without disclosing the source of the funds
Participant manipulation	Voter interference	The use of attempted voter suppression to demobilise, discourage or prevent specific segments of the population from voting
		The use of automated persuasion to affect candidate preference or to persuade on a variety of political issues
		The use of cognitive warfare to disrupt, delay, or distort an opponent's cognitive process while protecting one's own
	Participant interference	The use of trolls to provoke or disrupt participants
		The use of harassment to undermine civic participation by intimidating and silencing people
		The use of gendered disinformation to deter women from participating in the public sphere
		The use of deepfakes to impersonate people, such as a newsreader
		The use of lawfare / Strategic Lawsuits Against Public Participation (SLAPPs) to deter vital democratic participation
		The use of doxxing to disrupt political processes, violate privacy and self-determination, and manipulate the opinions of citizens

Examination of relevant literature

Category 1: Information manipulation

The first category in this literature review is information manipulation, which involves attempts to shape perceptions, narratives, or understanding of online content. This section contains the three techniques listed below, with several examples of how this manifested in the literature for each. Though we have separated these into three techniques, there is overlap between them.

1. Fabricating or altering content.
2. Shaping narratives.
3. Delegitimising elections.

Fabricating or altering content

Numerous cases illustrate the use of fabricated or altered information during and around elections. The following are examples that include the promotion of false or misleading claims, the impersonation of journalists and real people, and the use of fabricated personas.

Evidence examined suggests that electoral disinformation can be shaped both by the types of content circulated and by the actors who disseminate it. One study of the 2024 European Parliament elections found that false and decontextualised content was the predominant form of electoral disinformation.¹² According to Lewandowsky, people may share forms of misinformation even when they know it to be false, in a phenomenon referred to as ‘participatory propaganda’.¹³

The literature examined found that misleading claims can also be common including from political parties. For example, one study used content that had been checked by fact checking organisations to identify that ‘political actors in various countries also contribute’ to the dissemination of false information.¹⁴

The manipulation of statistics has been reported both during and outside elections from a range of actors. One researcher stated that there are many examples of state-sponsored disinformation campaigns using statistics to manipulate and undermine the other side. They also stated that even in the UK, ‘we see abuses, misuses and blunt manipulation using statistics by officials’.¹⁵ For example, The Guardian reported that the UK Statistics Authority had reprimanded the Home Office for using ‘misleading’ statistics in a Home Office press release. In the press release it claimed that crime had reduced by 14% between September 2019 and September 2021 while excluding the fastest-growing category of crime (fraud and computer misuse) ‘to give a positive picture of trends in crime’ according to the head of the UK Statistics Authority.¹⁶

Along with the manipulation of statistics, some literature highlighted the manipulation of opinion polls and fake survey platforms. According to one study, the threat to online survey research is increasing because autonomous AI agents can evade current detection methods and produce high-

¹² Casero-Ripolles et al, 2025. [Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections](#).

¹³ Lewandowsky, 2022. [Fake news and participatory propaganda](#).

¹⁴ Cazzamatta, 2024. [Global misinformation trends: Commonalities and differences in topics, sources of falsehoods, and deception strategies across eight countries](#).

¹⁵ As described in Farouk-Radwan & Lugo-Ocando, 2024. [Statistics and state-sponsored disinformation: understanding the propaganda war on numbers](#).

¹⁶ The Guardian, 2022. [Johnson and Patel’s claims about falling crime ‘misleading’, says UK watchdog](#).

quality survey responses that would appear as though generated by a human.¹⁷ No evidence for this occurring was found in this review. One report by FIMI-ISAC observed websites in the 2025 Moldovan election that appeared to be fake survey platforms, imitating Pro-European party PAS branding while disseminated polarising questionnaires tied to a Russian charity, the Promotion of Social Projects.¹⁸

The impersonation of news outlets was observed in the 2024 UK General Election. For example, one source stated that a disinformation network generated inauthentic and impersonated news sources which combined fabricated articles with real news stories re-written to include ‘pro-Kremlin’ narratives.¹⁹ A second source found that another Russia-connected network, ‘Pravda’, was reported to have disseminated inflammatory fake content in Scotland, in Gaelic, potentially to try to stoke discontent between the speakers and non-speakers of the language in the UK, as has been observed in other countries. The source stated that such content is likely to circulate undetected for longer periods as due to only being spoken by a relatively small population, and which may not be widely spoken at media outlets and fact-checking organisations.²⁰ According to a 2026 study, the Pravda network was ‘almost certainly intended to shape the responses of certain large language models’, sometimes referred to as ‘AI poisoning’.²¹

A pre-print study also highlighted the potential for LLMs to assist in the writing of political opinions that can make users seem ‘more opinionated, competent, and positive’. This ‘carries implications for public discourse, trust, and democratic deliberation that scale with AI adoption’.²²

Several sources stated that false claims can manifest in the forms of deepfakes in elections. For example, in the run up to the 2026 UK local elections, Full Fact concluded that ‘AI imagery is no longer a hypothetical factor in UK elections—it’s being used, and in increasingly complicated, sometimes surprising ways’, including fake videos of voters stating their intentions, fake videos of meetings and rallies, and alterations to images of real events.²³ In another source, Rapid Response Mechanism Canada reported on the ‘Spamouflage’ campaign which shared deepfakes on social media, accusing Canadian officials of ‘criminal and ethical violations, including ‘corruption’, ‘sexual scandals’, and ‘election bribery’.²⁴

Other sources have reported on deepfakes in elections though have highlighted the challenges in drawing a causal link between individual instances of them and an overall electoral outcome. One study described how, in the last days of campaigning for the 2023 Slovak election, an audio clip appeared to show a leading politician discussing electoral fraud.²⁵ It continued to describe how his main rival, a Pro-Russia candidate, won the election. However, the study considered it reductive to suggest the election was swung by a deepfake because of the ‘complex social, cultural, and political dynamics’ at play. Another study identified 16 confirmed viral cases of deepfake disinformation

¹⁷ Westwood, 2025. [The potential existential threat of large language models to online survey research](#).

¹⁸ Foreign Information Manipulation and Interference (FIMI) - Information Sharing and Analysis Centre (ISAC), 2026. [Election Report: Assessment of FIMI in the 2025 Moldovan Parliamentary Election](#).

¹⁹ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections](#).

²⁰ Disinformation Social Media Alliance, 2025. [Russian Exploitation of Gaelic Language and Artificial Intelligence to Disseminate Disinformation in Scotland](#).

²¹ Digital Forensics Research Lab, 2026. [Pravda in the pipeline: Early evidence of state-adjacent propaganda in AI training data](#).

²² Röttger et al, 2026. [Measuring and Mitigating Persona Distortions from AI Writing Assistance](#).

²³ Full Fact, 2026. [From AI videos to dodgy bar charts: what we learned from the 2026 elections](#).

²⁴ Government of Canada, 2025. [Canada targeted in a new Chinese transnational repression campaign linked to ‘Spamouflage’](#).

²⁵ de Nadal & Jancarik, 2024. [Beyond the deepfake hype: AI, democracy, and “the Slovak case”](#).

during the 2024 UK General Election, and 11 viral cases in the 2024 EU and French elections combined. It found no evidence that deepfakes meaningfully impacted UK or European election results.²⁶

False claims might also use temporal deception to create the perception that events from one period in time happened at another. For example, the BBC reported that false claims were made that a video of crowds at an anti-Trump protest in October 2025 was actually from 2017, alleging protestors were misleading the public about the size of the demonstrations.²⁷

Other literature described the use of true information in a decontextualised manner. One report described this as instances where people may 'stay close to reality and simply change some interpretations to strategically alter the meaning of information'.²⁸ Another source, this can be 'hard to identify because it is closer to half-truths, decontextualised true information, or skewed interpretations mingled with truths'.²⁹ For example, a study of the 2022 Colombian elections detected a significant presence of decontextualised information, where truthful facts were taken out of context and distorted by mixing with falsehoods.³⁰

Research shows that this is further complicated when AI-manipulated content might be used for purposes that are not intended to disinform, for example to edit images, show hypothetical situations, or translate content into other languages.³¹ For example, according to Pawelec and Labuz, a 'soft fake' is content that has been doctored by campaign teams to make a candidate look more appealing and for self-promotion. Yet such 'soft fakes' can blur the lines of what might be considered authentic and 'their structural impact on citizens' empowered inclusion in political processes, the integrity of the information space, public deliberation, and political accountability remains problematic'.³²

Large Language Models (LLMs), generative AI models that can generate text, can also be used to create election disinformation. One study tested LLMs released since 2022 to assess whether they could produce election disinformation that was deemed authentic by humans. In this study electoral disinformation included voter ID disinformation, disinformation about a voting location changing time or date and the political activity of MPs. This study found almost all of the LLMs assessed could be used to produce election disinformation content deemed authentic by human evaluators over 50% of the time, even in hyper-localised UK contexts.³³

Another study showed that, among the content examined that had been verified as false by 52 European fact-checking organisations about the campaign for the European elections in 20 EU countries, there appeared to be limited and underdeveloped incorporation of AI into disinformation.

