September 2025

Our Position

Council for Countering Online Disinformation

The Threat:

Disinformation is a serious threat facing UK security. Evidence submitted by both the Home Office and Ofcom to the Joint Committee on National Security Strategy (JCNSS) last year noted disinformation as an active threat to UK democracy. Moreover, while the Trump administration has decided to close the Counter Foreign Information Manipulation and Interference Office, formerly known as the Global Engagement Center, 2025's annual threat assessment from the Office of the Director of National Intelligence (DNI) is clear that disinformation remains a tactic by states such as China, Russia, and Iran as part of malign influence operations. The assessment states that these are aimed at either a) increasing their own global reputation and suppressing criticism, or b) undermining social cohesion, democratic processes, and the domestic security of adversaries abroad.

According to the Reuters Institute for the Study of Journalism, approximately three in five are worried globally about what is real and what is fake when it comes to news online, with only two in five claiming to trust most news most of the time. Meanwhile, according to Ofcom, over two in five UK adults say that they encounter misinformation or deepfakes, of which seven in 10 found while online. The communications regulator also found in 2022 that, despite 69% being confident in their ability to identify false content, only 22% were able to without mistake. Disinformation & Misinformation has also been ranked by the World Economic Forum (WEF) as the most severe risk facing the world over the next two years for the second consecutive time, ahead of extreme weather events, state-based armed conflict, pollution, inequality, and the erosion of human rights.

This threat is only being exacerbated by increasingly accessible and far-reaching technology such as artificial intelligence (AI). AI has lowered the barrier to disseminating intentionally false or misleading content on a mass scale, making use of algorithms and trends in user behaviour that favour emotional and negative content. Meanwhile, a recent shift towards emphasising AI innovation over regulation poses unassuming consequences for "careless speech" and information accuracy within large language models (LLM), whose use remains riddled with confirmation bias.

The Online Safety Act 2023 (OSA) was a step forward in addressing digital harms facing the UK, with Polis Analysis part of a successful advocacy attempt to include efforts to counter misinformation & disinformation within the text. However, the CCOD maintains that this did not go far enough, and the speed of implementation has been underwhelming. Moreover, while the National Security Act 2023 (NSA) vitally targets malign foreign interference, this does not cover domestic activity. Factors such as these led to now-former JCNSS chair Baroness Margaret Beckett concluding before last year's UK general election that "important legal loopholes" still presented clear dangers to the information landscape. This sentiment has only continued under a Labour government, which acknowledged itself within their electoral reform policy paper that misinformation is threatening British democracy.

However, amid shifting geopolitical headwinds, there is a growing fear that legislation such as the OSA will be watered down rather than strengthened in order to secure a comprehensive UK-US trade deal. Speaking to the Liaison Committee, Prime Minister Sir Keir Starmer acknowledged "questions about how technology impacts free speech" in relation to trade discussions. Although the OSA remained protected within the Economic Prosperity Deal signed earlier this year, discussions over a wider technology partnership remain ongoing, leaving the future of the legislation hanging in the balance. Therefore, a whole-of-society response to the threat of disinformation has never been more important, and a unified voice from all members of civic society will be key to ensuring that demands are treated seriously by the UK government.

The Council for Countering Disinformation seeks to represent this cause, advocating for solutions to the ongoing challenges to information integrity on behalf of members across a range of industries.

Our Three Pillars:

Note: Discussions over the best means to implement the three pillars are ongoing – solutions to protecting information integrity must be fluid and reactive to the technology that continues to undermine it.

Protect the OSA, speed up current obligations, and remove loopholes: Social media companies must remain liable to fines of up to £18 million or 10% of annual turnover if they fail to take down or filter out illegal and harmful content. Given the late establishment of Ofcom's misinformation & disinformation committee, the 18-month deadline to conclude its first report should be reduced. A far-reaching exemption list for "false communication offences," the intentional sending of false information likely to cause non-trivial psychological or physical harm, creates an unbalanced justice system..

Invest further in media literacy: Numerous studies have shown the efficacy of media literacy in identifying false/misleading content online. However, it has also been noted that scalability remains a key

drawback. There are several means to resolve this. As the government continues its England schools curriculum review, civil society must continue to encourage the inclusion of media literacy and digital literacy training within all forms of compulsory UK education. Access to media literacy and digital literacy training should become commonplace at work. The government should offer free optional media and digital literacy courses with emphasis on advertising during election periods.

Fund AI for good: A fact-first information landscape cannot be protected if AI is disproportionately used to undermine rather than protect it. Solutions are proven and available: DebunkBot, a product of GPT-4 designed by researchers from American University, MIT, and Cornell, has been found to reduce belief in a chosen conspiracy theory by an average of 20% after three back-and-forth interactions with a user. Moreover, the UK contains several companies focused on AI-led content moderation for businesses and platforms, while organisations such as Full Fact provide AI services to enhance fact-checking. Greater focus and funding towards AI solutions will level the playing field against those who harness the technology with malicious intent.

Editor's Note (25-11-25): We have corrected an Ofcom 2022 statistic: 22% of adults, not 11%, could accurately identify false content without mistake.