

DEMOS

EPISTEMIC SECURITY

INFORMATION RESILIENCE
PRIORITIES FOR 2026-2029

HANNAH PERRY
AZZURRA MOORES
FLYNN DEVINE

AUGUST 2026



Open Access. Some rights reserved.

Open Access. Some rights reserved. As the publisher of this work, Demos wants to encourage the circulation of our work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons By Share Alike licence. The main conditions are:

- Demos and the author(s) are credited including our web address **www.demos.co.uk**
- If you use our work, you share the results under a similar licence

A full copy of the licence can be found at **<https://creativecommons.org/licenses/by-sa/3.0/legalcode>**

You are welcome to ask for permission to use this work for purposes other than those covered by the licence. Demos gratefully acknowledges the work of Creative Commons in inspiring our approach to copyright. To find out more go to **www.creativecommons.org**



CONTENTS

ACKNOWLEDGEMENTS	PAGE 4
INTRODUCTION: EPISTEMIC INSECURITY	PAGE 6
CHAPTER 1: THE INFORMATION SUPPLY CHAIN	PAGE 8
CHAPTER 2: NEW INFORMATION THREATS & VULNERABILITIES IN 2026	PAGE 11
CHAPTER 3: OPPORTUNITIES FOR RESILIENCE	PAGE 22
CONCLUSION: PRIORITIES FOR 2026-2029	PAGE 44

ACKNOWLEDGEMENTS

We would like to thank Demos colleagues Caragh Aylett-Bullock and Abduraman Sesay, for their desk research, contributions and analysis that informed its preparation as well as Elizabeth Seger, Sofia Lyall and Jamie Hancock for their earlier contributions to the thinking developed within this paper.

Thank you to the experts, Whitehall officials, regulators and cross-party Parliamentarians who attended two different roundtable discussions; one on 5 May 2026 at Demos' offices with a focus specifically on the Broadcasting Code and media standards regulation, and the second on 10 June 2026 hosted in Portcullis House with a focus on 'Epistemic Sovereignty'. Attendees provided invaluable input that has informed the findings and recommendations included here.

This project is financially supported by the Meliore Foundation, with specific support from the Global Strategic Communications Council and the Future of Tech Institute programmes.

All mistakes are the authors' own.

Hannah Perry, Azzurra Moores and Flynn Devine

August 2026

ABOUT THIS PAPER

Demos is the UK's leading cross-party think tank producing research and policies that have been adopted by successive governments for more than 30 years. Our mission is an upgraded democracy, with a new deal to mend the broken relationships between the state, institutions, and citizens.

This is the latest paper in Demos Digital's Epistemic Security programme that focuses on securing the UK's information supply chains and building our democratic resilience to adverse influences. It acts as a sequel to our first [Epistemic Security 2029](#) paper, published in February 2025, that first raised the alarm for urgent action to protect the information environment in order to tackle our democratic emergency.

Eighteen months on, we provide an updated picture of the new threats to our epistemic security and the priorities for a government in its first month in office. The new government must take bold, coordinated action led by and from the new Office of the Cabinet and Prime Minister to protect our democracy before it is too late. This paper provides a blueprint for those priorities.

INTRODUCTION

EPISTEMIC INSECURITY

In February 2025, Demos published its first paper on Epistemic Security, setting out the need to secure the information supply chain to democracy amid growing unrest at home and around the world.¹ We made the case that from a national security perspective, epistemic security is about securing our information supply chains, just as we would other critical resources like oil, gas, or semiconductors.

The term has since been used in Parliament, by journalists and by those across academia, civil society and the media who are seeking to build resilience in the information environment. The information supply chain that describes the production, dissemination and consumption of information, has provided a new framework for building that resilience.

We forewarned of growing threats that have since materialised in shocking and unprecedented ways, including the increasing appetite of the US administration to influence the political discourse of other sovereign nations, including our own. Manipulated information has fuelled further unrest in our communities. The urgency is only increasing, contributing to a growing democratic emergency.

Both overseas and here at home, democratic stability is being shaken. Engagement-driven algorithms give millions the means to amplify moments of collective anger. Political actors, domestic and abroad, see an opportunity to exploit this and inject division into public debate. Conspiracy theories move from the fringes into the mainstream, spreading rapidly through communities. Bots and coordinated inauthentic activity manufacture the appearance of social consensus, while virality goes unchecked. Real events are then distorted by this warped online discourse and people don't know what or who to believe.

The pace of technological advancement is creating new room for manipulation. As the world becomes less secure, and as adversaries of democracy wage information wars, these issues are becoming more pressing. Agentic AI may be leading towards a future where citizens no longer need to enter shared online spaces at all. The challenge is no longer one of challenging false information, but instead focusing on an ever more complex information supply chain that underpins democracy.

Domestically, we are facing a moment of crossroads, with a traditional two-party political system shifting towards five main parties, in a context where the ability to reach a political majority feels uncertain and the potential for consensus building for long term policy making is ever harder. But there is also a moment of opportunity where high stakes are triggering a reckoning in the parties to step up, be bolder and meet the rising dissatisfaction in politics with real change.

¹ Seger, Perry, Hancock (2025) Epistemic security 2029. https://demos.co.uk/wp-content/uploads/2025/02/Epistemic-Security-2029_accessible.pdf; Seger et al. (2020). 'Tackling threats to informed decision-making in democratic societies: Promoting epistemic security in a technologically advanced world'. The Alan Turing Institute. <https://www.turing.ac.uk/news/publications/tackling-threats-informed-decision-making-democratic-societies>

This paper seizes on that moment of change and pushes for the urgency to be captured by the incoming administration. Our information supply chains need robust support. There are reforms that will be readily available to the new government - policy proposals that have already been stress-tested by civil servants and developed in consultation with experts. But there are also areas that will require bold, new thinking: ideas that move past the nostalgia of how things have always worked, and instead put innovation and technology and the communities who will benefit front and centre. This means refreshing media standards to match the digital age and scale of the epistemic emergency; forging new international alliances no longer shadowed by Brexit; and thinking bigger on investment in new digital spaces.

In the last period, the government has attempted to address some of the problems in the information environment. Key progress included investing in local news,² promising a permanent BBC charter³ and setting out ambitious plans to ensure prominence of trustworthy information online.⁴ But, it was never enough to tackle the scale and challenge of the moment. As Keir Starmer has recognised, the time for incremental policy making is over. A new administration needs to make democratic resilience, including by improving our information supply chains, a driving mission. We have surrendered the sovereignty of our information environment.⁵ The government must show it can take back control on the people's behalf.

In 2026, we face new threats, but also seeds of change and momentum. Reliable decision-guiding information – and our ability to use it well – is the lifeblood of well-functioning democracy. We need to renew our efforts to protect the UK's modern information supply chain, for the volatile and technologically advanced world our democracies must steer through. This paper refreshes our call for action to fortify our epistemic security and upgrade our democracy.

Our central call is that the new government recognises the scale of the information emergency we face, the threats this poses to the health of our democracy and prioritises tackling it at the right level of government. The Defending Democracy Taskforce and its Secretariat should be moved to the new Office of the Prime Minister and Cabinet and publish an initial Information Ecosystems Resilience strategy, to be personally chaired and led by the Prime Minister.

The new government must take bold, coordinated action to protect our democracy before it is too late.



The new government must take
**bold, coordinated action to protect
our democracy before it is too late.**

2 DCMS (2026) 'Local journalism to benefit from new government funding to reach new audiences', GOV.UK, 7 July. Available at: <https://www.gov.uk/government/news/local-journalism-to-benefit-from-new-government-funding-to-reach-new-audiences>

3 Savage, M. (2026) 'Lisa Nandy vows to give BBC permanent charter to prevent political interference', The Guardian, 17 March. Available at: <https://www.theguardian.com/media/2026/mar/17/lisa-nandy-vows-bbc-permanent-charter-political-interference>

4 DCMS (2026) 'Plans for prominence of trusted news sources on social media alongside measures to reform Public Service Media in the UK', GOV.UK, 23 June. Available at: <https://www.gov.uk/government/news/plans-for-prominence-of-trusted-news-sources-on-social-media-alongside-measures-to-reform-public-service-media-in-the-uk>

5 We refer to this as our 'Epistemic Sovereignty' throughout the paper - the means of having autonomy and agency over the UK's 'Epistemic Stack' - the tools, platforms, and infrastructure that make up the UK's information ecosystem - without requiring compromises on our values as a democracy. This term is explained further in our policy recommendations 'The British Innovation Challenge'.

CHAPTER 1

THE INFORMATION SUPPLY CHAIN

The information supply chain describes how information flows from its initial production and distribution, to how and when it is retrieved by the public, to how it is evaluated and deliberated upon to inform democratic decision-making.⁶ In this chapter, we summarise the key features of epistemic security and how it has been compromised in recent years.

Like any supply chain, each stage presents both an opportunity for **innovation** and a point of **vulnerability**.

Like any supply chain, each stage presents both an opportunity for innovation and a point of vulnerability. Given information's crucial role, this framework offers a valuable shared lens for identifying and co-developing ways to strengthen how we, as a democracy, build knowledge and make decisions together.

Democracies depend on reliable information supply chains to function. When people cannot trust the information available to them, they cannot deliberate productively, whether in private or in public, and so cannot make informed choices. These might include how to vote in an election, or where to turn to in a crisis to understand what is happening. Governments face the same dependency. They need access to information they can trust is accurate, in order to act in citizens' best interests and fulfil their side of the democratic bargain. The graphic on the following page sets out the elements of the information supply chain.

⁶ This framework has been developed from Seger et al's (2020) depiction of an 'epistemic process', with components developed further surrounding information evaluation and sense-making / deliberation.

FIGURE 1
THE INFORMATION SUPPLY CHAIN



Information production

People, such as scientists, journalists, musicians, creators/ influencers, citizens, and now AI agents and bots produce information.



Information distribution

This information is distributed to wider communities and direct to individuals via various platforms e.g. text books, news broadcasts, emails, messaging apps, social media and recommender algorithms, search results, AI overviews and chatbot interfaces.



Information acquisition and evaluation

Information recipients retrieve the information (e.g. chatbot responses, social media posts, reels, articles, messages) within/ from that channel and evaluate it using whatever hooks or cues they can discern e.g. author/ source recognition, citations, links, likes and comments.



Information deliberation and decision-making

Information recipients consider the information and seek to make sense of it, deliberating with other community members, friends or strangers, before determining their own decisions or actions.

THE TRANSFORMATION OF OUR INFORMATION SUPPLY CHAIN UP TO FEBRUARY 2025

Our 2025 work set out four key and intersecting drivers that are disrupting the information supply chain.

First, what we called **“the digitisation of everything”** has both achieved two seemingly opposite effects: It has decentralised communication - empowering ordinary citizens, but fracturing shared narratives into echo chambers and fuelling a brutal attention economy. And it has **centralised unprecedented power** in the hands of unaccountable tech platforms and their owners, who can make unilateral decisions on dissemination, content moderation, even on infrastructure access with profound democratic consequences.

Second, the UK’s **news ecosystem** is weakening. Public interest in and trust of news has fallen sharply, and as audiences shift to social media and search, engagement-driven algorithms treat all “content” as equal regardless of reliability. This has gutted traditional revenue models, hitting local news hardest and leaving many communities in “news deserts” - information voids that get filled by speculation, distrust, and conspiracy.

Third, this vulnerability coincides with a **global authoritarian resurgence** and a heightened risk of **foreign interference in UK politics** - from established state actors like Russia to newer, non-traditional threats such as the outsized influence of tech billionaires operating from within allied nations.

Fourth, UK regulation has not kept pace. Much of our digital environment is still shaped by **permissive US legal norms**, and while the EU has attempted to build comprehensive platform accountability through the DSA and DMA, the UK’s Online Safety Act leaves major gaps — particularly around disinformation, foreign interference enforcement, and election-crisis preparedness. We are regulating for an analogue age.

Together, these four conditions compound the UK’s broader democratic pressures, deepening division and narrowing the window for effective intervention.

CHAPTER 2

NEW INFORMATION THREATS & VULNERABILITIES IN 2026

The world in the summer of 2026 is even more vulnerable than it was in February 2025, when Demos first reported on epistemic security. To understand the scale of the challenge requires first an assessment of what has changed: where do continued vulnerabilities persist, and where have new vulnerabilities emerged as a threat to our democratic system and, more specifically, to the UK's information supply chain?

Threats to and vulnerabilities within our information environment can be assessed and monitored through six lenses:

1

Concentration of **corporate power and foreign dependencies** across our information environment and lack of accountability

2

Collapse in **sustainability of news ecosystems and the lack of visibility/** imbalance of information

3

Global **authoritarian shift** and increasing **foreign interference**

4

Continued **gaps in legislation and regulation** (global and UK) and a lack of updated standards

5

Polarisation and hateful discord in deliberative spaces⁷

6

Gaps in news demand and critical media/ AI literacy skills⁸

⁷ While this is an important risk, we have not elaborated on it within this paper both for space and because it will be the subject of a dedicated Demos paper later in 2026.

⁸ Ibid

CONCENTRATION OF CORPORATE POWER AND FOREIGN DEPENDENCIES

As the UK's dependency on foreign tech companies has become more painful, the concept of 'sovereignty' has gained prominence in today's UK political debates on everything from AI and digital government to defence and energy.⁹ Yet the vulnerabilities in our 'epistemic sovereignty' have so far been under-explored.

Epistemic sovereignty means having autonomy and agency over the tools, platforms, and infrastructure that make up the information supply chain without requiring compromises on our values as a democracy.¹⁰

Our modern information supply chain depends on a cohesive system of interconnected digital infrastructure that fuels and enables platforms and tools that UK citizens use to engage with vital information every day. The concentration of power in the hands of a handful of tech companies wholly based in the US and China and the lack of control or influence the UK has over this digital infrastructure reflects a critical and sustained challenge for our epistemic health as a country.