²⁶ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections](#).

²⁷ BBC, 2025. [Debunking claims US 'No Kings' crowd video is old footage](#).

²⁸ Hamaleers, 2023. [Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination](#).

²⁹ Echevarria et al, 2024. [State-Sponsored Disinformation Around the Globe](#).

³⁰ Gutiérrez-Coba & Rodríguez-Pérez, 2023. [Post-truth strategies and disinformation in the 2022 Colombian presidential elections](#).

³¹ For example, The Guardian, 2026. [The slopagenda era: 10 AI images posted by the White House – and what they teach us](#).

³² Pawelec & Labuz, 2026. [Are Soft fakes Really "Soft"? Semantic, Ethical, and Legal Perspectives on Deepfakes and AI-generated Visualizations in Political Campaigning](#).

³³ Williams et al, 2025. [Large language models can consistently generate high-quality content for election disinformation operations](#).

The study acknowledged that this could be indicative of low current detection and verification capacity.³⁴

One source highlighted the concept of a liar's dividend, referring to instances where 'politicians and other public figures...leverage an environment of misinformation and distrust to their benefit by falsely claiming that damaging true information about themselves (e.g., a scandal) is fake'. Experiments by Schiff et al., with 15,000 Americans found invoking uncertainty about information in response to a scandal can raise political support, and be a more effective response than staying silent or apologising.³⁵

Manipulating the conditions in which fabricated or manipulated content circulates

Besides altering or fabricating specific pieces of information, some studies examined the potential for false and misleading information to influence the broader agenda in an election with the aim of shaping wider public discourse.

One study reported that vulnerable communities have been found to be most at risk in this context.³⁶ Agenda setting can include discourse about the legitimacy of media. A 2020 study of over 50,000 pieces of content on two online services by politicians in Austria, Germany, and the Netherlands, found discourses that refer to misinformation or disinformation are more likely to be expressed by the so-called radical right than mainstream politicians.³⁷ It also found that disinformation becomes more visible in election times.

Several studies examined highlighted efforts to delegitimise elections through attempts to undermine public trust in the integrity of election processes and outcomes and that this can occur before, during and after an election period. One study found that in the run-up to the 2026 Bulgarian parliamentary elections, the information space was 'systematically shaped to pre-emptively delegitimise the electoral process and public institutions'. For example, attempting to erode trust in the political system before people vote. The study also found that three information operations gained over 340 million impressions across coordinated media and social networks.³⁸ The expected objective was not to convince voters of a specific narrative, but to erode trust in the system before voting took place. Moreover, legitimate state actions (anti-corruption and electoral law enforcement, human and voter rights protection, and counter-disinformation intelligence operations) were systematically reframed as evidence of anti-democratic manipulation.

Delegitimation narratives can also have an effect after an election. For example, analysis of surveys from multiple democracies suggests citizens who voted for the losing camp are more likely to view the electoral process as unfair than citizens who voted for the winners, resulting in political distrust.³⁹ A survey study of around 5,000 US voters also found those who voted for the losing candidate were more conspiratorial after the election than before.⁴⁰ However, one study of 8,500

³⁴ Casero-Ripolles et al, 2025. [Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections](#).

³⁵ Schiff et al, 2024. [The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability?](#)

³⁶ Yeoman & Morris, 2022. [The Agenda-Setting Power of Fake News](#).

³⁷ Hamaleers & Minihold, 2020. [Constructing Discourses on \(Un\)truthfulness: Attributions of Reality, Misinformation, and Disinformation by Politicians in a Comparative Social Media Setting](#).

³⁸ Trifonova & Malinov, Centre for Study of Democracy, 2026. [Cognitive Shaping and Electoral Delegitimation](#).

³⁹ Mauk, 2020. [Electoral integrity matters: how electoral process conditions the relationship between political losing and political trust](#).

⁴⁰ Miller et al, 2025. [Losers' Conspiracy: Elections and Conspiracism](#).

Americans in the 2022 US midterm elections found that official messaging about trust in elections can be ‘strongly effective at increasing trust in their own state elections’.⁴¹

According to research by Mauk and Grömping, drawing on data from 82 elections, and more than 80,000 respondents in 74 democracies, disinformation campaigns have been associated with less accurate and more polarised beliefs about election fairness.⁴²

One review concluded that ‘disinformation has played a central role in eroding public trust in electoral institutions across various democracies’, especially ‘when false narratives are strategically deployed to undermine confidence in vote counting and result certification’.⁴³ A US survey study (n=4,283) reported exposure to claims of voter fraud reduces confidence in electoral integrity, though not support for democracy itself.⁴⁴

Accusations of the violation of fair electoral procedures have been found by one study to be among the most significant topics in recent election campaigns: electoral integrity was the most common topic of debunked false information in a study of the 2024 European Parliament elections, making up over 20% of instances overall, and over 80% in Germany.⁴⁵

The public perception of election integrity can be affected by exposure to media.⁴⁶ A study using a global survey (n>16,000) found that traditional media exposure increases the accuracy of citizen election trust evaluations, but only when media freedom is high.⁴⁷

Several reports and studies highlighted that efforts to delegitimise elections can manifest through foreign interference or foreign information manipulation and interference. Foreign interference is considered by the Rycroft Review to be ‘real and persistent’ in British politics,⁴⁸ and another study by the Council of Europe reports a sharp increase in the scale of foreign information manipulation and interference in European electoral processes at local and regional levels.⁴⁹ One study found elections were the primary targets of Russian FIMI activity, including evidence of interference in the electoral processes in Germany, Poland, Romania, Moldova, Czechia, and Côte d’Ivoire.⁵⁰ It described a playbook which involves delegitimation of political leadership months before the elections, weaponising domestic divisions during electoral campaigns, and late-stage undermining of electoral integrity, with identified FIMI threats clustering in the 6 weeks before polling day, but also extending

⁴¹ Gaudette et al, 2025. [Can Official Messaging on Trust in Elections Break Through Partisan Polarization?](#)

⁴² Mauk & Grömping, 2023. [Online Disinformation Predicts Inaccurate Beliefs About Election Fairness Among Both Winners and Loser.](#)

⁴³ Suherman et al, 2025. [Information Disorder and Electoral Integrity: The Impact of Disinformation on Elections in Developing Democracies.](#)

⁴⁴ Berlinski et al, 2021. [The Effects of Unsubstantiated Claims of Voter Fraud on Confidence in Elections.](#)

⁴⁵ Casero-Ripolles et al, 2025. [Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections.](#)

⁴⁶ Kerr et al, 2024. [The Global Crisis of Trust in Elections.](#)

⁴⁷ Hilde Coffé, 2016. [Citizens’ media use and the accuracy of their perceptions of electoral integrity.](#)

⁴⁸ Philip Rycroft, 2026. [The Rycroft Review: Report of the independent review into countering foreign financial influence and interference in UK politics.](#)

⁴⁹ Stewart Dickson, Council of Europe, 2025. [Foreign interference in electoral processes at local and regional levels.](#)

⁵⁰ European External Action Service, 2026. [4th EEAS Report on Foreign Information Manipulation and Interference Threats.](#)

long before and after.⁵¹ Others have also described an interference life cycle that goes beyond the closing of the polls.⁵²

A report on the 2025 Moldovan election found it was subject to considerable foreign interference, including ‘Russian-generated narratives designed to deepen polarization and weaken trust in democratic institutions’.⁵³ These were found to rely heavily on AI-enabled propaganda, deepfake videos, authentic news reports, and algorithmic amplification across multiple online services, a significant proportion was found to be microtargeted by region and age group.

Several studies examined in the review focussed on the role of conspiracy theories as a means of influencing perceptions about elections, cutting across the categories of content fabrication and ecosystem manipulation in this review. One survey study with around 40,000 responses from 29 European countries including the UK found engagement with conspiracy theories can pose an information threat to elections.⁵⁴ It found endorsement of conspiracy theories comes with more negative evaluations of the integrity of elections, although this varies by country and context. It also found that the link between conspiracism and perceptions that electoral integrity is low was strongest when actual electoral integrity is high, and more negligible when actual integrity is low.

Another survey of over 20,000 people from ten European countries (excluding the UK) exploring the ‘great replacement’ and COVID-19 ‘anti-vax’ conspiracies, found:⁵⁵

- ‘Believing in a political conspiracy is related to a reduced willingness to participate in elections and a higher tendency to vote for far-right parties’.
- Low satisfaction with democracy, little trust in its institutions, and strong populist sentiments are associated with an increased openness to conspiracy narratives.
- Those who subscribe to conspiracy theories are more likely to believe their voices are not heard and they have no real influence, implying perceptions of political powerlessness.

Additionally, analysis of Spanish and Turkish elections proposed that conspiracy theories influence election results by stimulating conspiracy intuitions, intensifying affective polarisation and by unintended consequences arising from efforts to debunk conspiracy theories.⁵⁶

Another source suggested that political conspiracy theories can be social tools for mobilising action, including voting.⁵⁷

Some of the literature examined discussed ‘covert incitement’, in which subtle messages or dysphemism are used that do not breach laws or violate service guidelines. In a study by Bhat and Klein of extreme right-wing use of one online service during the 2016 US presidential election, they

⁵¹ European External Action Service, 2026. [4th EEAS Report on Foreign Information Manipulation and Interference Threats](#).

⁵² Casero-Ripolles et al, 2025. [Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections](#).

⁵³ Sanda, 2025. [External interference during the electoral period in the Republic of Moldova: risks, mechanisms and democratic responses](#).

⁵⁴ Schnaudt, 2024. [Conspiracy Beliefs and Perceptions of Electoral Integrity: Cross-National Evidence from 29 Countries](#).

⁵⁵ Herold, 2024. [The impact of conspiracy belief on democratic culture: Evidence from Europe](#).

⁵⁶ Nefes & Romero-Reche, 2024. [Exploring the impacts of conspiracy theories on election dynamics in Spain and Turkey](#).

⁵⁷ Marie & Peterson, 2026. [Political conspiracy theories as tools for mobilisation and signalling](#).

described that ‘dog whistle’ tactics were primarily used both as in group identity markers and to signal hate for outgroups.⁵⁸

One review found that the use of polarising and emotional language, particularly anger, fear, hatred, and anxiety, can be used to exacerbate the conditions in which false and misleading information circulate in. While these may not inherently be a ‘threat’, they were reflected as factors that could exacerbate the risks of information-based threats. They can amplify difference, increase message receptivity and drive engagement. The review concluded that ‘such emotional appeals function as a form of soft-power persuasion—aimed at co-opting rather than coercing audiences by tapping into shared anxieties, values, or aspirations. Ultimately, emotional mobilization operates not only as a tool for engagement but also as a mechanism for reinforcing social fragmentation and facilitating the spread of disinformation and misinformation’.⁵⁹

Studies examined reported that online disinformation campaigns can also be motivated by profit rather than a particular political belief or cause, as much-viewed content can earn advertising revenue from online services.⁶⁰ Research shows that some are deliberately crafting affective mobilisation, or ‘rage bait’: inflammatory content designed to provoke maximum outrage and engagement driving algorithmic amplification and bypassing critical evaluation by audiences. For example, a source found one Sri Lankan man profited from targeting anti-immigration content at UK audiences,⁶¹ and ‘a devout Muslim man living in Pakistan’ profited from spreading Islamophobic content also targeted at the UK.⁶² Another source found that false information about Donald Trump being endorsed by the Pope in 2016 was generated in Macedonia by individuals motivated by profit rather than politics.⁶³

Category 2: Ecosystem manipulation

The second category described in this literature review is ecosystem manipulation. We distinguish this from the previous category by focussing on three overlapping techniques which may aim to shape discoverability, delivery, or the apparent provenance of information. There is some overlap in the technique.

1. Manipulating platform affordances.
2. Obscuring provenance.
3. Technical disruption.

Manipulating platform affordances

Several sources examined in this review reported on attempts to manipulate features and functions of online services in an election context.

One article reported that search engine and algorithmic manipulation can amplify information threats for electorally relevant queries using search engine optimisation tactics, link farms, or

⁵⁸ Bhat & Klein, 2020. [Covert Hate Speech: White Nationalists and Dog Whistle Communication on Twitter](#).

⁵⁹ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review](#).

⁶⁰ For example, Ahmad et al, 2024. [The Role of Advertisers and Platforms in Monetizing Misinformation: Descriptive and Experimental Evidence](#).

⁶¹ The Bureau of Investigative Journalism, 2025. [King of slop: How anti-migrant AI content made one Sri Lankan influencer rich](#).

⁶² The Bureau of Investigative Journalism, 2026. [The devout Muslim making a living from Islamophobic AI slop](#).

⁶³ Forest, 2022. [Digital influence mercenaries: profits and power through information warfare](#).

coordinated searches.⁶⁴ This effect was demonstrated in a study of 800,000 headlines during the 2020 US election period.⁶⁵ In another example, a network of low-quality websites was found to generate millions of links to artificially boost ‘pro-Kremlin pseudo-think tanks’.⁶⁶ A source reported that some disinformation was intended to be amplified on services by its association with other popular content and themes on online services, by hijacking trending topics and hashtags, and by ‘tricking’ algorithms into amplification.⁶⁷

The structure of online information ecosystems was also reported as posing an information threat to elections. One article stated that a combination of recommendation algorithms and network effects can lead to the formation of echo chambers or filter bubbles in which like-minded users mutually reinforce opinions without exposure to alternative perspectives, often increasing polarisation.⁶⁸ Scharfbillig et al., stated that this is considered a danger when ‘democracy itself cannot survive without some degree of shared reality’.⁶⁹ However, a 2025 literature review found conflicting evidence about the existence and effects of echo chambers, with results found to be linked to the research methodologies used.⁷⁰

Data voids or news gaps, where there is a lack of valid organic content for particular topics or search terms, can be exploited by those sharing false narratives before accurate information is available.⁷¹ Coravu reports that similar techniques can be used to exploit other voids because online information is volatile and mutable, and ‘prone to amnesia’; for example, disinformation actors have been observed to take over expired domains or URLs previously cited by credible sources.⁷²

One literature review reported that fake accounts and bots can be used to engage in information saturation, a technique in which ‘excessive, irrelevant or misleading content’ saturates the public sphere ‘to obscure critical narratives and divert attention from contentious issues’.⁷³ One study found that it can prevent the identification of reliable information, and induce public fatigue, cynicism, and ultimately disengagement from democratic processes.⁷⁴ Another study estimated that the volume of online content has risen 20% annually for the past 5 years and this is expected to accelerate as generative AI makes content creation simpler, concluding that ‘whatever harms may affect democracy, scarcity of information is not one of them’.⁷⁵

⁶⁴ Bradshaw, 2019. [Disinformation optimised: gaming search engine algorithms to amplify junk news.](#)

⁶⁵ Zade et al, 2022. [Auditing Google's Search Headlines as a Potential Gateway to Misleading Content: Evidence from the 2020 US Election.](#)

⁶⁶ Williams & Carley, 2023. [Search engine manipulation to spread pro-Kremlin propaganda.](#)

⁶⁷ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review.](#)

⁶⁸ Nguyen, 2018. [Echo chambers and epistemic bubbles.](#)

⁶⁹ Scharfbillig et al, European Commission Joint Research Centre, 2026. [Fractured Reality: How democracy can win the global struggle over the information space.](#)

⁷⁰ Hartmann et al, 2025. [A systematic review of echo chamber research: comparative analysis of conceptualizations, operationalizations, and varying outcomes.](#)

⁷¹ Golebiewski & Boyd, Data & Society, 2019. [Data voids: Where Missing Data Can Easily Be Exploited.](#)

⁷² Coravu, 2024. [Fragile Reference, Faked Authority, and the Advance of Counterknowledge.](#)

⁷³ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review.](#)

⁷⁴ Szegofi et al, 2026. [“Flooding” using disinformation.](#)

⁷⁵ Scharfbillig et al, European Commission Joint Research Centre, 2026. [Fractured Reality: How democracy can win the global struggle over the information space.](#)

LLM chatbots and AI overviews are becoming increasingly important sources of information.⁷⁶ Despite this, a survey (n=1,461) before the 2024 German European elections found limited use of AI for news, even though many had experimented with it for other purposes. Notably, the survey found that individuals with a lower sense of duty about staying informed, who usually have a lower tendency for news consumption, were more likely to turn to AI for news.⁷⁷

Some sources examined reported on misleading information from chatbots. For example, a 2025 study of ten of the leading chatbots found rates of false information increased from 18% of answers in August 2024 to 35% a year later.⁷⁸ A 2026 BBC investigation, in the context of the 2026 Welsh Senedd election, ‘found that some [chatbots] gave misleading information – including inaccurate policy details, incorrect constituencies and candidates who will not appear on the real ballot paper’.⁷⁹

According to Fendley et al, LLMs can be subject to poison attacks, in which a model’s training data is manipulated to influence its outputs.⁸⁰ Research by Disinformation Social Media Alliance shows that one type of poison attack, referred to as LLM grooming, involves saturating the internet with specific narratives in an effort to increase the likelihood that LLMs echo those narratives, and this may be a potential effect of the volume of content produced by the ‘pro-Kremlin’ Pravda network.⁸¹ According to the American Sunlight Project, in many cases this content, with unique URLs, is extremely low quality or unusable by humans, since the intended audience is search engine crawlers and LLM training.⁸² One study found popular LLMs may repeat ‘Russian disinformation narratives’ about Ukraine, although there is substantial variation and ‘less than half of chatbot responses mention the Russian perspective on war-related issues’.⁸³ while another assessment did not find evidence of ‘consistent recapitulation of Russian propaganda by LLMs’.⁸⁴

Obscuring provenance

Several studies examined in this review highlighted attempts to obscure the identity or original source of online content around elections.