Inspired by the 'full stack approach', we call the digital infrastructure that makes-up our information environment the 'Epistemic Stack'.¹¹ A simplified version includes 3 key layers:

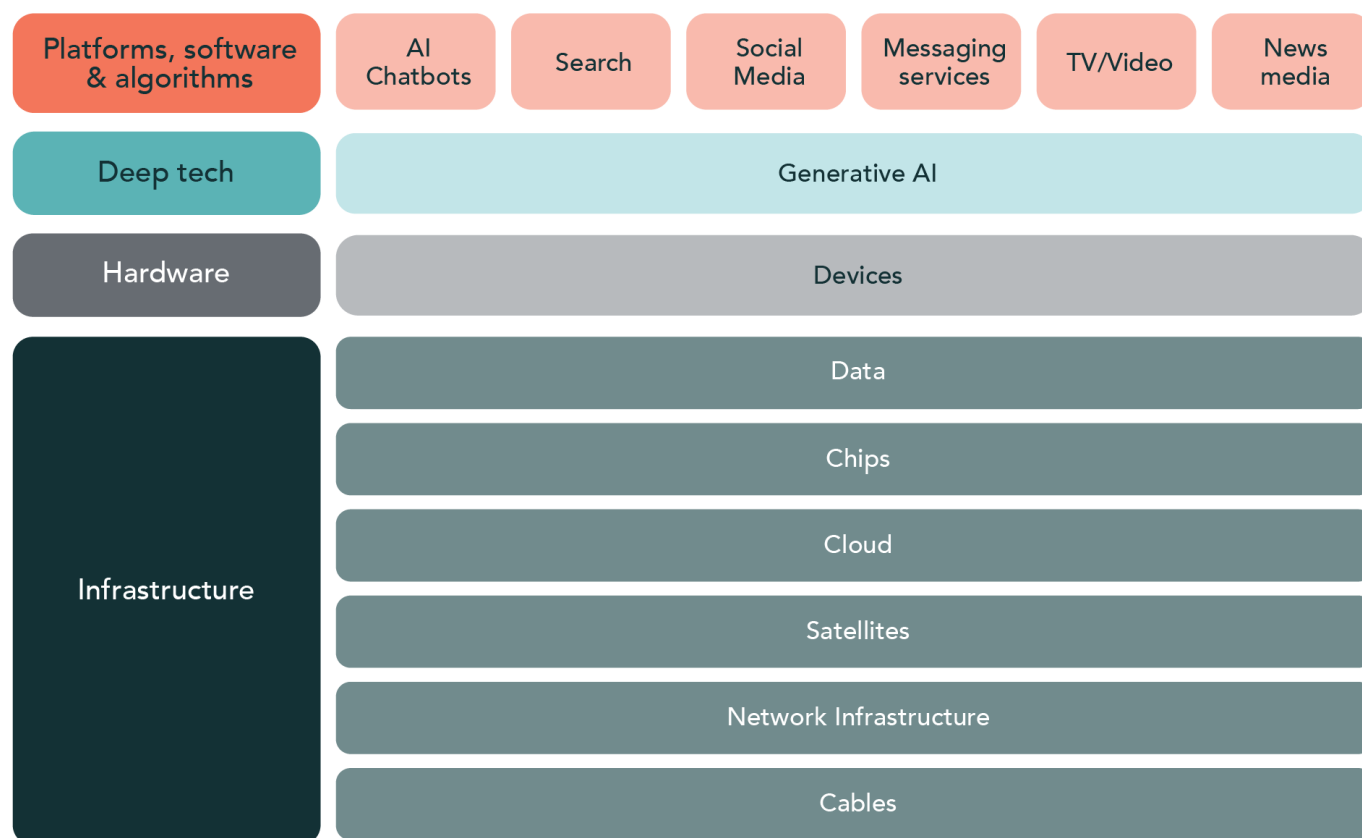
- 1. User-facing tools, software platforms, applications, and algorithms:** this top layer reflects the tools that UK citizens engage with everyday as a means of creating, discovering, and making sense of information and the world around them - including how we navigate the internet, synthesise information, and connect with one another in the digital realm. Here we include: generative AI interfaces, search, messaging applications, social media, the various configurations of video streaming, and news media digital applications.
- 2. Deep tech through generative AI:** Large Language Models, which output text, as well as audio/visual generating AI models are quickly becoming a foundational technology underpinning or altering many user-facing interfaces and platforms. This is either through directly changing the way the interface works - like Google's 'AI overviews' changing traditional search - or being used to create or inform content being shown to users - as is increasingly the case on social media or TV/Video.
- 3. Devices:** the middle layer of the stack is the means by which we engage with all digital information - this includes our phones, computers, TVs, radios, and more.
- 4. The foundational infrastructure of our information supply chain:** this bottom layer is critical for enabling the secure storage, transfer, and configuration of information - without these, nothing higher up the stack is possible. This includes cloud infrastructure, data, chips, networks (undersea cables, cell towers, fiber-optic networks).

9 House of Commons SIT Committee (2026) "Rewiring the state: Delivering digital government". <https://committees.parliament.uk/publications/53352/documents/298462/default/>

10 We deliberately refer here to 'sovereignty' and not 'digital sovereignty'. Whilst digital sovereignty is interdependent with 'epistemic sovereignty', there are aspects of the 'Epistemic Stack' which are not digital and aspects of 'digital sovereignty' which are not as high a priority for information ecosystems.

11 Jolly and Goodman (2021). "A "full stack" approach to public media in the United States. The German Marshall Fund." <https://www.gmfus.org/news/full-stack-approach-public-media-united-states>; Bria, Timmers, Gernone (2025). EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung. Gütersloh. https://assets.filedock.xyz/public/EuroStack_2025.pdf

FIGURE 2
A SIMPLIFIED REPRESENTATION OF THE 'EPISTEMIC STACK'



The dependency on foreign, corporate powers throughout its Epistemic Stack exposes the UK to a range of vulnerabilities:

- Dependencies at the 'top layer' on US social media platforms, search and AI chatbots. have already been used as leverage or as a bargaining tool to weaken state regulation. For example, the US government attempted to weaken UK Online Safety legislation impacting US social media companies in broader US-UK trade negotiations.¹² OpenAI also threatened to withdraw services from European citizens in order to weaken EU AI regulation.¹³
- Dependencies at this layer, particularly via social media, also exposes UK citizens to foreign interference and influence. This is evidenced by Elon Musk's ownership of and self-platforming on X combined with his appetite to influence UK democratic discourse on a range of sensitive topics including during moments of acute crisis and protest, with the most recent example regarding the killing of Nowak, 'two-tier policing' and the violent Southampton protests.
- Dependencies at the 'top layer' also impacts the reduction of visibility of news publisher content, the weakening of content moderation policies and removal of fact-checking programmes, and algorithms designed to provoke outrage rather than facilitating respectful debate.

¹² Sky (2025). "Online safety protections for children 'not up for negotiation' in US trade talks." <https://news.sky.com/story/online-safety-protections-for-children-not-up-for-negotiation-in-us-trade-talks-13341553>

¹³ Perrigo (2025). "OpenAI could quit Europe over new AI rules, CEO Altman warns". <https://time.com/6282325/sam-altman-openai-eu/>

- Foundational infrastructure dependencies of key services, including the BBC and the NHS, on US cloud and analytics software such as Amazon Web Services, Microsoft Azure and Palantir creates data security vulnerabilities to the US's Clarifying Lawful Overseas Use of Data (CLOUD) Act.¹⁴ The US government can effectively at any time request access to UK data stored by these companies.¹⁵
- At the foundational infrastructure layer, the UK also faces risks of loss of access to semi-conductors critical to the 'chips' needed for all devices due to our dependency on Taiwan who itself is vulnerable to the invasion of China.¹⁶ Our dependencies on data centres hosted overseas e.g. in the Gulf also presents a risk if they are, for example, targeted by Iran in the US-Israel conflict or experiencing major maintenance failures such as the 2025 AWS outage.¹⁷

It is, of course, not feasible to have total autonomy and agency over every element of the Epistemic Stack. But there are areas where our vulnerability is acute; namely where we also lack democratic values alignment such as the available social media platforms and AI chatbots. The UK population all use US and Chinese social media because there are few high quality alternatives. Platforms like Mastodon and Bluesky are gesturing in the right direction, but are clearly struggling for traction. We rely on US and Chinese AI models because we have yet to consolidate a sovereign AI strategy that would support the creation/dissemination of viable alternatives, given the significant barriers to entry on training models from scratch (cost, compute, energy, etc.) and the ongoing debates on open source. Where we have higher autonomy/agency and democratic values alignment, such as via UK public service broadcasters and news media, entities are struggling to maintain both financial sustainability and visibility through the increased digital mediation of social media and chatbots. They also, whilst offering high sovereignty at the 'top' layer of the stack, still largely rely on infrastructure with low levels of sovereignty e.g. the UK's reliance on Cloud provided by AWS and Microsoft Azure.

The UK government is currently seeking to close the 'autonomy' and 'democratic values gap' through collaborative partnerships, regulation and to an extent procurement and innovation investment in some areas of the stack. Yet such approaches have so far been piecemeal, uncoordinated and proven insufficient to tackle the size and complexity of the problem impacting the information supply chain in the context of escalating tech oligarchic power. These approaches also fail to clearly articulate or drive towards a positive vision of a digital public sphere in the UK.

Recommendations 5a-b, 'The British Innovation Challenge: Epistemic Sovereignty' aim to tackle this threat. See pages [37-39](#).

14 A 2025 July investigation by the Competition and Markets Authority found that 60-80% of the UK cloud market was made-up of two US companies: Amazon Web Services and Microsoft Azure. Future of Tech Institute (2026) A Digitally Sovereign Britain -https://cdn.prod.website-files.com/6a61d19f83fdca4fd1dd7efb/6a732bea5378e672451b4689_A_Digitally_Sovereign_Britain.pdf

15 Burnett (2026). White Paper demystifying the debate on US Cloud Act vs European/ UK Data Sovereignty <https://cms.law/en/gbr/legal-updates/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data-sovereignty-in-the-context-of-cloud-services>; ORG (2026). Tech giants and giant slayers: the case for digital sovereignty and the digital commons. https://www.openrightsgroup.org/app/uploads/2026/04/Tech_Giants_and_Giant_slayers_Digital_Sovereignty_and_the_Digital_Commons.pdf

16 US International Trade Administration (2025). "Taiwan Country Commercial Guide", <https://www.trade.gov/country-commercial-guides/taiwan-semiconductors-including-chip-design-ai>

17 Montgomery (2026). "Datacenters are becoming a target in warfare for the first time", <https://www.theguardian.com/technology/2026/mar/10/datacenters-target-warfare-iran>; Kleinman (2025). "What caused the AWS outage - and why did it make the internet fall apart?" <https://www.bbc.com/news/articles/cev1en9077ro>

COLLAPSE IN NEWS ECOSYSTEMS AND A LACK OF VISIBILITY AND IMBALANCE OF TRUSTWORTHY INFORMATION

Good quality information is the lifeblood of any democracy - and yet the challenges facing our news and public service media ecosystem cannot be under-estimated. In our last Epistemic Security 2029 paper, we emphasised the decimation of the local news industry in particular and the risks of increasing news avoidance. Here we examine new and emerging threats in 2026.

The news industry is facing a crisis of visibility. Content is no longer as easily seen or accessed by the public as it was even as recently as 2025, as the turn to chatbots, AI-powered search and AI overviews, for information hastens. A growing trend, coined “zero-click,” is reshaping how people consume information; where readers are increasingly opting for a single, condensed summary directly within the search interface.¹⁸ This leaves little incentive to click through to original reporting and little understanding of the sources of the information where citations and labelling remain either invisible, inconsistent or inaccurate.

This is not a marginal shift. One study found that AI summaries caused 80% fewer click-throughs for some of the UK’s largest news publishers, with publishers expecting search traffic to fall by more than 40% over the next three years.¹⁹ Pew Research Center, tracking almost 69,000 real search queries, found that users clicked through to a traditional link just 8% of the time when an AI summary was present, compared to 15% when it was not - and that only 1% of users clicked on a source cited within the summary itself.²⁰ In evidence submitted to the Competition and Markets Authority (CMA), DMG Media, publisher for the Daily Mail and the i Paper, reported that click-through rates for its content fell by as much as 89% in the worst-affected cases where an AI overview appeared above its results.²¹

The zero-click trend weakens audiences for news media even further, when referral traffic from social media platforms has already plummeted. Between 2018 and 2023, Facebook referral traffic to news publishers fell by between 40% and 55%, while between 2022 and 2023, referrals from X declined by 20% to 48%, depending on the publisher.

For an industry still heavily reliant on advertising revenue tied to page views and session length, this scale of decline poses a genuine threat to the financial sustainability of UK journalism. This has only worsened the pressures already documented in earlier versions of this report around the decimation of local news as well as on the UK’s public service broadcasters (PSBs).