Studies examined in this review highlighted how online fake accounts or ‘sock puppets’, often using automated bots, can be used through coordinated activity, spreading content at scale, amplifying content with false engagement, or giving profiles the impression of popularity. Research examined observed consistent, statistical associations between the spread of low-quality sources, disinformation, and coordinated activity. For example, Rogers and Righetti reported that coordinated networks were found to be more likely to share news sources that had previously been

⁷⁶ Simon et al, 2025. [Generative AI and News Report 2025: How People Think About AI’s Role in Journalism and Society](#); see also, Ofcom, 2025. [The Era of Answer Engines: Generative AI’s impact on search experiences and online safety](#).

⁷⁷ Reiss et al, 2026. [Will News Find Them With Generative AI? Exploring the Affordances and Potential of GenAI for News Consumption](#).

⁷⁸ Cybernews, 2025. [Fed on falsehoods, AI chatbots generate more false information](#).

⁷⁹ BBC, 2026. [AI chatbots giving misleading voting advice in run-up to election](#).

⁸⁰ Fendley et al, 2025. [A Systematic Review of Poisoning Attacks Against Large Language Models](#).

⁸¹ Disinformation Social Media Alliance, 2025. [Disinformation Propagation via LLM Manipulation Tactics](#).

⁸² American Sunlight Project, 2025. [A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops](#).

⁸³ Makhortykh et al, 2024. [Stochastic lies: How LLM-powered chatbots deal with Russian disinformation about the war in Ukraine](#).

⁸⁴ Shapiro, CREST, 2025. [Disinformation: What did we learn from the year of elections?](#)

flagged by fact checkers during the 2019 Italian European elections, the 2020 Italian national election, and the 2021 German elections.⁸⁵

There were multiple studies reporting on the use of bots and fake accounts for disinformation, including:

- A study published in 2026 found, across seven major online services, over 30,000 inauthentic accounts, delivering over 100,000 units of inauthentic engagement.⁸⁶
- A report stating that in the run up to the 2025 German federal election, a coordinated network of 50 accounts amplified by a bot network of over 6,000 accounts, was found to have spread false claims through videos designed to look like they come from legitimate media outlets, law enforcement agencies and academics.⁸⁷
- A report stating that in the run up to the 2023 Serbian local, regional, and national elections, approximately 14,000 bots were suspected to be manipulating public discourse on social media in favour of the ruling party.⁸⁸
- Reports of a page on an online service spreading disinformation being amplified by a network of interconnected accounts leading to an inauthentic appearance of extreme popularity.⁸⁹

One report also stated that there is an active market for buying online accounts which bypasses the slow process of authentic audience-building and is used to promote disinformation into existing follower networks.⁹⁰ According to Dawson and Innes, this technique may have been employed, for example, by Russia's Internet Research Agency to promote Russia's agenda against Germany and the UK's EU referendum.⁹¹

Inauthentic websites, which might masquerade as established media, can be used to both amplify information threats, and make them appear more credible.⁹² For example, the Foreign Affairs Committee reported that a Russian network of campaigns, referred to as Doppelgänger, has been reported to frequently imitate legitimate media organisations while 'promoting Russian narratives'.⁹³ The UK's Foreign, Commonwealth & Development Office has attributed the use of impersonated trusted media outlets and cloned websites by the Doppelgänger network to the Social Design Agency which 'is tasked and funded directly by the Russian state'.⁹⁴ There are reports that another operation, Storm-1516, attempted to influence Germany's 2025 elections with more than 100 fake websites which used false content to target political figures.⁹⁵ According to Murray et al., there are also reports that Storm-1516 ran a coordinated influence operation during the 2026

⁸⁵ Rogers & Righetti, 2025. [Coordinated inauthentic behaviour on Facebook? A typology of manufactured attention.](#)

⁸⁶ Bergmanis-Korats et al, NATO, 2026. [Social Media Manipulation for Sale.](#)

⁸⁷ Institute for Strategic Dialogue, 2025. [Coordinated disinformation network uses AI, media impersonation to target German election.](#)

⁸⁸ Dickson, Council of Europe, 2025. [Foreign interference in electoral processes at local and regional levels.](#)

⁸⁹ Debunk.org, 2023. [Bot accounts spread the vision of the "Russian World" on social media platforms.](#)

⁹⁰ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review.](#)

⁹¹ Dawson & Innes, 2019. [How Russia's Internet Research Agency Built its Disinformation Campaign.](#)

⁹² Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review.](#)

⁹³ Foreign Affairs Committee, 2026. [Disinformation diplomacy: How malign actors are seeking to undermine democracy.](#)

⁹⁴ FCDO, 2026. [UK action against Russian foreign information warfare.](#)

⁹⁵ Slerka, Vsquare, 2025. [Hacking Democracy: Russia's Digital War on German and European Elections.](#)

Hungary election, leveraging a network of inauthentic social media accounts, fabricated media outlets, commercial marketing accounts, and influencer accounts to disseminate fabricated narratives, amplify political attacks, and undermine trust in Hungarian opposition leader Péter Magyar and the TISZA party.⁹⁶ Another source found a network of sites was reported to have mixed Russian talking points with true and false specific local social concerns and controversies, targeting content at specific subsets of the US population.⁹⁷

According to Tiilikainen, the use of domestic proxies is ‘a commonplace tool for exerting expert and referent power’.⁹⁸ A study by Sikorski has observed them to be a key component of Russian influence operations in Central Europe, functioning within an ecosystem of official state channels and an extensive network of shell institutions and intermediaries including think tanks, quasi-news agencies, and simple blogs.⁹⁹ The study describes dense networks that complicate provenance and attribution, increase reach to diverse audiences, and help overcome cultural and linguistic barriers.

Other parts of the literature examined described these tactics as forms of ‘information laundering’, which mask the provenance of information and may influence how it spreads and how it is received by audiences. One article reported on the use of ‘pseudo think tanks’, defined as ‘organisations that present themselves as independent and research-driven, but whose primary purpose is to advance a particular agenda, often that of their funders’.¹⁰⁰ Another report focussed on ‘black knight NGOs’, described as ‘organisations that generate and disseminate content that aims to undermine the legitimacy of multilateral organisations, cast doubt on state institutions in Western democracies, or support the rhetoric of authoritarian states’.¹⁰¹ A review by The Alan Turing Institute stated that private messaging networks ‘can act as a ‘laundering point’ between foreign and domestic threat actors’.¹⁰²

Information laundering may also be an inadvertent consequence of circular reporting. For example, the Foreign Affairs Committee stated that Russian-sourced disinformation on bedbugs in France, suggesting that false claims can get wider coverage once they have been sufficiently amplified.¹⁰³

One review highlighted that inauthentic websites, proxies, astroturfing, information laundering, alongside echo chamber effects, can combine to create closed media ecosystems that ‘appear credible and community-driven while in fact systematically excluding dissent’.¹⁰⁴

One source highlighted that bots and fake accounts can also be used for astroturfing, the practice of disguising the source of content to give the impression that it originated spontaneously and

⁹⁶ Murray et al, 2026. [Hungary for more? Russian Storm-1516 narratives and engagement tactics targeting Hungary’s 2026 parliamentary election](#). The UK Government has described Storm-1516 as ‘a Russian FIMI network’ which ‘produces content that seeks to undermine European unity and create support for Russia’s illegal war in Ukraine’. Foreign, Commonwealth & Development Office, 2026. [UK action against Russian foreign information warfare](#).

⁹⁷ Chatterje-Doody, 2024. [Five disinformation tactics Russia is using to try to influence the US election](#).