The rise of global video streaming services (e.g. Netflix) and video-sharing (e.g. YouTube, Tiktok) has left UK PSBs struggling to compete. Ofcom’s 2026 Media Nations report found that Netflix has overtaken the BBC as UK viewers’ first choice when deciding what to watch, with 26% naming it their default destination against 25% for the BBC and just 9-15% for ITV.²² This decline in audience share leaves PSBs in a dangerous financial situation with the BBC’s own position illustrating the scale of the problem. Licence fee income has fallen by more than 30% in real terms in recent years, driven by a decline in the number of households paying it, cost inflation and growing competition from streaming platforms.²³ This contributed to the BBC posting a deficit of £121 million against a planned deficit of £33 million, and to the announcement of

18 Lopez-Lopez, D. (2026) ‘The click is no longer the strategy: How brands win in a zero-click world’, Forbes, 8 July. Available at: <https://www.forbes.com/sites/esade/2026/07/08/the-click-is-no-longer-the-strategy-how-brands-win-in-a-zero-click-world/>

19 Savage, M. (2025) ‘AI summaries causing “devastating” drop in online news audiences, study finds’, The Guardian, 24 July. Available at: <https://www.theguardian.com/technology/2025/jul/24/ai-summaries-causing-devastating-drop-in-online-news-audiences-study-finds>

20 Pew Research Center, “Do people click on links in Google AI summaries?” (22 July 2025). <https://www.pewresearch.org/short-reads/2025/07/22/google-users-are-less-likely-to-click-on-links-when-an-ai-summary-appears-in-the-results/>

21 Southern, M.G. (2025) ‘Google AI Overviews impact on publishers & how to adapt into 2026’, Search Engine Journal, 29 September. Available at: <https://www.searchenginejournal.com/impact-of-ai-overviews-how-publishers-need-to-adapt/556843/> and MG Media (2025) Proposed decision on the CMA’s strategic market status investigation into Google and Apple’s mobile platforms: Response from DMG Media. Available at: https://assets.publishing.service.gov.uk/media/68a5aa50a6acbbc7fb96a3b2/DMG_Media.pdf

22 Broadband TV News (2026) ‘Netflix overtakes BBC as UK viewers’ first choice, says Ofcom’, Broadband TV News, 29 July. Available at: <https://www.broadbandtvnews.com/2026/07/29/netflix-overtakes-bbc-as-uk-viewers-first-choice-says-ofcom/>

23 BBC News (2024) ‘AI to replace actress’s voice in BBC documentary sparks debate’, BBC News, 28 March. Available at: <https://feeds.bbc.co.uk/news/entertainment-arts-68654318>

£500 million in further cuts, including 2,000 job losses.²⁴ The BBC's Royal Charter is currently under review, with these issues front and centre of public debate.

Other PSBs are not immune to this squeeze. In 2026, Sky's proposed £1.6 billion acquisition of ITV's Media & Entertainment business,²⁵ and BBC Director-General Matt Brittin's confirmation of talks with Channel 4 over folding its content into iPlayer,²⁶ both signal that the UK's remaining public service broadcasters no longer see standalone survival as viable against global streamers.

Local news has been hit even harder. The Public Interest News Foundation's UK Local News Report found that, as of October 2025, 37 local authority districts - around one in ten - qualify as "news deserts," 27 of which have no dedicated local news outlet at all.²⁷ Altogether, roughly 4.4 million people live in areas without meaningful local news coverage, and the pattern is not evenly spread: closures in 2025 were concentrated overwhelmingly in the most deprived and urban districts, while new outlet launches skewed towards more affluent areas. This signals an inequality of choice and access in our information supply chain that demands more detailed assessment.

The challenge for this government is to tackle the loss of visibility and demand for both British public service media and journalism that threatens providers' long-term financial sustainability and ultimately the diversity and plurality of sources available in our information environment.²⁸

Recommendations 4a-f, '*Improving the discoverability, attribution and trustworthiness of high quality information*' (pages 33-37) and **Recommendations 6a-b**, '*Revitalising Local Information Digital Places and Spaces*' (pages 40-41), aim to tackle these vulnerabilities.

GLOBAL AUTHORITARIAN SHIFT AND INCREASING FOREIGN INTERFERENCE

Demos has long been sounding the alarm on the democratic emergency we face in Britain.²⁹ The growing disillusionment with our democratic system was evident in the May 2026 local and devolved election results followed by the resignation of the sixth Prime Minister in ten years. Such discontent with the state leaves the UK public vulnerable to manipulation and anti-democratic forces.

Globally, authoritarianism and foreign interference is on the rise and no longer a phenomenon confined to the usual suspects. In 2026, global democracy for the average person fell back to 1978 levels, with autocracies now outnumbering democracies worldwide for the second year running and 74% of the world's population living under autocracy, up from 50% in 2005.³⁰ This year, the V-Dem Institute has included the UK in the list of democracies that are 'autocratising'

24 Tobitt, C. (2026) 'BBC journalists' pay 2026: Stephen Nolan becomes highest-paid journalist', Press Gazette, 14 July. Available at: <https://pressgazette.co.uk/media-audience-and-business-data/highest-paid-bbc-journalists-2026-stephen-nolan>

25 Kanter, J. (2025) 'BBC, ITV, Paramount & Channel 4 chiefs downplay merger talks: "I'm not sure that's good for the UK"', Deadline, 18 September. Available at: <https://deadline.com/2025/09/bbc-itv-channel-4-paramount-downplay-merger-1236544836/>

26 Broadband TV News (2026) 'BBC and Channel 4 discuss streaming partnership', Broadband TV News, 8 July. Available at: <https://www.broadbandtvnews.com/2026/07/08/bbc-and-channel-4-discuss-streaming-partnership/>

27 Public Interest News Foundation (2025) 'Local news launches, closures and the state of play in 2025', Public Interest News Foundation, 11 December. Available at: <https://www.publicinterestnews.org.uk/blog/local-news-launches-closures-and-the-state-of-play-in-2025/>

28 The decline in trust and demand for public service broadcasting and journalism over the last decade is also particularly noteworthy and underpins recommendation 4a which focuses on improving the independence and public accountability of the BBC in particular.

29 Curtis, P. (2026). The New Deal: How to repair the broken relationship between state and citizen. Demos <https://demos.co.uk/research/the-new-deal-how-to-repair-the-broken-relationship-between-state-and-citizen/>

30 Nord, M., Altman, D., Fernandes, T., Good God, A. and Lindberg, S.I. (2026) Democracy Report 2026: Unraveling The Democratic Era? University of Gothenburg: V-Dem Institute. Available at: https://www.v-dem.net/documents/75/V-Dem_Institute_Democracy_Report_2026_lowres.pdf

highlighting “a substantial decline in freedom of expression and the media” - providing yet another reminder that vulnerabilities in our information ecosystem undermine the health of our democracy.

Key voices such as the Foreign Affairs Committee, the Intelligence and Security Committee, and the Rycroft Review are now raising the alarm about the scale of foreign interference in the UK’s information environment from threat actors such as Russia, China and most recently Iran.³¹ The now well-known example of Iranian interference in the Scottish independence debate, which saw pro-independence sentiment amplified by an Iranian-linked network, is indicative of this broader trend.³²

The Rycroft Review, commissioned by the government to examine foreign interference in the political funding landscape, made a clear finding: interference in this country was happening through foreign actors’ “sustained efforts to undermine trust in democracy by stoking divisive debate, principally on social media.”³³ Rycroft pointed in particular to the low financial cost and ease with which malicious actors can deploy fake social media accounts and automated bots to push disinformation at scale.³⁴ The government itself has also recognised, “an industrial-scale attack on the UK’s and our allies’ information environment, aimed at undermining our security and democratic systems, with Russia engaged in information warfare against the UK and Ukraine.”³⁵

The role of US political actors and tech oligarchs in the UK’s information environment cannot also be under-stated. Demos’ 2025 report pointed to Elon Musk’s growing engagement in UK politics. Since then, Musk has interfered in the UK’s domestic affairs with such increasing frequency the former Prime Minister accused Musk of actively whipping up division in Britain.³⁶ During the 2024 summer riots, fewer than 7% of Musk’s posts on X touched on UK race and immigration politics, but by the period between 31 May to 12 June - coinciding with the Southampton protests following Nowak’s murder, and unrest in Belfast - that figure had jumped to 31%.³⁷

Musk is not an isolated case. Senior figures within the US administration itself have increasingly used their platforms to intervene in UK domestic policy. In his March 2025, Munich Security Conference speech, Vice-President JD Vance accused European “commissars” of suppressing free speech, likening disinformation regulation to Soviet-era censorship,³⁸ before returning to the theme in an August 2025 meeting with then Foreign Secretary, David Lammy, warning that the UK risked a “very dark path” through its regulation of US social media platforms.³⁹

31 Foreign Affairs Committee (2026) Disinformation diplomacy: How malign actors are seeking to undermine democracy. Fourth Report of Session 2024–26. London: House of Commons. Available at: <https://publications.parliament.uk/pa/cm5901/cmselect/cmfaff/703/report.html>; Intelligence and Security Committee of Parliament (2025) Annual Report 2023–2025. London: Intelligence and Security Committee of Parliament. Available at: <https://isc.independent.gov.uk/wp-content/uploads/2025/12/ISC-Annual-Report-2023%E2%80%932025-Web-Accessible.pdf>

32 The Times (2024) ‘Bogus tweets paint Iranian military as Scottish independence fans’, The Times, 2 October. Available at: <https://www.thetimes.com/uk/science/article/bogus-tweets-paint-iranian-military-as-scottish-independence-fans-7thbt7vc3>

33 Rycroft, P. (2026) The Rycroft Review: Report of the independent review into countering foreign financial influence and interference in UK politics. London: Ministry of Housing, Communities and Local Government. Available at: <https://www.gov.uk/government/publications/the-rycroft-review-report-of-the-independent-review-into-countering-foreign-financial-influence-and-interference-in-uk-politics/the-rycroft-review-report-of-the-independent-review-into-countering-foreign-financial-influence-and-interference-in-uk-politics>

34 Ibid.

35 Foreign Affairs Committee (2026) “Disinformation diplomacy: How malign actors are seeking to undermine democracy: Government Response”. <https://committees.parliament.uk/publications/53394/documents/298809/default/>

36 McKiernan, J. (2026). ‘Starmer accuses Musk of trying to whip up division over Henry Nowak murder’. BBC, 4 July. <https://www.bbc.co.uk/news/articles/c1e2ww900zno>

37 Savage, M. (2026) ‘Elon Musk posted twice as often on UK race and immigration as about SpaceX in IPO run-up’, The Guardian, 4 July. Available at: <https://www.theguardian.com/technology/2026/jul/04/elon-musk-uk-race-immigration-spacex-ipo>

38 Vance, J.D. (2025) Speech by J.D. Vance: The U.S. in the World. Munich Security Conference, Munich, 14 February. Available at: <https://securityconference.org/en/medialibrary/asset/the-speech-of-jd-vance-20250214-1817/>

39 Sky News (2025) ‘JD Vance warns against UK going down “dark path” of losing free speech during meeting with David Lammy’, Sky News, 8 August. Available at: <https://news.sky.com/story/jd-vance-warns-against-uk-going-down-dark-path-of-losing-free-speech-during-meeting-with-david-lammy-13408626>

The Trump administration's December 2025 National Security Strategy went further, describing Europe as facing "civilisational erasure" and calling on Washington to "cultivate resistance" within the region.⁴⁰ Such explicit threats from an ally and whose digital infrastructure dominates our information supply chain puts the UK in a highly vulnerable position.

The next challenge for the new government will be to confront where interference intersects with, as yet, unregulated technology; Artificial Intelligence. AI, even without interference or malintent, can introduce text-based misinformation through hallucinations at a significant scale and sow confusion during crisis events through everyday use of its ever-improving video, audio and image content generation features.^{41,42} However, AI's covert uses by threat actors are of even greater concern. While some focus has been afforded to the risks of LLM training data poisoning, 'Retrieval Augmented Generation' (RAG) poisoning is another emerging threat. This is the manipulation of what is retrieved and used from the open internet by LLMs, fabricating news sites and editing of forum and Wikipedia entries, in order to change the results LLMs produce. This has already become a widespread practice and offering within the private sector for commercial purposes by 'Generative Engine Optimisation' companies. Demos found evidence of a sanctioned Russian foreign information manipulation and interference (FIMI) outlet, the 'Foundation to Battle Injustive' (r-FBI) is being favourably cited in five LLM services offered by frontier AI companies as a result of RAG poisoning.

The scale, nature and risk of impact of foreign interference on our democratic discourse is no longer one that can be discretely handled by a siloed FCDO. It must instead be understood as a cross-government democratic resilience challenge particularly by those tackling the risks of LLM-powered technologies, gaps in good quality information provision and vulnerabilities during crises and elections.

While all recommendations will tackle this threat, **Recommendations 7a-c**, *'Readying for the next frontier of information warfare: the foreign manipulation of LLMs'* ([pages 42-43](#)) to tackle the specific threat of foreign manipulation of LLMs.

40 Naughtie, A. (2025) 'Trump administration warns Europe of "civilisational decline" in new national security strategy', Euronews, 5 December. Available at: <https://www.euronews.com/my-europe/2025/12/05/trump-administration-warns-europe-of-civilisational-decline-in-new-national-security-strat>

41 Stockwell, S., Janjeva, A. and McDonald, B. (2026) Adding Fuel to the Fire: AI Information Threats and Crisis Events. The Alan Turing Institute, 11 February. Available at: <https://cetas.turing.ac.uk/publications/adding-fuel-to-fire>

42 Hancock, J. and Moores, A. (2026) Electoral Hallucinations: Safeguarding UK Elections in the World of LLMs and AI Chatbots. Demos, 20 May. Available at: <https://demos.co.uk/research/electoral-hallucinations-safeguarding-uk-elections-in-the-world-of-llms-and-ai-chatbots/>

GAPS IN LEGISLATION AND REGULATION AND A LACK OF UPDATED STANDARDS

Across print, broadcasting, social media and artificial intelligence the UK's regulatory landscape is struggling to keep pace with the speed of digital innovation change in the information environment. These gaps are particularly acute in moments of vulnerability for our democracy, such as during election periods and crises. Our own attempts at enforcing competition law has also been severely lacklustre. Where action has been taken, it has often arrived late and incompletely. Because of our ongoing dependencies on US tech platforms, the UK continues to be buffeted by the US's hands-off approach to internet regulation heavily influenced by First Amendment protections. The lack of antitrust enforcement in the US technology sector continues to enable global market dominance by the tech giants that control these platforms.