⁹⁸ Tiilikainen, 2026. [Foreign Influence Operations and Their Proxies](#).

⁹⁹ Sikorski, 2025. [Proxy Sources in Cognitive Warfare: The Hidden Architecture of Russian Influence Operations in Central Europe](#).

¹⁰⁰ Mendizabal, 2025. [The art of deception: How pseudo think tanks and researchers influence policy](#).

¹⁰¹ Shyrokykh & Kragh, 2024. [Black knight NGOs and international disinformation](#).

¹⁰² Stockwell et al, The Alan Turing Institute, 2026. [Adding Fuel to the Fire: AI Information Threats and Crisis Events](#).

¹⁰³ Foreign Affairs Committee, 2026. [Disinformation diplomacy: How malign actors are seeking to undermine democracy](#).

¹⁰⁴ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review](#).

represents community concerns.¹⁰⁵ Research by The Alan Turing Institute stated that astroturfing by automated social media bots was observed in the 2024 UK and European elections.¹⁰⁶

Some of the literature examined synthetic avatars and false personas and described these as being similar to fake accounts, but distinguished by how convincingly authentic they appear to be. For example, the European Digital Media Observatory found a network of nearly 100 profiles of AI-generated personas that systematically spread content supporting the governing party in the run up to the 2026 Hungary election (a so-called sybil attack).¹⁰⁷ The Bureau of Investigative Journalism reported that a British political party paid for AI-generated political campaign content and that this was an example of a reported broader trend of AI characters endorsing political candidates.¹⁰⁸

By contrast, one study examined reported that real candidates might also be accused of being fake. For example, The Alan Turing Institute found that during the 2024 UK General Election, some media outlets claimed one candidate was AI-generated after they failed to attend voter hustings and the election count.¹⁰⁹

A study of 2025 Moldovan election found growing convergence between foreign and domestic information manipulation.¹¹⁰ AI-driven bot networks on certain online services amplified anti-government and anti-EU rhetoric, while inauthentic observer recruitment campaigns targeting the diaspora spread fabricated reports of electoral fraud. The study noted that 22 incident alerts of 'coordinated disinformation, influence operations, and hybrid interference' were documented during the election, which collectively generated 136.1 million views and 3.79 million interactions, according to platform-provided metrics. It highlighted that this far exceeded the 2.4 million population of Moldova, 'underscoring the disproportionate saturation of Moldova's digital space by foreign and domestic influence campaigns.'

Technical disruption

While not a major focus of this literature review in and of itself, a significant volume of literature identified highlighted risks related to the technical disruption of election infrastructure, including hacking and cyber-attacks. In turn, some studies examined reported that this may have some impact on trust and the availability of online information.¹¹¹

One study described how this can erode trust in the systems that underpin online interactions, creating instability and undermining confidence. Highlighted threat examples included interference with:¹¹²

- The Domain Name System (DNS), redirecting users to malicious websites disguised as legitimate ones, facilitating phishing attacks and the spread of malware.

¹⁰⁵ Definition from Caled & Silva, 2021. [Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation.](#)

¹⁰⁶ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections.](#)

¹⁰⁷ Lakmusz, European Digital Media Observatory, 2026. [Young, attractive, fans of football, Orbán and relationship drama: inside the most sophisticated pro-Fidesz fake-profile network on Facebook.](#)

¹⁰⁸ The Bureau of Investigative Journalism, 2026. [Meet the AI rapper funded by a far-right party.](#)

¹⁰⁹ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections.](#)

¹¹⁰ FIMI-ISAC, 2026. [Election Report: Assessment of FIMI in the 2025 Moldovan Parliamentary Election.](#)

¹¹¹ Dawood, 2021. [Combating Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats.](#)

¹¹² Bradshaw & de Nadis, 2024. [Technical infrastructure as a hidden terrain of disinformation.](#)

- Undersea cables and network connections, disrupting communication, isolating entire regions, or disrupting critical services.
- Public key infrastructures, undermining trust in online transactions and creating opportunities for fraud and identity theft.

One study by Sanda reported technical disruption in the 2025 Moldovan elections, where there was a surge in ransomware attacks against government websites and news portals which was traced to the GRU-linked group APT28.¹¹³ The incidents coincided with critical campaign milestones, 'suggesting a synchronised effort to disrupt communications and create public confusion'.

Even if technical disruption does not cause much physical harm, it may have an outsized psychological impact in a process termed 'perception hacking'. One article describes this as 'a relatively small-scale intrusion that probably won't cause much actual harm, yet it may have an outsized psychological impact once it's uncovered and enters the public bloodstream via government officials, news organizations and social media'. This is considered especially risky if votes are close or counting is extended.¹¹⁴

Category 3: Marketing manipulation

The third category in this literature review is marketing manipulation, describing literature reporting on efforts to shape electoral outcomes through illicit or opaque funding or manipulation of advertising. Within this, some studies included what might otherwise be legitimate techniques that were conducted without sufficient disclosure. There are two techniques covered in this section, with examples provided for each based on the literature examined.

1. Increasing reach.
2. Circumventing restrictions.

Increasing reach

The discovery process for literature in this review surfaced sources highlighting the role of political advertising. For example, one source reported that billions of dollars is spent on political advertising in the US alone.¹¹⁵ However, a study of over 60,000 users on two online services in the run up to the 2020 US presidential election found no detectable effects of removing political ads on political knowledge, polarisation, perceived legitimacy of the election, political participation (including campaign contributions), candidate favourability, or turnout.¹¹⁶

One literature review reported that digital services facilitated microtargeting, the delivery of disinformation to specific audience segments based on behavioural and demographic data; this 'allows agents of information disorder to influence and mobilise groups with tailored narratives'.¹¹⁷ However, studies examined on of the effectiveness of political microtargeting showed inconclusive results. For example, one survey experiment focusing on US policy issue advertising found a

¹¹³ Sanda, 2025. [External interference during the electoral period in the Republic of Moldova: risks, mechanisms and democratic responses](#).

¹¹⁴ Myre, NPR, 2020. [A 'Perception Hack': When Public Reaction Exceeds The Actual Hack](#).

¹¹⁵ See Brennan Center for Justice, 2024. [Online Ad Spending in 2024 Election Totaled at Least \\$1.9 Billion](#).

¹¹⁶ Allcot et al, 2025. [The Effects of Political Advertising on Facebook and Instagram before the 2020 US Election](#).

¹¹⁷ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review](#).

microtargeting strategy produced a larger persuasive impact under highly favourable conditions, but with much more limited effects in different advocacy scenarios.¹¹⁸

A report by the Foreign Affairs Committee stated that social media influencers may be paid to disseminate disinformation to their extensive networks.¹¹⁹ According to Martinescu et al., such techniques were reported to have been used in the annulled 2024 Romanian presidential election.¹²⁰ Another study found that during the 2024 European Parliament and municipal election campaigns, the ruling Hungarian party, Fidesz was reported to have spread disinformation through a pro-government political influencer network known as the Megafon Központ (Megafon Centre).¹²¹

Influencers and celebrities can affect an audience's assessment of the credibility of content, as demonstrated in experiments with social endorsements on one online service.¹²² These endorsements might be fake; for example, according to the Irish Times, the Irish Tánaiste was impersonated in a deepfake endorsement of fraudulent investment products.¹²³

Some studies indicated that artificial intelligence has begun to feature in election campaigns around the world, and that it can also influence the reach of online content.¹²⁴ It offers new tools including voter targeting, campaign planning, and content generation.¹²⁵ One study observed that China has used AI tools for 'tailored content generation, large scale monitoring, and targeting foreign audiences', although this is 'primarily to augment rather than replace existing approaches'.¹²⁶

Circumventing restrictions

One report describes how motivated actors may seek to circumvent election campaign spending limits and mask the source of funding for political ads, or route through ad networks that do not apply adequate political advertising disclosure requirements.¹²⁷

Inauthentic advertising can be used for election disinformation; for example, according to Bergmanis-Korats et al., one experiment generated 206,234 views, 200 likes, and 17,442 inauthentic comments for a total cost of €252.¹²⁸ One study found that automated ad-buying systems can place disinformation or divisive content at scale across thousands of websites, targeting audiences based on behavioural and demographic data.¹²⁹

¹¹⁸ Tappin et al, 2023. [Quantifying the potential persuasive returns to political microtargeting](#).

¹¹⁹ Foreign Affairs Committee, 2026. [Disinformation diplomacy: How malign actors are seeking to undermine democracy](#).

¹²⁰ Martinescu et al, Foreign Policy Centre, 2024. [Networks of Influence: Decoding foreign meddling in Romania's elections](#).