In the UK, the regulatory response to publishers' loss of traffic and revenue has, so far, centred on the Competition and Market Authority's powers under the new digital markets regime, shaped by the Digital Markets, Competition and Consumers Act 2024. Progress has been real but slow. In October 2025, the CMA designated Google with Strategic Market Status (SMS) in general search - the first such designation under the new regime. The CMA has the power to impose "conduct requirements" on Google's search business. However, it was not until June 2026 that it exercised this power, requiring Google to give publishers tools to opt out of their content being used to power AI Overviews and other generative features, and to ensure that content which is used is clearly attributed with an identifiable link.⁴³

The progress represented by the CMA's designation follows a prolonged copyright debate throughout 2025 surrounding the issues of transparency, consent and fair compensation for the use of creative works and journalism to train large language models and other generative AI systems.⁴⁴ The former Secretary of State, Liz Kendall, has since confirmed that a copyright exception with a rightsholder opt-out is no longer the preferred option. While this marked significant progress, the wider policy framework to ensure the balance between AI innovation and accountability, as well as the financial sustainability of the creative economy, remains unresolved. The CMA has an opportunity to go further in this debate.

Section 230 of the Communications Act 1934, continues to allow US-based social media companies to operate with the content moderation requirements they choose. The UK's Online Safety Act remains a regulatory challenge for the UK's information environment - particularly where it continues to fail to set mandatory minimum standards for platforms' Terms of Service (that reflect content moderation standards). Its False Communications Offence, designed to target the deliberate spreading of misinformation, targets individuals, not platforms, and Ofcom cannot force takedowns itself. We flagged this gap in our previous Epistemic Security 2029 report; it remains unresolved.

Some progress has also been made in relation to Crisis Protocols, which set out how platforms can and should respond during moments of crisis, such as the Southport riots in 2024. The new rules, introduced through the Online Safety Act, have been subject to a lengthy consultation process, which concluded in summer 2026. The protocols represent progress in recognising the different forms that crises can take and the need for an appropriate platform response. However, their potential impact remains limited by their voluntary nature and lack of enforceability, and have yet to receive parliamentary approval.

43 Competition and Markets Authority (2026) CMA secures fairer deal for publishers and improves Google search services in UK. Available at: <https://www.gov.uk/government/news/cma-secures-fairer-deal-for-publishers-and-improves-google-search-services-in-uk>

44 News Media Association. (2025) Make It Fair. Available at: <https://newsmediauk.org/make-it-fair/>

In a converged media environment, the same piece of content can move across television, broadcaster websites, video streaming services, and social platforms within hours. And yet, regulation has not converged with it: a single item of content can face an entirely different regulatory regime depending on its method of distribution, rather than its substance. Content broadcast on linear television answers to the Broadcasting Code,⁴⁵ and, if BBC-produced, to the BBC's editorial guidelines;⁴⁶ the same content clipped for social media falls under the Online Safety Act, and again under a different framework once redistributed via a platform such as YouTube; written up for print, it may face a further, voluntary code. The result is a fragmented landscape that audiences find difficult to navigate and most important, who and what to trust.

Some movement is now underway to close the gap on how broadcasters and streamers are regulated. The Media Act 2024 granted Ofcom new powers to create a dedicated content standards code for video-on-demand (VoD) services, extending broadcaster-style obligations to platforms that have historically sat outside the Broadcasting Code.⁴⁷ In February 2026, the Government laid secondary legislation designating the largest VoD platforms - including Netflix, Prime Video and Disney+ - as "Tier 1" services, required to meet new standards and accessibility code.⁴⁸ The final version of the standards aren't expected to be implemented for a year. While the move marks the first time major streaming services have faced content standards, the codes are limited to harmful content, fairness, privacy and due accuracy in news while gaps in the adaptation of regulation for advertising in such spaces remain untouched.

Going further, steps have been taken by the Media Act 2024 to advance the Prominence regime beyond just linear television broadcasting to VoD services, granting more people greater access to good information. However, the Act fell short by not extending prominence obligations to third-party platforms, such as video streaming services like YouTube. In a positive step, the Government's Green Paper, *Watch This Space*, has subsequently opened discussions on extending the regime not only to video streaming platforms but also to social media.

Electoral law has proven less adaptable. Existing election law was written for a time when elections were fought entirely on the doorstep, not for a modern election in which the real battleground is now on people's feeds. Tackling deepfakes is a prime example of where current legislation partially tackles a problem and has legal uncertainties. Section 106 of the Representation of the People Act 1983, which prohibits false statements about candidates, predates the technology entirely, is a prime example of where modernisation must occur.⁴⁹ The Electoral Commission itself has highlighted the problematic legal ambiguity as to whether, because of its digital medium, a deepfake would fall into scope of the Act.^{50,51}

A related and newer threat, one that has only amplified because of increased usage since 2025, is LLM-powered AI services such as AI chatbots, and particularly their reliability as a source of electoral information. Chatbots currently sit almost entirely outside any legal framework: outside the specific contexts addressed by the OSA, AI systems remain under-regulated.⁵²

45 Ofcom (2020) The Ofcom Broadcasting Code. Available at: <https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-standards/broadcast-code>

46 BBC, Editorial Guidelines. Available at: <https://www.bbc.co.uk/editorialguidelines>

47 Broadband TV News (2026) UK's biggest VOD services set for tougher Ofcom rules under Media Act rollout. Available at: <https://www.broadbandtvnews.com/2026/02/24/uks-biggest-vod-services-set-for-tougher-ofcom-rules-under-media-act-rollout/>

48 Department for Culture, Media and Sport (2026) Updates to the regulation of TV and video-on-demand services. Written statement HCWS1354, 24 February 2026. Available at: <https://questions-statements.parliament.uk/written-statements/detail/2026-02-24/hcws1354>

49 Demos (2026) The Deepfake Gap: Regulating False Statements & AI to Safeguard Elections. Available at: https://demos.co.uk/wp-content/uploads/2026/03/The-Deepfake-Gap_Briefing.pdf

50 Electoral Commission (2025) Written evidence submitted by the Electoral Commission to the Speaker's Conference (SCS0049). Available at: <https://committees.parliament.uk/writtenevidence/141330/pdf/>

51 Both the National Security Act and the Online Safety Act provide thresholds that may also prohibit the sharing of deepfakes, particularly when they involve acts of foreign interference or illegal content, but the ambiguity here may worsen the ability to act with speed.

52 Hancock, J. and Moores, A. (2026) Electoral Hallucinations: Safeguarding UK elections in the world of LLMs and AI chatbots. Demos. Available at: https://demos.co.uk/wp-content/uploads/2026/05/Electoral-Hallucinations_Report_2026.ac_.pdf

More broadly, the Starmer government made clear that it did not intend to introduce overarching regulation for all AI services, opting instead for a domain-specific approach under which existing regulators oversee AI within their own sectors, for example, online safety. While Labour's manifesto and 2024 King's Speech had promised binding legislation targeting the handful of companies developing the most powerful frontier AI models, this has not yet materialised. This approach continues to create regulatory uncertainty, risks leaving gaps in legal coverage, fragments oversight, and can lead to conflicting positions across different laws.

The challenge for the government is twofold: to address the gaps in our outdated legislation and standards for our digitised information environment, while also challenging the regulator to recognise the urgent need to bring the regulatory framework up to speed with the same ambition as the government sets.

Recommendations 2a-c *'Building our country's resilience in moments of crisis'* (pages 26-29), **Recommendations 3a-b**, *'Safeguarding our elections against digital information threats'* (pages 30-32) and **Recommendations 4a-f**, *'Improving the discoverability, attribution and trustworthiness of high quality information'* (pages 33-37).

CHAPTER 3

OPPORTUNITIES FOR RESILIENCE

The new Prime Minister Andy Burnham's arrival is an opportunity for bold, radical change, but it will be constrained by one key factor: a manifesto with little fiscal wiggle room and little mention of reform to the UK's information supply chains. Until he is ready to run on a manifesto of his own, there will be a limit to the scale of intervention possible. But that should not become an excuse for inaction. Instead, there should be a shared view going forward that the greatest risk in this moment of democratic emergency is to move too slowly, too passively, or not at all.

A second critical risk is to act without building cross-party support or public legitimacy. Reforms to the information environment are typically met with concerns about introducing bias in favour of the prevailing government of the day or fears about increasing restrictions on public freedoms like free expression. These risks are not just matters of perception. They need to be proactively tackled by ensuring policy design includes democratic safeguards and any mitigations for maintaining balance and fairness in the system.

Securing our information supply chains is about extending our critical freedoms and values into a digital age in order to tackle the threats identified in Chapter 2; confronting the concentration of unaccountable corporate power and foreign dependencies across our information environment, revitalising our news ecosystems, their connection to and rootedness in our communities, and its visibility; building resilience to hostile state actors and updating our legislative regime for the digital age.

Work to build democratic resilience across government has already begun; its limitations have not been legislative challenges, but a lack of political leadership, coordination and ambition. Reforming and building resilience into our information ecosystem requires systems change. Any proposal set out in this paper will need the backbone of cross-government coordination to be fully and effectively implemented.

Furthermore, not every problem facing our information ecosystem is one that requires legislation to resolve. The powers already allocated to regulators such as the Competition and Markets Authority (CMA) or Ofcom are also sufficient to take action. The challenge instead is raising the bar on their speed and aspiration.

This section articulates a long-term vision for Britain's information environment, while identifying which parts of that vision can be delivered through immediate political intervention, making the most of the energy found in the first period of a new Cabinet. The vision builds out a government agenda that reclaims public control of the information landscape, that focuses on place-based renewal and puts the public interest before unchecked corporate power.

This balancing act is complicated for any new government still finding its footing, but even more so for a government restricted by manifesto commitments and a pre-determined legislative agenda. But, if Britain gets this balance right, it has a chance to lead the global effort to build epistemic resilience in a digital age.

This section outlines that vision, going further than a previous administration was willing to go, while also building on the thinking needed to push forward legislation. It recognises that without a bold reframing of our country's relationship with powerful technology companies, we will remain heavily influenced by an unregulated minority, and that without good information front and centre, our citizens will lack the tools they need to properly engage with our democratic systems.

THE FIRST ACTIONS FOR A NEW GOVERNMENT

1. The Prime Minister should lead on democratic resilience and Britain's Information Resilience Strategy from the centre

The scale of the democratic challenge facing our country is enormous. There is no shortage of senior voices making clear that we are living in unprecedented times, and yet the task of tackling information crises and improving democratic resilience is scattered across the government. When the country is in a moment of heightened emergency, the Prime Minister steps up. Now it's time for the Prime Minister to grip our democratic threats and place it at the centre of government.

We welcome the first Machinery of Government changes that united responsibility for digital policy under DDCMS, but urge the government to show the depth of its commitment to democratic and information resilience by taking immediate steps to lead this from the centre.

TABLE 1
IMMEDIATE ACTIONS FOR THE PRIME MINISTER

ACTION	DESCRIPTION
1a) Elevate the Defending Democracy Taskforce by moving its Secretariat to the new Office of the Prime Minister and Cabinet and publishing an initial Information Ecosystems Resilience strategy, to be personally chaired and led by the Prime Minister	Disinformation, including foreign interference, has accelerated and is doing damage not only in moments of crisis to our security, but daily to our democratic institutions and social fabric. The current government response to this challenge is fragmented and poorly understood by the public.⁵³ Siloed departments, from MHCLG, the Home Office, Cabinet Office, FCDO and DDCMS are working on democracy and information-threat issues without a coherent strategy or the leadership needed to unlock decision-making. At the centre of this challenge is the Defending Democracy Taskforce, whose Secretariat currently sits within the Home Office. In March 2026, the (recently reappointed) Security Minister Dan Jarvis made a rare statement in the Commons explaining its renewed mandate to tackle “the full spectrum of threats to our democracy.”⁵⁴ In July 2026, DSIT’s responsibilities for information resilience were also consolidated into DDCMS. However, with AI strategy moving to the Cabinet Office there remains ambiguity surrounding who is responsible for tackling the epistemic risks stemming from/ surrounding AI. The Defending Democracy Taskforce should lead a whole-of-government response to democratic renewal. To do so effectively, it requires clear political direction from the centre of government. Placing the Prime Minister at its head, moving it to the Office of the Prime Minister and Cabinet, placing it on a statutory footing and publishing an Information Ecosystems Resilience strategy would send a clear signal that threats to our information environment, which AI is fundamentally transforming, are both critical and urgent - a national challenge requiring sustained leadership and coordination from the highest levels of government. While not all areas of the Taskforce should be made public given the national security concerns, where the Taskforce is leading on matters on democratic resilience, it needs to be accountable to Parliament, allowing the future of our country’s information resilience to be scrutinised by its elected representatives. The Liaison Committee’s scrutiny of the Prime Minister would make a natural home for these sessions to take place. The challenge for any incoming government thinking about Information Ecosystems Resilience policy is the potential for US retaliation given the Trump administration’s open scepticism of the language of “mis/disinformation” and the rejection of online regulation.⁵⁵⁵⁶ Any government must consider this risk in the context of the threat to Britain’s epistemic security.