¹²¹ Horvath et al, 2025. [Outsourced Political Campaign: Role of Pro-Government Political Influencers in Spreading Hostile Narratives in Hungary](#).

¹²² Shin et al, 2022. [Twitter and Endorsed \(Fake\) News: The Influence of Endorsement by Strong Ties, Celebrities, and a User Majority on Credibility of Fake News During the COVID-19 Pandemic](#).

¹²³ Dooley, The Irish Times, 2026. [‘I had to watch it twice to check it wasn’t me’: Harris a victim of deepfake video scam](#).

¹²⁴ Sifry, The Nation, 2024. [How AI Is Transforming the Way Political Campaigns Work](#).

¹²⁵ Foos, 2024, [The use of AI by election campaigns](#).

¹²⁶ Hanhijärvi, European Centre of Excellence for Countering Hybrid Threats, 2026. [Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian approaches](#).

¹²⁷ Diaz Ruiz, 2025. [Disinformation and fake news as externalities of digital advertising: a close reading of sociotechnical imaginaries in programmatic advertising](#).

¹²⁸ Bergmanis-Korats et al, NATO, 2026. [Social Media Manipulation for Sale](#).

¹²⁹ Diaz Ruiz, 2025. [Disinformation and fake news as externalities of digital advertising: a close reading of sociotechnical imaginaries in programmatic advertising](#).

One book described a ‘growth industry’ of ‘disinformation actors’ using ‘dark PR’ to promote narratives without disclosing the source of funds.¹³⁰

Other approaches to obscuring provenance already discussed, such as proxies and information laundering, can also be used to circumvent restrictions.

Some online services have banned political ads at times.¹³¹ However, literature examined reported that this has not always been well enforced: after Meta’s ban, according to the European Digital Media Observatory, 457 political ads (including deepfakes) appeared in the first 6 weeks of campaigning in the 2026 Hungarian election.¹³²

Category 4: Participant manipulation

The final category in this literature review is participant manipulation, describing techniques in the literature which involve efforts to change participation in elections rather than beliefs or preferences. There are two techniques covered in this section, with examples included for each.

1. Voter interference.
2. Participant interference.

Voter interference

Voter suppression is defined as ‘a strategy that demobilises, discourages, or prevents specific segments of the population from voting’ in a study of exposure to targeted ads and voter turnout (n=13,500) in the six weeks prior to the US 2016 elections.¹³³

One study examining advertising in elections identified four types of voter suppression ads:

- ‘election boycott’ – casting doubt and dampening enthusiasm;
- ‘deception’ – misleading information about voting practicalities;
- ‘candidate promotion’; and,
- ‘candidate attack’.

The study found, on average, those exposed to voter suppression ads were less likely to turn out to vote (65.89%, compared to 67.75% turn out for those not exposed to voter suppression ads), ‘which amounts to approximately 4.7 million fewer votes nationally’.

The literature reported that several means of deception may be used in attempts to persuade voters. A study of 16 different persuasion techniques found they are tailored to different disinformation domains, with ‘doubt’, ‘loaded language’, ‘name calling-labelling’, and ‘appeal to fear-prejudice’ being the four most common.¹³⁴

Chatbots can be used for automated persuasion, as demonstrated by a meta-analysis covering 17,000 participants.¹³⁵ Several studies reported that chatbots can affect candidate preference, as

¹³⁰ Forest, 2022. [Digital influence mercenaries: profits and power through information warfare](#).

¹³¹ For example, Meta, 2025. [Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation](#).

¹³² Lakmusz, European Digital Media Observatory, 2026. [Russian disinformation campaigns against Hungarian opposition figures, 457 political ads in 6 weeks and AI-generated videos once again](#).

¹³³ Kim et al, 2026. [Targeted digital voter suppression efforts likely decrease voter turnout](#).

¹³⁴ Leite et al, 2025. [A Cross-Domain Study of the Use of Persuasion Techniques in Online Disinformation](#).

¹³⁵ Holbling et al, 2025. [A meta-analysis of the persuasive power of large language models](#).

shown in a series of experiments in the context of the 2024 US presidential election (n=2,306), a 2025 Massachusetts ballot (n=501), the 2025 Canadian federal election (n=1,530) and the 2025 Polish presidential election (n=2,118).¹³⁶ These effects were greater than those typically observed from traditional video ads. The chatbots typically persuaded with facts and evidence rather than psychological techniques, although notably not all facts and evidence were accurate.

In a more recent study of over 40,000 people, LLMs were deployed to persuade people on a wide variety of political issues to test their persuasiveness and the techniques that may influence this.¹³⁷ More persuasive LLM techniques were found to rely on a high volume of factual claims which were not always accurate. Personalising arguments on the basis of user data had a comparatively small effect on persuasion. Notwithstanding these studies, according to Simon and Altay 'it remains an open question to what extent the persuasiveness of LLMs' arguments correlates with the factual accuracy of the conclusions they advocate'.¹³⁸

Taking a different perspective on the implications of LLM use, an examination of well over a million LLM fact-checking requests indicated users had polarised and partisan attitudes towards different LLMs.¹³⁹

According to Rushing et al., cognitive warfare can be 'framed as competition to disrupt, delay, or distort an opponent's cognitive processes while protecting one's own'.¹⁴⁰ It is a research field that is growing rapidly, especially in NATO-aligned ecosystems.¹⁴¹ NATO stated that elections and the processes of democracy are one cognitive warfare battleground.¹⁴² Research shows that one approach is to attempt to overwhelm audiences and induce voter paralysis with contradictory information, false complexity, or hopelessness. This aims to suppress civic engagement and reduce likelihood of political action by creating a feeling that nothing can be known, that nothing can be done, or that voting is pointless because politicians are 'all the same'.¹⁴³ Other research by the European Commission Joint Research Centre reports that often the likely goal is not to make individuals believe false claims but to distract, generate distrust, and encourage anti-democratic norms.¹⁴⁴

Participant interference

Several studies examined in this review highlighted the effects of certain types of online content on their involvement in democratic processes. For the purposes of this review, we have termed this as 'participant interference'.

Several reports and studies focussed on harassment and intimidation. In the 2024 Irish General Election, 55 incidents of politically motivated violence, threats, harassment, targeting and smears, including explicitly racist, misogynistic and anti-Muslim slurs, were observed in the last five weeks of campaigning, and 20 candidates used threatening rhetoric against other elected politicians on online

¹³⁶ Lin et al, 2025. [Persuading voters using human-artificial intelligence dialogues.](#)

¹³⁷ Hackenburg et al, 2025. [The levers of political persuasion with conversational artificial intelligence.](#)

¹³⁸ Simon & Altay, 2025. [Don't Panic \(Yet\): Assessing the Evidence and Discourse Around Generative AI and Elections.](#)

¹³⁹ Renault et al, 2026. [Grok Is This True? LLM-Powered Fact-Checking on Social Media.](#)

¹⁴⁰ Rushing et al, 2026. [Cognitive Warfare: Definition, Framework, and Case Study.](#)

¹⁴¹ Russo & Yazdanjue, 2026. [Mapping the cognitive warfare literature: A strategic analysis.](#)

¹⁴² NATO, 2026. [Cognitive Warfare.](#)

¹⁴³ Westin et al, 2025. [Grappling with post-truth politics - facilitation strategies for policy-making in troubled times.](#)

¹⁴⁴ Scharfbillig et al, European Commission Joint Research Centre, 2026. [Fractured Reality: How democracy can win the global struggle over the information space.](#)

services.¹⁴⁵ According to the Electoral Commission, in the 2024 UK General Election, many candidates, especially women and those from ethnic minority background, ‘experienced unacceptable levels of intimidation and harassment’, and over half of candidates responding to an Electoral Commission survey said they avoided some form of campaigning because of fear of abuse.¹⁴⁶ Another report highlighted examples of AI-enabled smear campaigns in the General Election including ‘AI-generated videos, voice clones, images, and pornographic content of political candidates making false controversial statements or being depicted in fabricated activities’.¹⁴⁷ In contrast to previous research of AI misuse in recent elections globally, the report noted that the 2024 UK General Election had fewer viral smear campaigns using AI than had been predicted, ‘primarily due to a combination of the snap announcement, the short campaigning period, and relative confidence in the outcome from opinion polls – which all reduced the incentives for malicious interference’. The 2026 UK local elections occurred while this report was being prepared, and there are already emerging evidence of harassment having a deleterious effect.¹⁴⁸

One study described ‘trolls’ as ‘humans that are hired to disseminate false information and to engage with disinformation to increase the virality and prominence of dishonest information’.¹⁴⁹ Another study described trolling as dishonest, inflammatory behaviour intended to provoke and disrupt; it has been shown to significantly decrease participants’ willingness to engage in online discussions.¹⁵⁰ According to research, trolls may be involved in harassment or ‘pile on’ campaigns which aim to undermine civic participation by intimidating and silencing critics, journalists, researchers, public figures, political candidates, or those simply expressing their political views. Some studies reported on informal networks of supporters being involved in such activity and that targeted harassment can have measurably negative effects on political debate and media freedom.¹⁵¹

According to The Alan Turing Institute, politicians have been targeted with non-consensual intimate image (NCII) abuse, resulting in harm to their wellbeing and professional reputation.¹⁵² Research shows that NCII, either real or deepfake, can also be used to threaten, blackmail, silence, humiliate, undermine, or intimidate candidates.¹⁵³ This approach is much more commonly used against women.¹⁵⁴

Gendered disinformation, often with the aim of deterring women from participating in the public sphere, is particularly prominent in the literature examined. For example, an analysis of comments under videos on one service published by French, German and Hungarian candidates for the 2024 European Parliament elections, found women candidates received substantially more hateful,

¹⁴⁵ Institute for Strategic Dialogue, 2024. [Political violence, harassment, intimidation & threats during Ireland’s 2024 general election campaign](#).