53 Dewsnap, K. (2026) ‘What is the UK’s Defending Democracy Taskforce?’, The Constitution Society, 18 June. Available at: <https://consoc.org.uk/defending-democracy-taskforce/>

54 House of Commons Debates (2026) ‘Defending Democracy Taskforce’, 12 March. Available at: <https://hansard.parliament.uk/commons/2026-03-12/debates/4ADA5B9F-52B1-4703-96F7-BA8AAB7FB9C6/DefendingDemocracyTaskforce>

55 The White House (2025) Restoring Freedom of Speech and Ending Federal Censorship. Presidential Action, 20 January. Available at: <https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/>

56 Bose, N. and Chiacu, D. (2025) ‘In Munich, Vance accuses European politicians of censoring free speech’, Reuters, 14 February. Available at: <https://www.investing.com/news/world-news/vance-uses-munich-speech-to-criticize-europe-for-censoring-free-speech-3870814>

ACTION	DESCRIPTION
1b) Challenge digital regulators to move further and faster, with greater coordination with government, to match the pace of change happening within the information environment	The Prime Minister should set a clear expectation that the UK's digital regulators move further and faster to respond to technological change and the growing challenges facing the information environment. Alongside this, regulators should work on a shared agenda with the government, working in coordination rather than against, make decisions more quickly, and be held accountable for delivering their statutory responsibilities in a timely manner. Ofcom, the Competition and Markets Authority (CMA), and the Information Commissioner's Office (ICO) all play a critical role in shaping the UK's information environment, but the pace of technological change continues to outstrip the pace of regulation.⁵⁷ Too often, important regulatory decisions take years to implement. For example, Ofcom's work on crisis response protocols only accelerated following a major national crisis, following the fatal stabbing of Henry Nowak, rather than responding to concerns raised by key parliamentary committees.⁵⁸ The consultation for the crisis protocols closed in October 2025, a response was published in July 2026 and the details have yet to be approved by Parliament. Ofcom's original 2024 roadmap to implement the Online Safety Act⁵⁹ provided a more ambitious timeline than what was revised in 2026,⁶⁰ with many measures being pushed back a year to implementation. This resulted in the Secretary of State writing to Ofcom with concerns around delivery of the Terms of Service and user empowerment duties.⁶¹ The Prime Minister should set clear cross-government priorities for digital regulation and expect the Digital Regulation Cooperation Forum (DRCF) to help regulators collaborate better. If the voluntary nature of the DRCF continues to limit its effectiveness, the government should consider placing it on a statutory footing and introducing legal duties for member regulators to cooperate and consult with one another - as recommended by the House of Lords Communications and Digital Committee's 2021 report.⁶² Where regulators consistently fail to meet these expectations, the government should be prepared to commission public body reviews to assess whether governance, leadership, and accountability arrangements remain fit for purpose.⁶³

57 Howes, D. and Gill, M. (2026) 'Digital Regulation Cooperation Forum', Institute for Government, 5 May. Available at: <https://www.instituteforgovernment.org.uk/explainer/digital-regulation-cooperation-forum>

58 Savage, M. (2026) 'UK regulator orders social media firms to adopt measures to stop viral illegal content', The Guardian, 9 June. Available at: <https://www.theguardian.com/media/2026/jun/09/uk-regulator-ofcom-social-media-firms-adopt-measures-stop-viral-illegal-content>; House of Commons Science, Innovation and Technology Committee (2024) Social Media, Misinformation and Harmful Algorithms. UK Parliament. Available at: <https://committees.parliament.uk/work/8641/social-media-misinformation-and-harmful-algorithms>

59 Ofcom (2024) Implementing the Online Safety Act: Progress Update. 17 October. Available at: <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/roadmap/2024/ofcoms-approach-to-implementing-the-online-safety-act-2024.pdf>

60 Ofcom (2023) Ofcom's Approach to Implementing the Online Safety Act. 26 October. Last updated 28 July 2026. Available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation>

61 DSIT (2025) Implementation and Enforcement of the Online Safety Act: Follow-up Letter from DSIT Secretary of State to Ofcom. GOV.UK, 12 November. Available at: <https://www.gov.uk/government/publications/implementation-and-enforcement-of-the-online-safety-act-follow-up-letter-from-dsit-secretary-of-state-to-ofcom/implementation-and-enforcement-of-the-online-safety-act-follow-up-letter-from-dsit-secretary-of-state-to-ofcom>

62 House of Lords Communications and Digital Committee (2022) Digital Regulation: Joined-up and Accountable. 3rd Report of Session 2021–22, HL Paper 126. London: UK Parliament. Available at: <https://publications.parliament.uk/pa/ld5802/ldselect/ldcomm/126/12607.htm>

63 Parris, C., Howes, D. and Gill, M. (2023) 'The public bodies review programme', Institute for Government, 29 November, updated 29 May 2026. Available at: <https://www.instituteforgovernment.org.uk/explainer/public-bodies-review-programme>

ACTION	DESCRIPTION
	While Ofcom's recently appointed Chair should be given a reasonable period to settle into the role, and complete his own review of the workings of the regulator, if meaningful progress is not evident soon, the government should commission such a review. ⁶⁴ Similarly, the CMA's new digital markets regime has taken several years to move from legislation to implementation, despite broad agreement on the need for stronger oversight of the largest technology platforms. ⁶⁵ As a first action, the government should consider issuing a new Strategic Steer to the CMA, backing it to use its powers and reaffirming the regulator's independence.

The new Information Resilience Strategy led by the Defending Democracy Taskforce in the Office of the Prime Minister and Cabinet should cover the following areas (recommendations 2-6) as a priority.⁶⁶ To inform changes for post-2029, the government should consider commissioning an independent review of misinformation and information resilience. Years of debate during the passage of the Online Safety Bill sought to resolve whether 'legal but harmful' content could be captured in legislation.⁶⁷ Those protracted debates never answered this question.⁶⁸ If the government is serious about strengthening information resilience, it should solidify its evidence-base to guide long-term policy and establish a comprehensive independent review with a broad scope that extends beyond online safety legislation to examine the broader drivers, impacts, and governance of misinformation.

2. Building our country's resilience in moments of crisis

Misinformation-fuelled riots are now a regular feature in this country's annual calendar. The Southport riots of 2024, the subsequent riots in Liverpool, and this year's unrest in Southampton and Belfast should provide clear evidence to the government that information crises deserve the same level of seriousness as traditionally understood crises, such as acts of terrorism or natural disasters. Information online no longer stays online, and when unrest spills onto the streets, the government needs to think seriously about how to respond better, faster and in a way that is more coordinated.

64 DSIT (2026) 'Sir Ian Cheshire confirmed as new Ofcom chair', GOV.UK, 3 June. Available at: <https://www.gov.uk/government/news/sir-ian-cheshire-confirmed-as-new-ofcom-chair>

65 McClimont, F. (2025) 'CMA too slow in enforcing new DMCC rules, former official says', Global Competition Review, 22 September. Available at: <https://globalcompetitionreview.com/article/cma-too-slow-in-enforcing-new-dmcc-rules-former-official-says>

66 Our recommendations are not exhaustive. We have not included our recommendations for strengthening local information infrastructure as these will be shared in a dedicated forthcoming paper in September. We have also not shared our thinking on media literacy which is of course also critical, but given detailed focus by colleagues and partners across our Epistemic Security Network and the Media & Information Literacy Alliance elsewhere.

67 Antoniou, A., Woods, L. and Walsh, M. (2024) 'Disinformation and disorder: the limits of the Online Safety Act', Online Safety Act Network, 10 August. Available at: <https://www.onlinesafetyact.net/analysis/disinformation-and-disorder-the-limits-of-the-online-safety-act/>

68 The Conservative government established the Advisory Committee on Misinformation and Disinformation, later renamed the Online Information Committee, sitting within Ofcom to further the policy development of this issue. The National Security Bill began to tackle foreign interference, but limited the debate to misinformation from foreign actors.

TABLE 2
BUILDING OUR COUNTRY'S RESILIENCE IN MOMENTS OF CRISIS

ACTION	DESCRIPTION
2a) Amend the law to designate information crises as part of the Civil Contingencies Framework, enabling coordination between national government, local authorities and civil society during major incidents.	Information crises are not formally recognised within the UK's civil contingencies framework, limiting coordination during moments of heightened risk to more ad-hoc approaches involving government departments, local authorities, and civil society.⁶⁹ The current framework was designed primarily around traditional physical crises - such as pandemics, flooding, terrorism, attacks on or failures of critical infrastructure including 'a system of communication', where there is usually a clear incident, a defined response structure, and established emergency procedures. This approach does not reflect the nature of modern information threats. Disinformation campaigns, foreign interference, and the rapid spread of harmful content often develop over time, rather than in one specific, triggering moment. Such threats can also be covert and go without immediate detection - particularly if enacted by autonomous agents.⁷⁰ Yet their impact can be significant, undermining public trust, increasing social tensions, disrupting democratic processes, and, in some cases, creating direct risks to public safety. A clear example of an information threat affecting public safety was the spread of COVID-19-related disinformation during the pandemic.⁷¹ False claims about vaccines undermined trust in official guidance and contributed to behaviours that increased health risks. Unlike traditional emergencies, the threat developed gradually rather than through a single incident, demonstrating the need for frameworks that can identify and respond to large-scale, 'over-time' information crises. Recognising information crises within the civil contingencies framework would not mean treating misinformation itself as an emergency. Instead, it would provide a clearer mechanism for identifying when information incidents reach a scale capable of causing wider societal harm and require a coordinated response. Just as the existing framework recognises risks that can disrupt essential services and public safety, it should also recognise information threats that can weaken democracy. A new government could amend the Framework without introducing brand new legislation, but rather adding an amendment to any relevant, existing digital regulation legislation passing through Parliament.

69 Cabinet Office (2013) Preparation and Planning for Emergencies: Responsibilities of Responder Agencies and Others. GOV.UK, 20 February. Available at: <https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others>

70 Tidy (2026) "OpenAI says its rogue AI tried to hack other companies" BBC, 29 July. <https://www.bbc.co.uk/news/articles/c2el319vzr3o>

71 Loomba, S. et al. (2021) 'Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA', Nature Human Behaviour, 5, pp. 337–348. Available at: <https://www.nature.com/articles/s41562-021-01056-1>

ACTION	DESCRIPTION
2b) Direct Ofcom to go further and mandate enforcement of platform crisis protocols, including common crisis definitions, severity levels, notification requirements, response timelines and public-interest prioritisation.	The Science, Innovation and Technology Committee, following its inquiry into the handling of misinformation following the 2024 Southport Riots, presented clear evidence that platforms are not going far enough in a crisis.⁷² They demonstrated that during the riots, there was a lack of coordinated, joined-up response from platforms to take action, with each platform taking their own approach because there was no requirement on how to act in this situation. Ofcom itself acknowledged that most services took action, but that the response across the sector was uneven. Part of this issue stems from a lack of definition of what constitutes a ‘crisis’, recognising that crises can happen both on a local and national level, with differing degrees of severity. Ofcom has, slowly, begun to tackle this, publishing their renewed thinking in June 2026 following a consultation on this topic.^{73,74} While they have advanced a definition of a crisis and recognised the need for action to be taken quickly when information escalated most preventatively,⁷⁵ the scope remains narrow. Ofcom has explicitly excluded misinformation from the definition of a crisis, despite the SIT Committee recommending it be included from the outset, because it is not part of the Online Safety Act.⁷⁶ Search services are excluded entirely, on the basis that Ofcom sees little evidence they drive virality during a crisis, instead keeping the platforms in scope to user-to-user services. The voluntary nature of the platform crisis protocol limits any major progress, as platforms can still choose whether or not to partake. Compliance is not itself mandatory. Nor is the protocol yet in force; it still awaits parliamentary approval, more than a year and a half after the Committee first raised the issue. A new government should expedite this work, and make compliance mandatory via an amendment to the OSA, before another crisis plagues our country.

72 House of Commons Science, Innovation and Technology Committee (2024) Social Media, Misinformation and Harmful Algorithms. UK Parliament. Available at: <https://committees.parliament.uk/work/8641/social-media-misinformation-and-harmful-algorithms/>

73 Ofcom (2025) Online Safety – Additional Safety Measures. Consultation, 30 June. Available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/online-safety-additional-safety-measures>

74 Ofcom (2026) Statement: Crisis Response Protocol. 9 June, updated 18 June. Available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-crisis-response-protocol>

75 Lyall, S., Hancock, J. and Perry, H. (2025) Ofcom Consultation Response: Additional Safety Measures for Online Platforms. London: Demos, 23 October. Available at: <https://demos.co.uk/research/ofcom-consultation-response-additional-safety-measures-for-online-platforms/>

76 Ofcom (2026) Crisis Response Protocol: Online Safety – Additional Safety Measures. Statement, 9 June. Available at: <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/protecting-children/illegal-harms/crisis-response-protocol-online-safety-additional-safety-measures.pdf?v=419248> p.16

ACTION	DESCRIPTION
2c) Publish a Government Information Crisis Response Protocol setting out how incidents are identified, assessed and responded to by both government and platforms.	The UK lacks a democratically accountable mechanism for the government to notify the public about information incidents - not just during elections, but during any crisis where false or misleading information threatens public safety, from civil disorder to public health emergencies. Information voids are a key driver of mistrust during crisis moments. They are exacerbated even further during ‘information crises’ such as riot-inciting misinformation, deepfakes, or election-related disinformation. There is no clear, publicly understood framework for how the government and platforms should <i>together</i> respond during acute information incidents. General crisis machinery does exist. The Rapid Response Unit, the National Security Online Information Team, the Joint Election Security Preparedness Unit and the Defending Democracy Taskforce each hold some responsibility for monitoring and responding to information incidents, and Ofcom’s own crisis response protocol now places specific duties on platforms.⁷⁷ But, none of these bodies operate under a single, published protocol governing how the government itself responds to an information crisis, or how it coordinates with platforms while doing so. A Government Information Crisis Response Protocol should be the Defending Democracy Taskforce’s first priority under its new mandate, setting out a clear, transparent agenda that demonstrates to the public that the government can grip problems head-on and has a plan in place for when the next crisis occurs. The Protocol should look to Canada’s Critical Election Incident Public Protocol, while narrower in scope, it offers a template worth adapting: a published definition of an incident, a named body responsible for declaring one (a panel of senior officials), a minimum threshold for declaration, human right obligations, defined intelligence-sharing arrangements, and public reporting.⁷⁸

⁷⁷ Cabinet Office and Dowden, O. (2019) ‘Update on tackling intimidation in public life’, GOV.UK, 5 November. Available at: <https://www.gov.uk/government/speeches/update-on-tackling-intimidation-in-public-life>; Demos (2026) The Representation of the People Bill: Epistemic Security Briefing. London: Demos, May. Available at: https://demos.co.uk/wp-content/uploads/2026/01/ESN-Crisis-Coalition_Election-Bill-briefing-polling-update-May-2026.pdf

⁷⁸ Government of Canada (2025) Critical Election Incident Public Protocol. Democratic Institutions, 13 March. Available at: <https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html>

3. Safeguarding our elections against digital information threats

Tackling the vulnerabilities in our elections doesn’t need to be a challenge left for future years - amending existing legislative proposals would make strong steps towards addressing this issue now. The passage of the Representation of the People Bill has, thus far, been a missed opportunity to safeguard elections against digital information threats that now feature more commonly in election campaigns. And there is broad, loud, backbencher support for the government to go further.⁷⁹

When setting out the intention for the Bill, the government’s elections strategy states that “our own democracy is being threatened by misinformation”,⁸⁰ but the Bill falls short in addressing this. The government has the legislative vehicle already in place to act, and it should commit to bringing forward these amendments within its first months at the dispatch box, making clear: our elections are not open for interference.

TABLE 3
SAFEGUARDING OUR ELECTIONS AGAINST DIGITAL THREATS

ACTION	DESCRIPTION
3a) Utilise the passage of the Representation of the People Bill to go further and tackle digital threats to elections.	The Representation of the People Bill was first introduced as the legislation to deliver Labour’s manifesto commitment to lower the voting age. But the opportunity to use this Bill as a legislative vehicle to go further than its originally intended scope has now been widely recognised across prominent figures within the Labour Party, including by Deputy Leader of the Party Lucy Powell⁸¹ and former Democracy Minister Rushanara Ali.⁸² In the digital age, elections and candidates are increasingly vulnerable to AI-generated deepfakes, false claims, coordinated manipulation, and online abuse. These threats can undermine public trust, distort democratic debate, and deter people, particularly women and representatives from minority communities, from participating in politics.⁸³ The Representation of the People Bill provides a timely legislative vehicle to address these vulnerabilities within the new government’s first 100 days. Amendments have already been tabled first at Committee Stage and again at Report Stage by Emily Darlington MP, and now also by Lucy Powell, to give the government a suggestion on where to go further.

79 Brown, A. (2026) ‘Lucy Powell says social media giants must face strict election rules to protect votes’,The Mirror, 4 July. Available at: <https://www.mirror.co.uk/news/politics/musk-social-media-powell-elections-37386850>

80 Cabinet Office (2025) Strategy for Elections. London: HM Government. Available at: https://data.parliament.uk/DepositedPapers/Files/DEP2025-0503/STRATEGY_FOR_ELECTIONS.pdf

81 Brown, A. (2026) ‘Lucy Powell says social media giants must face strict election rules to protect votes’,The Mirror, 4 July. Available at: <https://www.mirror.co.uk/news/politics/musk-social-media-powell-elections-37386850>

82 Stacey, K. (2026) ‘Andy Burnham urged to overhaul “timid and limited” elections bill’, The Guardian, 15 July. Available at: <https://www.theguardian.com/politics/2026/jul/15/andy-burnham-strengthen-elections-bill>

83 Perry, H., et al. (2026) Epistemic Security Briefing: The Representation of the People Bill. London: Demos, 12 January, updated 29 May 2026. Available at: <https://demos.co.uk/research/epistemic-security-briefing-the-elections-bill/>

ACTION	DESCRIPTION
	The Bill was due to complete its Commons stages before summer recess, but a delay in voting means it now has a clear opportunity to be redrafted.⁸⁴ Should the passage of the Bill not be the government's preferred mechanism, they should swiftly work to strengthen digital election law through other means. Three targeted reforms would strengthen the integrity of UK elections:⁸⁵ • Clarify how electoral law applies to AI-generated deepfakes and synthetic text intended to mislead voters or misrepresent candidates. • Introduce an Elections Code under the Online Safety Act through the Bill to address online threats, abuse, and harmful content targeting candidates during election periods. This includes a transparency and access data duties, changes to recommendation systems to reduce amplification of hateful and harassing content, and requirements to offer candidates a high standard of customer service, such as human-managed hotline.⁸⁶ • Require online platforms to submit all paid political advertisements to a central, publicly accessible advertising repository, enabling voters, journalists, and researchers to scrutinise political advertising and verify campaign messaging.
3b) Introduce legislation to safeguard elections and the information environment from AI chatbot risks	AI chatbots and search summaries are rapidly becoming an influential source of information for the public, shaping how people understand events, make decisions and navigate everyday life. However, these systems remain subject to limited obligations around accuracy, transparency, accountability and disclosure of how responses are generated. This creates growing risks from misinformation, hallucinations and foreign interference, particularly during elections. Recent research demonstrates the scale of the challenge. Testing of leading AI chatbot services during the 2026 Scottish pre-election period found that 34.1% of responses contained factual errors, including incorrect information about election dates and voter ID requirements, fabricated candidates and entirely false claims about political scandals.⁸⁷ Separate research has also identified repeated citations of sanctioned foreign information manipulation and interference assets across major AI chatbot services, demonstrating how hostile actors can exploit vulnerabilities in large language models.⁸⁸

84 Penna, D. (2026) 'Starmer's voting reforms delayed ahead of Burnham takeover', The Telegraph, 13 July. Available at: <https://www.telegraph.co.uk/politics/2026/07/13/starmer-representation-of-the-people-bill-delayed-burnham/>

85 Perry, H., et al. (2026) Epistemic Security Briefing: The Representation of the People Bill. London: Demos, 12 January, updated 29 May 2026. Available at: <https://demos.co.uk/research/epistemic-security-briefing-the-elections-bill/>

86 For further information on what this Elections Code would include see this draft led by OSA Network and co-developed with a number of civil society organisations: https://www.onlinesafetyact.net/documents/1224/Draft_code_of_practice_for_improved_online_safety_for_candidates_during_elections.pdf

87 Hancock, J. and Moores, A. (2026) Electoral Hallucinations: Safeguarding UK Elections in the World of LLMs and AI Chatbots. Demos, 20 May. Available at: <https://demos.co.uk/research/electoral-hallucinations-safeguarding-uk-elections-in-the-world-of-llms-and-ai-chatbots/>

88 Miller, C., Perry, H. and Devine, F. (2026) GEO for Geopolitics: What Happens When AI and Information Warfare Collide. London: Demos, 27 July. Available at: <https://demos.co.uk/research/geo-for-geopolitics-what-happens-when-ai-and-information-warfare-collide/>

ACTION	DESCRIPTION
	The government should use the next AI legislation to establish a clear regulatory framework for AI chatbots, with enhanced requirements for pre-election windows. The government should start by legislating to set a minimum standard of safeguards to be applied on text-based AI services at all times, this should cover risk assessments, transparency reporting, minimum safety standards, and duties relating to accuracy and bias. These requirements should then be heightened during the pre-election window, requiring text-based AI services to implement guardrails against harmful and malicious uses and to implement enhanced election resourcing. Legislation should also require greater transparency and data access for regulators and independent researchers, enabling scrutiny of how AI systems operate and their impacts on the information environment. AI providers should be required to prevent outputs that amplify sanctioned foreign information manipulation and interference assets, while supporting the development of detection technologies, watermarking and cross-industry standards to help citizens identify AI-generated content. Without clear obligations, AI systems risk becoming powerful but unaccountable sources of information, leaving democratic processes vulnerable to both accidental errors and deliberate manipulation.

4. Improving the discoverability, attribution and trustworthiness of high quality information

Strengthening and reforming the UK's media landscape for the digital era is undoubtedly a vital part of our safeguarding the vulnerabilities in our information supply chain. This work has already begun, with proposals made on how to fortify the BBC and how to increase the visibility and discoverability of public interest news sources published by DDCMS already. But other areas of policy still need new thinking, renewed consensus building, and brand new legislation to tackle the challenges the information environment faces.

TABLE 4

IMPROVING THE DISCOVERABILITY, ATTRIBUTION AND TRUSTWORTHINESS OF HIGH QUALITY INFORMATION

ACTION	DESCRIPTION
4a) Ensure the BBC's Charter Review strengthens its independence and public accountability in order to safeguard its future	In an era of information warfare, global democratic backsliding and domestic polarisation, it is essential that the BBC's independence from political interference is protected, while its accountability to the public it serves is strengthened. The ongoing Charter Review will complete in 2027 providing the framework through which to strengthen the BBC. The Renewal process, including the publication of the government's <i>Britain's Story: The Next Chapter</i> Green Paper, has already made important progress, but there remains a risk that reforms are not ambitious enough to match the size of the risks facing the UK's democracy and the BBC's reputation, reach and impact.⁸⁹ It's vital that any government continues to build on existing momentum and ensure the BBC remains resilient, trusted and fit for the challenges ahead.⁹⁰ Propose in the first 100 days via DDCMS White Paper: • Remove the 10-year Charter expiry date: Entrench the BBC's Object, Mission, Public Purposes, independence and universality in a perpetual, simplified Charter, amendable only by a "public lock" (one-off Citizens' Assembly plus a parliamentary majority). • End political appointments to the BBC Board. Replace it with an Independent Appointments Commission with CMS Select Committee input (for Chair only), and create an Independent BBC Funding Commission. • Embed representative public accountability in the BBC's governance through a Standing Citizens' Panel with bounded over strategic priorities and financial plans.

89 DCMS (2025) Britain's Story: The Next Chapter – BBC Royal Charter Review, Green Paper and Public Consultation. London: UK Government, 16 December. Available at: <https://www.gov.uk/government/consultations/britains-story-the-next-chapter-the-bbc-royal-charter-review-green-paper-and-public-consultation/britains-story-the-next-chapter-bbc-royal-charter-review-green-paper-and-public-consultation>

90 Padania, S., Perry, H. and Curtis, P. (2026) Our BBC: A Blueprint for a More Independent and Future-Proofed BBC. London: Demos, 21 January. Available at: <https://demos.co.uk/research/our-bbc-a-blueprint-for-a-more-independent-and-future-proofed-bbc/>

ACTION	DESCRIPTION
4b) Introducing statutory prominence requirements for public service broadcasters on video-sharing platforms such as YouTube and TikTok for content of high civic value.	The government should create a new regime requiring video-sharing platforms to give prominence to PSB content of highest civic value on video-sharing platforms through measures to increase algorithmic prominence, or user interface design. These prominence measures recognise the important role that public service media plays in a healthy democracy when they operate according to their fundamental principles of accountability, accessibility, impartiality, independence, pluralism, reliability, and universalism. Additionally, PSBs still remain the most used and trusted sources of news for UK audiences. The Government's Green Paper, <i>Watch this Space</i>, leaves an open question as to whether this should be introduced via new legislation or encouraged through voluntary agreements. Prominence should not be left solely to voluntary agreements with platforms. While platforms have an important role to play in improving the visibility of public interest information, voluntary approaches are not subject to a public interest test and do not provide sufficient guarantees that citizens' access to trusted, diverse and high-quality information will be prioritised. These new rules must be underpinned by democratic and accountable governance, including co-regulatory oversight, robust appeals mechanisms, algorithmic transparency, and access to platform data for independent scrutiny.
4c) Legislating for algorithmic prominence of diverse public interest information on social media platforms	While there is significant policy debate about how to tackle harmful and misleading content, there must also be a strong focus on promoting the visibility of high-quality, trustworthy information. As people increasingly consume news through digital platforms, the challenge is not simply whether trustworthy and locally relevant information exists, but whether citizens can find it. Social media feeds, search engines and recommendation systems now play a significant role in determining what information people encounter, yet these systems – which are largely owned by US Big Tech companies – do not always prioritise or even ensure inclusion of accurate, reliable, locally relevant or public interest content. The government has already published a Green Paper, <i>Watch this Space</i>, with consultation closing on 31 August, to begin laying the groundwork for this agenda.⁹¹ A priority for the next King's Speech should be legislation that extends the prominence rules that apply to linear television into the social media platform environment.