¹⁴⁶ Electoral Commission, 2024. [Report on the 2024 UK Parliamentary general election and the May 2024 elections](#).

¹⁴⁷ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections](#).

¹⁴⁸ For example, Rouane-Williams, 2026. [Is online abuse driving good people out of local politics in Ipswich?](#)

¹⁴⁹ Hamaleers, 2023. [Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination](#).

¹⁵⁰ Taylor & Richey, 2026. [Trolling Democracy: How Trolls Distort Digital Discourse](#).

¹⁵¹ Ricard et al, 2025. [A Framework for Information Disorder: Modelling Mechanisms and Implications Based on a Systematic Literature Review](#). See also Nonnecke et al, 2021. [Harass, mislead, & polarize: An analysis of Twitter political bots’ tactics in targeting the immigration debate before the 2018 U.S. midterm election](#).

¹⁵² Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections](#).

¹⁵³ For example, BBC, 2024. [Giorgia Meloni: Italian PM seeks damages over deepfake porn videos](#).

¹⁵⁴ For example, The Spectator, 2024. [Deepfake porn site targets female politicians](#).

defamatory, derogatory or discriminatory comments than their male counterparts.¹⁵⁵ The Centre for Information Resilience highlighted that common gendered narratives include speculation about a woman's fitness for office, the 'motherhood conundrum', sexualisation, transphobia, and anti-feminism.¹⁵⁶ This literature review surfaced research and evidence on gendered disinformation and hate speech in politics in Malaysia,¹⁵⁷ France,¹⁵⁸ Czechia,¹⁵⁹ Italy,¹⁶⁰ and Central Europe,¹⁶¹ and we are aware of research indicating it is even more widespread.¹⁶²

In the 2025 federal election, analysis by the Government of Canada reported that most detected disinformation content did not gain significant traction or visibility among the broad Canadian public, and the election was not observed to be influenced by any significant use of generative AI by hostile state actors.¹⁶³ Even so, it found that disinformation was observed about candidates in the 2025 leadership campaign for the Liberal Party of Canada, including millions of views of disparaging articles on WeChat.¹⁶⁴ It also observed a pro-People's Republic of China 'spamouflage' campaign across certain services. This included a doxxing website and doctored videos, accusing Canadian officials of criminal and ethical violations, including corruption, sexual scandals and election bribery. It primarily targeted Chinese-speaking online commentators.¹⁶⁵

Deepfakes might also imply candidates have done or said something they have not. For example, in the Republic of Ireland, according to The Irish Times, a deepfake designed to look like a RTÉ News bulletin, including false depiction of a newsreader, falsely showed a candidate withdrawing from the presidential election.¹⁶⁶

Intimidation might also include doxxing, in which malicious actors publish or threaten to publish non-public and potentially embarrassing or compromising personally identifiable information. This can disrupt political processes, violate privacy and self-determination, and manipulate the opinions of citizens.¹⁶⁷ For example, a 2025 report described a 'Spamouflage' campaign in Canada which 'involves the operation of a 'doxxing' website'.¹⁶⁸

According to Kanellia, 'Lawfare' including strategic lawsuits against public participation (SLAPPs) may 'deter vital democratic participation: under the shadow of potential SLAPPs, individuals and media

¹⁵⁵ Institute for Strategic Dialogue, 2025. [Crushing Comments: Gendered Harassment during the 2024 EU Parliament Elections on TikTok](#).

¹⁵⁶ Centre for Information Resilience, 2024. [Holding our digital ground: Addressing gendered disinformation during elections and beyond](#).

¹⁵⁷ Tapsell & Chandraroo, 2024. [Gendered Disinformation and Election Campaigning: A Malaysia Case Study](#).

¹⁵⁸ Institute for Strategic Dialogue, 2024. [Votes and Vitriol: Online Abuse Targeting Women Candidates in the 2024 French Legislative Elections](#).

¹⁵⁹ Varekova, 2025. [The gender dimension of disinformation and hate speech in the political sphere](#).

¹⁶⁰ Sportelli & D'Errico, 2025. [Does Disinformation Toward Women Politicians Reflect Gender Stereotypes? Exploring the Role of Leaders' Political Orientations](#).

¹⁶¹ Saner et al, 2026. [Gender and identity disinformation: impacts on female politicians, and implications for democratic participation - roundtable discussion](#).

¹⁶² Ofcom, 2025. [A Safer Life Online for Women and Girls](#).

¹⁶³ Government of Canada, 2025. [Retrospective Report on the 45th General Election](#).

¹⁶⁴ Government of Canada, 2025. [Security and Intelligence Threats to Elections Task Force Reports](#).

¹⁶⁵ Government of Canada, 2025. [Canada targeted in a new Chinese transnational repression campaign linked to 'Spamouflage'](#).

¹⁶⁶ The Irish Times, 2025. [Deepfake AI video depicting Catherine Connolly quitting presidential race removed by Meta](#).

¹⁶⁷ Kilovaty, 2018. [Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information](#).

¹⁶⁸ Government of Canada, 2025. [Canada targeted in a new Chinese transnational repression campaign linked to 'Spamouflage'](#).

may self-censor'. One study stated that Europe, including the UK, has witnessed an 'alarming rise in the misuse of the legal system as a tool to suppress criticism and democratic oversight'.¹⁶⁹

Other themes and analysis identified in the literature

This section outlines additional information surfaced as a part of the literature review. These do not map neatly onto the taxonomy, instead provide points that cut across the analysis.

Other themes

Additional information threats were mentioned in the literature and are listed below. In some cases, these were referenced in passing by specific studies with much of the literature tending to be organised by country or election, or by research methodology (e.g., surveys, an experiment, or content analysis) rather than by information threat. This tension between the evidence base and the focus of this review means there are some commonly accepted information threats for which no quality evidence was surfaced. This does not mean that these might not be important factors in UK elections now or in the future. These include:

- **Framing techniques** including cherry picking, context stripping, false attribution, false connections, false equivalence, misleading framing, selective editing / quote mining, shifting the Overton window, and translation distortions.
- **Coercive techniques** including threats, extortion, blackmail, and suppression of dissent.
- **Ecosystem manipulation techniques** including keyword stuffing, link farms, cloaking, click bait, and link rot exploitation.
- **Technical disruption**, including network, connectivity, power, or other utility outages; tampering with digital voting systems, defacement of official or candidate websites.
- **Market influence**, including media or platform capture or ownership.
- **Electoral process interference**, including legal or bureaucratic interference, gerrymandering, manipulating eligibility criteria, uneven application of rules.

Several parts of the literature examined in this review pointed to satire or humour – which are rightly afforded high levels of protection under the right to freedom of expression in the European Convention of Human Rights – as a factor that can exacerbate information-based threats or cause confusion. . A study of over 3,000 debunking articles in 2022 found UK audiences topped the ranking in misunderstood satires and parodies. These debunking articles were written by fact checkers from eight different countries.¹⁷⁰ Another study found that parody and satire received high user engagement in the 2024 UK General Election, yet even when presented as satirical, the realism of some forms of deepfake satire can confuse voters.¹⁷¹ A third study by Chatterje-Doody found that the Russian state routinely uses humour strategically as part of attempts to influence international audiences, including during elections.¹⁷²

Research on experiences of online information

Studies in a range of academic journals and the wider literature, across many countries, using a range of methods, have found that election disinformation can pose a challenge to democratic

¹⁶⁹ Kanellia, 2025. [The Rule of Law Under Siege: SLAPPs and the Chilling of Democratic Participation in Europe](#).