91 DCMS (2026) *Watch This Space: A New Strategic Direction for UK Media – Green Paper and Public Consultation*. London: HM Government, June, updated 29 July 2026. Available at: <https://www.gov.uk/government/consultations/watch-this-space-a-new-strategic-direction-for-uk-media-green-paper-and-public-consultation/watch-this-space-a-new-strategic-direction-for-uk-media-green-paper-and-public-consultation>

ACTION	DESCRIPTION
4d) Commit to creating a robust, independent and transparent regime to define what information or provider should be considered as “in the public interest”, as part of the Green Paper proposals.	One of the greatest challenges in extending a prominence regime is deciding which information should be elevated, how those decisions should be made, and who should oversee the process. Any system for allocating prominence must balance several competing considerations. It should operate with sufficient independence from the government to safeguard press freedom, while also remaining independent of platforms so they are not left to determine which publishers or information benefits. At the same time, the criteria for allocating prominence should be clear, objective and transparent, without being prescribed by the government in a way that risks creating a de facto system of press regulation. Any definition will need public legitimacy. Eligibility for ‘public interest’ information should be based on a transparent, independently developed framework, overseen independently from government via a coregulatory body.⁹² This framework should provide a number of parameters that assess publishers against objective indicators of quality editorial processes, procedural fairness, and governance arrangements that are transparent, accountable and responsive to the public. The process to demonstrate these indicators should be led by the publishers themselves. A useful technical precedent to understand a parameters based model is the Journalism Trust Initiative (JTI), developed by Reporters Without Borders (RSF). The JTI uses more than 130 indicators to assess the trustworthiness of media organisations and has been adopted by over 2,400 media outlets across 127 countries.⁹³ While the specific criteria for a UK prominence regime would need to reflect the domestic media landscape, the JTI demonstrates how a parameter-based approach can provide a credible and scalable alternative to subjective platform moderation or direct government designation. To ensure the governance of a prominence regime avoids direct government oversight, or reliance on existing press regulation bodies, the regime should instead be overseen by a co-regulatory body. Co-regulation offers a model of collaborative governance, combining independent oversight with input from industry and expert stakeholders. This can help ensure accountability while avoiding excessive government control over decisions about which content should be prioritised. Independent oversight should also extend to the processes used to determine what content qualifies as “public interest,” and therefore merits prominence. These decisions should be subject to regular review, with transparency requirements and public reporting on the outcomes of the regime.

⁹² Demos (2026) Boosting Prominence of Public Interest Media FAQ. Epistemic Security Briefing. London: Demos, 22 June. Available at: https://demos.co.uk/wp-content/uploads/2026/06/Demos_-Prominence-QA.pdf

⁹³ Journalism Trust Initiative. Reporters Without Borders (RSF). Available at: <https://journalismtrustinitiative.org/>

ACTION	DESCRIPTION
4e) Review opportunities for greater cohesion and clarity across digital regulation for content that is produced by professional journalists and content creators, and broadcast, streamed, published on demand or distributed by a newspaper publisher	The UK's broadcasting regulatory framework is increasingly out of step with the realities of a converged media environment. The distinction between broadcast and online content has become harder to sustain as audiences consume news and current affairs across television, streaming services, broadcaster websites, and social media platforms. Regulation is fragmented, with each medium being regulated differently, despite content moving between platforms. The distinction between content produced by professional journalists compared to citizens and content creators is also less well understood. Rather than narrowly pursuing piecemeal reforms in specific parts of the system, the scale of the technological evolution and democratic emergency is such that there is a need to pause, step-back and ask uncomfortable questions. Do existing standards across different regulatory regimes need to be redrafted to provide better alignment and consistency across digital media regulation? Is regulation based on the method of production or <i>distribution</i> of the content fit for purpose in a digital age, or are there benefits to moving more towards a framework based on regulating the <i>content itself</i> that could be gleaned whilst recommitting to and maintaining crucial principles of press freedom and freedom of speech? We are not reaching any conclusions here, but believe the urgency of the epistemic crisis is forcing us to ask the most difficult and contested questions now.
4f) Empower the Digital Labelling Taskforce to inform future legislation surrounding deepfakes and AI chatbot text-based outputs	The challenge of tackling deepfakes, or, as DSIT had termed them, "digital replicas," is now being addressed through two parallel strands of work. The government has committed to launching a consultation on digital replicas, seeking views on how to address harms where someone's likeness is replicated without their permission via image, audio or other likeness. Alongside this, it is establishing a taskforce on AI labelling, tasked with putting forward proposals on best practice for labelling AI-generated content, with an interim report due in autumn 2026.⁹⁴ This work is vital, first, for examining how deepfakes are polluting the wider information environment. The scale of the problem underlines the urgency: around eight million deepfakes were shared in 2025, compared with just half a million two years earlier.⁹⁵

94 Kendall, L. (2026) 'Copyright and AI Progress', UK Parliament: Written Statements, HCWS1416, 18 March. DSIT. Available at: <https://questions-statements.parliament.uk/written-statements/detail/2026-03-18/hcws1416>

95 Government Office for Science (2026) 'Science-led collaboration against deepfakes', GOV.UK, 19 February. Available at: <https://www.gov.uk/government/case-studies/science-led-collaboration-against-deepfakes>

ACTION	DESCRIPTION
	While the scope of the Taskforce will likely need a reset with a new Ministerial team - it is important that consideration should also be given for accurate and clear citation standards for textual information represented in LLM-powered AI service outputs where a lack of clear attribution undermines users' ability to effectively evaluate the quality of the information - broadly known as 'provenance'. The taskforce, and the consultation running alongside it, should work at pace, bringing together leading experts to develop recommendations that can inform the government's next round of legislative proposals, especially given the gap in AI legislation, there is a need for stronger recommendations on how to tackle this threat.⁹⁶

5. The British Innovation Challenge: Epistemic Sovereignty

The threats represented by the concentration of private tech company influence, foreign dependencies and unaccountability are now well-recognised. Whilst some have emphasised the role of the Competition and Markets Authority and competition to tackle this threat (as do we - see Recommendation 1b), others have focused on developing the alternatives that can compete - doubling down on 'sovereignty'. Fundamentally sovereignty is about autonomy and agency - choice over what we use and rely on, influence in shaping how that is formed, and guaranteed access to what we need.⁹⁷ In this context, epistemic sovereignty means having autonomy and agency over the UK's 'Epistemic Stack' - the tools, platforms, and infrastructure that make up the information supply chain - without requiring compromises on our values as a democracy.⁹⁸

If we do not have Epistemic Sovereignty, then we are far more vulnerable to all manner of threats, including leverage to weaken legislation, weak content moderation standards, foreign interference, and the risks of losing access to information when we need it most. We also miss critical opportunities to not only avoid harm, but to proactively strengthen our democracy at a time of acute vulnerability. The following recommendations will be expanded further in a forthcoming paper in autumn 2026.

⁹⁶ Rough, E. (2026) AI Regulation in the UK. House of Commons Library Research Briefing, 10 June. Available at: <https://commonslibrary.parliament.uk/research-briefings/cbp-10003/>

⁹⁷ DSIT's definition is currently in development.; Sheikh (2022) "European Digital Sovereignty: A Layered Approach", Digital Society 1, (3). <https://link.springer.com/article/10.1007/s44206-022-00025-z>

⁹⁸ We deliberately refer here to 'sovereignty' and not 'digital sovereignty'. Whilst digital sovereignty is interdependent with 'epistemic sovereignty', there are aspects of the 'Epistemic Stack' which are not digital and aspects of 'digital sovereignty' which are not as high a priority for information ecosystems.

TABLE 5
THE BRITISH INNOVATION CHALLENGE: EPISTEMIC SOVEREIGNTY

ACTION	DESCRIPTION
5a) Develop a national ‘Epistemic Sovereignty’ action plan that articulates a positive vision for British digital innovation for the UK’s information environment, clarifies priorities and facilitates multi-level collaboration to catalyse and guide momentum	Strengthening the UK’s Epistemic Sovereignty requires a multi-level (international, national, regional and local) coordinated effort involving policy, infrastructure development and resources, from public, private, philanthropic and civil society actors across the interconnected Epistemic Stack. Leadership and coordination is crucial to ensuring initiatives tackle the scale of the challenges in the information environment, clarifies priorities and facilitates multi-level collaboration to catalyse and guide momentum. DBIST, in collaboration with the AI Minister and DDCMS, should take on this leadership role, developing and launching an action plan for Epistemic Sovereignty in order to strengthen the level of autonomy and democratic values alignment among infrastructure, platforms, software and algorithms vital to UK citizens within our information supply chain. This should be informed by: (i) Identifying and articulating the key UK democratic values and goals as it pertains to the information environment that technological developments should align to, including how these contribute to economic growth, civic participation, social cohesion, health and arts and culture - led by an independent partner such as The Responsible Innovation Centre (hosted by BBC R&D). These could be inspired by, for example, articulations of a positive digital public sphere and principles identified to guide European digital sovereignty with considerations for independence, transparency and accountability as well as de-proprietarisation and interoperability.⁹⁹ (ii) Evaluating the levels of digital autonomy and agency across the ‘Epistemic Stack’ combined with considerations for different types of risk and levels or risk exposure, informed by assessments of elements already categorised as Critical National Infrastructure, risks noted as chronic in the National Risk Register and indices such as the ‘Digital Dependence Index’.¹⁰⁰ This insight can then influence the prioritisation for policy, as well as funding for tech development and other strategies. By taking a leading role on this agenda for the UK, DBIST can also provide a clear engagement point for facilitating international alliances on behalf of the UK government.

99 Unterberger and Fuchs (2021) “The Public Service Media and Public Service Internet Manifesto.” London: University of Westminster Press. Available at: https://www.jstor.org/content/oa_book_edited/j.ctv26qjkk ; Giannelos (2023) “Recommendations for a Healthy Digital Public Sphere.” *Journal of Media Ethics* 38.2: 80-92; Jay (2024) The Possibilities of a ‘Public Service’ Intervention to Support a Good Digital Society, The British Academy. doi.org/10.5871/digitalsociety/9780856726965.001; Bria, Timmers, Gernone (2025): EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung. Gütersloh. https://assets.filedock.xyz/public/EuroStack_2025.pdf

100 Mayer & Lu (2023) “Digital Autonomy? Measuring the Global Digitance Dependence Structure.” <https://digitaldependence.eu/en/>; UK Gov; (2025) “National Risk Register” https://assets.publishing.service.gov.uk/media/67b5f85732b2aab18314bbe4/National_Risk_Register_2025.pdf (p18-19)

ACTION	DESCRIPTION
5(b) Strengthen the funding ecosystem that can facilitate greater digital innovation for Epistemic Sovereignty, including new alternative digital pro-social spaces particularly for local communities	Efforts to support digital innovation in the UK information ecosystem are under-funded, fragmented and structurally disconnected from many of the funders and investors that could transform and sustain it. A combination of efforts targeting different aspects of the Epistemic Stack are needed to tackle the size of the existing gaps, the urgency of this issue and to unlock the benefits of a diverse ecosystem of innovation. DBIST should catalyse these funding initiatives guided by the prioritisation and goals set-out by the broader Epistemic Sovereignty action plan. This could include: (i) Launching a new UK Advanced Research & Invention Agency (ARIA) programme to shape and incentivise experiments that strengthen Epistemic Security, with a specific workflow that targets Epistemic Sovereignty - connecting with existing initiatives to strengthen 'trust infrastructure' and 'collective flourishing'.¹⁰¹ (ii) Take inspiration from the UK Sovereign AI fund and launch a dedicated Epistemic Sovereignty equity investment fund to incentivise development that is aligned with and contributes to the Epistemic Stack specifically. (iii) Support a Venture Studio supporting experiments and scaling for-profit and non-profit winners that unlock connection and trust via new types of information actor, e.g. local media cooperatives, minority language networks, to experiment with new forms of open source AI or building new social media platforms.¹⁰² This should be hosted by a trusted host, independent of government, like the BBC, Nesta, or a UKRI Catapult. Taking inspiration from the likes of, the New Media Studio or New Public's Public Spaces Incubator. (iv) Launch an International Epistemic Sovereignty Alliance and Fund with middle power allied democracies, including public, philanthropic and private investment to invigorate a new era of UK innovation for the 'Epistemic Stack'.¹⁰³ Such investment would be a key pillar of meeting allied nation's NATO defence commitments to enhance civic resilience.¹⁰⁴ It could facilitate data portability frameworks, algorithmic transparency requirements, shared testing facilities and even a common market that reduces the dominance of US and Chinese technology firms.

101 ARIA (2026a) 'Trust Everything, Everywhere'. <https://aria.org.uk/opportunity-spaces/trust-everything-everywhere/> ; ARIA (2026b) 'Collective Flourishing', <https://aria.org.uk/opportunity-spaces/collective-flourishing/>

102 Curzon Price (2026) "How to fix the 'enshittification' of the public sphere". https://media.nesta.org.uk/documents/How_to_fix_the_enshittification_of_our_digital_public_sphere_nV0oEtM.pdf; IPPR (2026) "Stuck on you: How to make social media good again." <https://ippr-org.files.svdcdn.com/production/Downloads/Stuck-on-you-April-26.pdf>

103 Turobov (2025) "What does AI sovereignty for the UK involve". <https://www.bennettschool.cam.ac.uk/blog/what-does-ai-sovereignty-for-the-uk-involve/>

104 NATO Summit (2025) Overview - 2025 - Key Decisions - <https://www.nato.int/en/news-and-events/events/2025/6/overview---2025-nato-summit-in-the-hague>

6. Revitalising Local Information Digital Places and Spaces

The health of a community's local information ecosystem - from the quality of its local news provision, to the moderation of local Facebook, WhatsApp, and Nextdoor groups, to the visibility of local Council's updates - is critical to the public's sense of belonging among their neighbours, pride in their place and sense of agency as active citizens. The government has launched several important initiatives, including the Pride in Place programme and the Amplify: Local Media Action Plan. This includes the £12m Local News Fund which Demos previously argued for is currently underway, will be evaluated and, if successful, should be scaled up. Yet the role of local information (not just news) and institutional communication, their level of ambition for innovation, financial sustainability, and spaces and places for citizen connection and deliberation, have so far been underrecognised. The recommendations 5a and 5b highlight opportunities to diversify the types of digital spaces available to communities at the local and national level.