¹⁷⁰ Cazzamatta, 2024. [Global misinformation trends: Commonalities and differences in topics, sources of falsehoods, and deception strategies across eight countries](#).

¹⁷¹ Stockwell et al, The Alan Turing Institute, 2024. [AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections](#).

¹⁷² Chatterje-Doody, 2024. [Five disinformation tactics Russia is using to try to influence the US election](#).

participation, including in terms of apathy, decreased voter turnout, lower political engagement, and often resulting in political tensions and declining trust in the electoral process.¹⁷³ According to Gromping et al., disinformation has been found to distort election outcomes, create a disconnect between public perceptions of election fairness and the actual quality of the election; moreover the ability to disseminate false or misleading information with speed and scale has accelerated, raising urgent questions about how to preserve electoral integrity.¹⁷⁴

One review found that estimates of misinformation prevalence ‘exposure as a percentage of civic/ news content consumed online tend to hover around 1%-10%, with prevalence increasing considerably, to 10%-30%, for content involving contentious topics (i.e., climate, health, Russia/Ukraine)’.¹⁷⁵ Another found that ‘the use of disinformation in the context of electoral campaigns has been spreading in recent years across various parts of the world’.¹⁷⁶ In the UK, Ofcom published a General Election tracker in 2024 which found that a majority (60%) ‘claimed they had encountered information regarding the General Election that they felt might have been false or misleading at least once in the prior week’.¹⁷⁷

The Electoral Commission’s report on the 2024 UK General Election presented survey results which indicated that:¹⁷⁸

- Many said they saw misleading or inaccurate information about political parties’ policies (61% of survey respondents) and candidates (52%).
- Fewer than one third (30%) saw misleading or inaccurate information about how the elections work.
- Around a quarter (24%) saw or heard a deepfake photo, video or audio clip about the election.
- The most common response to seeing or hearing misleading content was to ignore it (64%). Around half (49%) of respondents said they took specific action, such as ‘fact-checking or reporting this information in some way’. Of these, 12% said they reported it to the service they saw it on.

In the 2025 UK local elections, the Electoral Commission found public confidence in the elections to be high, but misinformation / disinformation was the third biggest worry among survey respondents (and perceived bias in the media was second).

A Council of Europe report noted that ‘electoral campaigns are in essence information campaigns... designed to convince the voters and that therefore... some content shared by political contestants might be labelled disinformation but fall under the candidate’s freedom of expression’.¹⁷⁹ Another report found that measures designed to protect electoral integrity can, paradoxically, have the effect

¹⁷³ For example, Dragomir et al, 2024. [Beyond online disinformation: assessing national information resilience in four European countries.](#)

¹⁷⁴ Gromping et al, 2026. [How election management bodies disrupt electoral disinformation: Australia and the UK in comparative perspective.](#)

¹⁷⁵ Scharfbillig et al, European Commission Joint Research Centre, 2026. [Fractured Reality: How democracy can win the global struggle over the information space.](#)

¹⁷⁶ Casero-Ripolles et al, 2025. [Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections.](#)

¹⁷⁷ Four waves of 2,000 respondents, Ofcom, 2024. [UK General Election news and opinion-formation survey 2024.](#)

¹⁷⁸ Electoral Commission, 2024. [Report on the 2024 UK Parliamentary general election and the May 2024 elections.](#)

¹⁷⁹ Dickson, Council of Europe, 2025. [Foreign interference in electoral processes at local and regional levels.](#)

of impairing basic democratic and constitutional rights, preventing freedom of expression.¹⁸⁰ The difficulty of balancing approaches is highlighted by a May 2026 preprint discussing the results of a survey of over 47,000 people from 40 countries. It found a nearly even split between public preference for prioritising the protection of free expression (51%) and the prevention of misinformation spreading (49%).¹⁸¹

Questions about studies of the impact of information-based threats

Some of the literature examined in this review raised questions about the impact of certain information-based threats or stated challenges with analysing them. These included:

- One review reported that disinformation ‘is a limited problem with limited reach among the public’, when compared to other information and entertainment.¹⁸² It suggested instead a focus on the structural transformations that have impacted information flows and ‘attention allocation’ in the public arena.
- One study argued that common misperceptions include that average exposure to problematic content is high, that algorithms are largely responsible for this exposure, and that social media is a primary cause of broader social problems such as polarisation. Instead, it is argued, there is a pattern of low exposure to false and inflammatory content, and that exposure is concentrated among a narrow fringe with strong motivations to seek out such information.¹⁸³
- Another report argued that attempts to disinform are often marginal, ineffective, or ephemeral. People do not come across disinformation very often and when they do, they are able to recognise and selectively dismiss it. People mostly consume misinformation they are predisposed to accept. Acceptance should not be conflated with attitude or behavioural change since people do not change their minds easily, let alone their behaviour. Moreover, the volume of engagement with disinformation should not be conflated with belief, impact or acceptance. Sharing or liking is not endorsing or believing. The digital traces that are most easily studied do not always mean what we expect them to, nor do they reflect the plenitude of experience.¹⁸⁴
- One review stated that despite predictions of AI-driven electoral manipulation through the elections of 2024, this was largely overshadowed by more impactful factors including politicians’ willingness to misinform, lie, and break other norms. This is because of the inherent challenges of mass persuasion, the difficulty of reaching target audiences in an oversaturated high-choice information landscape, the complex interplay of multiple factors that shape voting behaviour, and the varied ways in which people consume information and form beliefs. The review also stated that people do not approach elections as blank slates, waiting to be persuaded by information. Instead, voting behaviours are shaped by multiple factors including long-standing predispositions and short-term context.¹⁸⁵

¹⁸⁰ Dawood, 2021. [Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats](#).

¹⁸¹ Spampatti et al, 2026. [Preferences for speech governance are polarized across 40 countries](#).

¹⁸² Jungherr & Schroeder, 2021. [Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy](#).

¹⁸³ Budak et al, 2024. [Misunderstanding the harms of online misinformation](#).

¹⁸⁴ Altay et al, 2023. [Misinformation on Misinformation: Conceptual and Methodological Challenges](#).

¹⁸⁵ Simon & Altay, 2025. [Don't Panic \(Yet\): Assessing the Evidence and Discourse Around Generative AI and Elections](#).

- One review reported that exposure to misinformation is lower than often believed, people are less gullible than commonly assumed, and misinformation often reflects, rather than causes, underlying sociopolitical issues.¹⁸⁶
- A 2026 study of the activities of over 600 users on one service during the German federal election campaign found political content was about 5% of videos watched and there was no clear evidence for asymmetric algorithmic curation of extreme political content. Instead, most of the political content users see on a certain service aligns with their stated political preferences.¹⁸⁷
- Finally, another review contended that democratic states and citizens have tools for countering disinformation and, thus, the apparent ubiquity of disinformation will not necessarily damage institutions nor hinder citizens' freedoms.¹⁸⁸

¹⁸⁶ Altay, 2025. [Rethinking the problem of misinformation and its solutions](#).

¹⁸⁷ Wedel et al, 2026. [Political content and news exposure of German TikTok users during the 2025 Federal German Elections](#).

¹⁸⁸ Echevarria et al, 2024. [State-Sponsored Disinformation Around the Globe](#).

Annex

Methodology

Approach to examining sources

Around 1,000 sources were returned from the searches. These were filtered based on a preliminary assessment of their credibility and their applicability to the study's focus, with over 250 making it into a long list. These were then prioritised on a scale of 1 to 3 based on their contribution to understanding the intersection of digital disinformation and elections in the UK, and the criteria below:

- High quality or high impact research published in high impact factor journals; or research from well-established civil society organisations, regulatory bodies, or journalists. To build upon this, we have also included media reporting which cover more recent events that might not have the same volume of research associated with it, preferring long-established sources where possible.
- Recent research, capturing the latest developments in the online information environment.
- Primary research based on data science, experiments, or surveys, over opinion or theoretical pieces.
- Studies of the UK, or countries with comparable electoral systems such as Australia, Canada, and Ireland.
- Studies of countries with recent elections which may indicate information-based future threats to UK elections, such as Romania, Moldova, or Czechia.
- Where there is particularly pertinent or substantial evidence, we have included studies from other countries.
- Studies of deceptive or abusive information tactics, techniques, and behaviours.

A score of 1 indicated the source was highly relevant for the research focus, a score of 2 indicated it had some relevance to background understanding or for specific disinformation behaviours, and a score of 3 indicated a useful paper on the general topic of disinformation or information interference. Any other papers were discarded. There were around 50 papers with a score of 1, over 120 with a score of 2, and around 80 with a score of 3.