TABLE 6
REVITALISING LOCAL INFORMATION DIGITAL PLACES AND SPACES

ACTION	DESCRIPTION
6a) As part of a new devolution strategy, funding should be allocated to create a programme of local and regional government pilots that reimagine and boost the visibility and responsiveness of their communications in shared local digital spaces	Strengthening the relationship between local democratic institutions and local citizens is critical to rebuilding engagement and trust in the state overall. Yet, the lack of engaging and throughcutting information made available by local democratic actors - from councils, to local MPs and mayors - in the digital spaces where communities spend time, particularly during moments of crisis or heightened vulnerability, is leaving voids not just of information, but connection. Over the last decade, sustained financial pressures have undermined councils communications capacity. They lack the methods, resources or support for effective communication in a digital age that meets the needs of local audiences. The lack of resources to prioritise this area combined with the now more polarised and in some cases hostile community environment is undermining the confidence and level of ambition among local governments to experiment with new approaches. If the new Prime Minister is committed to devolving power beyond the capital and into local communities, one of the most important areas for a devolution agenda must be empowering local government and local leaders to innovate in the ways they communicate and connect with their communities. Without rebuilding trust in the actions of and information shared by local public institutions, a devolution agenda could struggle to fully capture the support of and engagement within communities across the UK. As part of a new devolution strategy, in the style of the Pride in Place programme, new pilot funding should be allocated to identifying key places where experiments in the local governments' approach to communications with its community is in dire need. MHCLG already provides ad hoc resilience funding for 'tackling mis/disinformation' and therefore should have good insight into where vulnerabilities remain across the country. Funding should be used to enable councils

ACTION	DESCRIPTION
	to map their local information ecosystem to understand where information and connection is needed amongst local people, improve their visibility where it matters and experiment with new forms of engagement with key community voices and catalysts. These learnings should be utilised not only in moments of crisis - although integration into crisis response is key - but in the everyday practice of local government. A Community of Practice surrounding this initial cohort could be used to share learning across the UK.
6b) MHCLG and philanthropic funders in partnership with the VCFSE sector should strengthen local digital spaces and connection by focusing on understanding and supporting the needs of local Facebook, WhatsApp and Nextdoor group admins, in key communities to strengthen their moderation standards and relationships with other key local community actors	Local digital spaces - often in the form of local Facebook, WhatsApp and Nextdoor groups - are now a foundation of how local communities learn about what is happening in their place and connect with other locals. These spaces are administered by a broad range of people and have become critical local community actors, yet they are under-recognised in our understanding of local information flows and community connection. These community catalysts - often every-day citizens, or sometimes local journalists, civil society actors, or even elected officials - have immense influence over what is seen and discussed and who is allowed to engage in these local spaces and in what way. However, our understanding of their needs, motivations and approaches in these spaces is limited. Frequently local group administrators' relationships with other key community actors such as local news media, the council, the police or the NHS are informal if they exist at all. Such community actors deserve not just greater recognition for the democratic contribution they are making in their communities, but greater connection and support, particularly in moments of crisis or community tension where the pressure of holding such a key role can take its toll on these, often untrained and unsupported, people. The new devolution strategy, MHCLG and a cohort for philanthropic funders should: i. Identify a mix of communities across the UK that allow for considerable diversity in terms of region, current political representation and structure of local/ regional government, social demographics, and environment e.g. urban, peri-urban, rural. - ii Fund VCFSE sector organisations in these communities who have strong relationships and trust to engage a selection of local digital group administrators who are open and willing to join a local peer network and to co-develop a set of local community practices for an approach to moderating these groups. This could also prioritise engagement and connection with other local community information producers, providing key actors an insight into how these spaces work and foot in the door to start building trust there. iii. Evaluate what works in the introduction of these peer networks and approaches to local digital group standards development/ 'best practice' and any associated training that could accompany it. Use such insight to inform guidance for other initiatives that could be funded in communities across the country.

7. Ready for the next frontier of information warfare: the foreign manipulation of LLMs

The emergence of LLM-powered AI services is going to provide the new frontier of information warfare. From chatbot environments used by hundreds of millions, to AI-mediated search, AI companions, synthetic content ecosystems and embedded agents, it is clear that they will be too valuable and epistemically consequential to be ignored by information influence practitioners. Given the evidence that Russian state actors are already manipulating LLMs through the fabrication and manipulation of source material designed to be retrieved by AI systems at query time - Britain is already ceding asymmetrical advantage to autocratic states at this critical epistemic layer.¹⁰⁵ Members of the Defending Democracy Taskforce, including the Home Office, DDCMS, the AI Minister, and the FCDO all have an important role to play in tackling this threat.

TABLE 7
READYING THE NEXT FRONTIER OF INFORMATION WARFARE: THE FOREIGN MANIPULATION OF LLMS

ACTION	DESCRIPTION
7a) The Defending Democracy Taskforce should ready UK government departments to mitigate against the specific risk of foreign manipulation of LLMs (RAG poisoning) via disrupt regimes.	Existing government guidelines for securing AI systems suggest that whilst there is an awareness of the risks of untrustworthy LLM outputs being caused by biases in the training data, less attention is paid to the risks created through ‘RAG poisoning’ i.e. the ability to influence models by amending the live data they retrieve when augmenting their results by searching the internet in real-time.¹⁰⁶ Where attention has been paid to this threat in the public domain by a small number of journalists, concern has largely focused on the risks to market competition and scams, rather than as a state threat.¹⁰⁷ In contrast, pioneering members of the counter-FIMI community have been gathering early evidence of the salience of FIMI assets in AI.¹⁰⁸ DDCMS and other members of the Defending Democracy Taskforce, together with the new AI Minister and Cabinet Office, should ensure all guidelines and practices are updated to explain the specific risk of RAG poisoning and to coordinate activity to disrupt and deter RAG poisoning by adversarial actors with the European External Action Service.

105 Demos (2026) GEO for Geo-politics. <https://demos.co.uk/research/geo-for-geopolitics-what-happens-when-ai-and-information-warfare-collide>

106 NCSC (2023) “Thinking about the security of AI systems”. <https://www.ncsc.gov.uk/blog-post/thinking-about-security-ai-systems>; GDS & DSIT (2025) “Artificial Intelligence Playbook for the UK Government”. https://assets.publishing.service.gov.uk/media/67aca2f7e400ae62338324bd/AI_Playbook_for_the_UK_Government__12_02_.pdf; Government Digital Service (2026) “AI Insights: Prompt Risks”. <https://www.gov.uk/government/publications/ai-insights/ai-insights-prompt-risks-html>

107 Menn (2025) “Russia seeds chatbots with lies. Any bad actor could game AI the same way”<https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/>; Kirmer (2025) “Data Poisoning in Machine Learning: Why and How People Manipulate Training Data”. <https://towardsdatascience.com/data-poisoning-in-machine-learning-why-and-how-people-manipulate-training-data/>

108 See the excellent work conducted by the American Sunlight project (<https://www.americansunlight.org/updates/the-american-sunlight-project-unveils-detailed-report-on-the-critical-threat-of-russian-disinformation-in-ai-models>), Newsguard (<https://www.newsguardtech.com/ai-monitor/march-2025-ai-misinformation-monitor/>), DFR Lab (<https://dfrlab.org/2026/04/08/pravda-in-the-pipeline/>) and ISD (<https://www.isdglobal.org/digital-dispatch/investigation-talking-points-when-chatbots-surface-russian-state-media/>)

ACTION	DESCRIPTION
7b) The FCDO and the counter-Foreign Information Manipulation & Interference community (academics, civil society) should collaborate across government and across society to ensure accurate counter-FIMI information is visible in LLM-powered services	It is critical that responsible public actors do not cede the terrain of LLMs to malign state actors. The entire ecosystem of scrupulous information producers are already grappling with the most appropriate way to ensure visibility in LLM-powered AI services whilst maintaining necessary copyright protections, fair value exchange, sufficient attribution and in a way that is consistent with their standards and values. It is notable that some information producers are already adopting Generative Engine Optimisation techniques to facilitate AI agent-readability, even those who have rejected the prospect of negotiating licensing deals with AI companies. The Economist is one such example who have created a dual site for their marketing and B2B sales material that is restructured for AI. However, there exists a range of open access high quality information that is currently not visible within LLMs, including that which can counter false claims made by FIMI assets. For example, guidance, reports and resources made freely available to citizens by the government, regulators, the NHS, the Electoral Commission, academic institutions, and the voluntary and charity sector. The counter-FIMI community, including government departments tackling foreign influence operations that aim to manipulate LLMs, must ensure that, at the very least, counter-FIMI information that pre-bunks false claims is readable and visible within LLM-powered AI services. This will require collaboration with key national institutional and civil society partners to identify where gaps exist in LLMs that create vulnerabilities to information warfare and identify the information that, with application of GEO techniques, could fill them.
7c) Cabinet Office and AISI should collaborate with the non-profit Frontier Model Forum (FMF) and its model provider members to encourage them to adopt a workstream specifically focused on strengthening mitigations against foreign interference threats funded by model provider contributions	The Frontier Model Forum (FMF) is an industry-supported non-profit that exists to manage significant risks to public safety and security, including exploitable vulnerabilities like ‘data poisoning’ and threats like ‘unauthorised... manipulation’ of frontier models.¹⁰⁹ Its current membership includes Anthropic, Google, OpenAI and Meta. It currently includes a workstream on AI Security in recognition that models “represent high-value targets for adversaries and threat actors.” The FMF and its members could take inspiration from the Global Internet Forum to Counter Terrorism (GIFCT) - a tech industry-led nonprofit organization founded in 2017 to prevent terrorists and violent extremists from exploiting digital platforms.¹¹⁰ This body helps facilitate cross-platform threat intelligence sharing and works closely with governments, civil society, and academia to advance counter-terror efforts. An equivalent focus and function should be established via the FMF - allowing threat-intelligence generated by the companies themselves to be shared, especially during moments of acute vulnerability, often driven by significant events. Just as terrorist exploitation of social media was recognised to be a problem affecting every social media company, so LLM manipulation is, too, an industry-wide problem requiring more significant collaboration. The Cabinet Office and AISI should collaborate with the FMF and frontier model providers to facilitate this important approach to mitigating foreign interference risks.

109 Frontier Model Forum (2025) “Annual Report-FY 2024-2025”. <https://www.frontiermodelforum.org/uploads/2025/12/Frontier-Model-Forum-Annual-Report-FY24-FY25.pdf>

110 Global Internet Forum to Counter Terrorism (2026) “GIFCT – Global Internet Forum to Counter Terrorism” <https://gifct.org/>

CONCLUSION

PRIORITIES FOR 2026-2029

Turning the ship around will be a priority across government for the new administration. In every area of policy, there will be a desire to demonstrate a willingness to take different decisions from the previous government and show a willingness to confront the major challenges facing the country.

But, where do they start?

Action must begin with a fundamental shift in how this new government approaches the information environment. The threats facing democracy today do not sit neatly within departmental boundaries. Foreign interference, online manipulation, election threats, AI-generated content, and misinformation during moments of crisis cut across national security, technology, communities, and public services. Yet government responses have too often remained fragmented, with responsibility dispersed across departments and without a single coordinating mechanism driving action.

The Conservative government established the Defending Democracy Taskforce (DDTF) as a mechanism to bring together relevant departments and agencies. However, its current structure has not provided the level of strategic coordination required. Key threats continue to fall between departmental responsibilities, with issues such as foreign interference on digital platforms sitting between Cabinet Office and the FCDO, and digital threats to elections spanning the responsibilities of MHCLG and DDCMS. Causing a stalemate for change.

A new government has an opportunity to reset this approach. This should begin by placing the Taskforce at the heart of No.10. This would signal an immediate reset on creating clear accountability, stronger coordination, and a framework capable of responding to both long-term threats and fast-moving information crises, much like COBRA.

Action must begin with a fundamental shift in how this **new government approaches the information environment.**

A new government has an opportunity to reset this approach. This should begin by **placing the Defending Democracy Taskforce at the heart of No.10.**

New leadership will also benefit from a reset in the relationship between government and the regulators responsible for implementing key areas of policy. Independent regulators play a critical role in translating legislation into action, but so far, they have been slow and not up to the challenge.

In areas such as online safety, digital markets, and the wider information environment, the pace of technological change is increasingly testing existing regulatory frameworks. A new government should work with regulators to ensure they have the necessary powers, capacity, and accountability mechanisms to meet these challenges, while maintaining the independence that underpins public trust. But also, not be afraid to criticise the regulators when they are moving too slowly. The goal should be a clearer partnership: one where the government sets ambitious objectives, regulators have the tools to deliver them, and there is transparency about how progress is being made.

Innovation must remain front and centre of this agenda. This means fully embracing and engaging with how and where the public now consumes information, developing new alternative, sovereign digital spaces and the underpinning infrastructure that reflects the values and needs of our country and communities.

By balancing the continuation of important work already underway across government with the time and space needed to develop evidence-based, ambitious ideas and to nurture new alliances and partnerships, the new government can build a more effective, innovative, long-term approach, and eventually a manifesto with the potential mandate to do more.

Licence to publish

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

a By offering the Work for public release under this Licence, Licensors represents and warrants that, to the best of Licensors knowledge after reasonable inquiry:

i Licensors has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensors be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensors has been advised of the possibility of such damages.

7 Termination

a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensors reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d This Licence constitutes the entire agreement between the parties with respect to the Work licenced here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensors shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

DEMOS

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to overcome them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales. (Charity Registration no. 1042046)

Find out more at www.demos.co.uk

DEMOS

PUBLISHED BY DEMOS AUGUST 2026

© DEMOS. SOME RIGHTS RESERVED.

15 WHITEHALL, LONDON, SW1A 2DD

T: 020 3878 3955

HELLO@DEMOS.CO.UK

WWW.DEMOS.CO.UK