EUROPEAN POLICY CENTRE

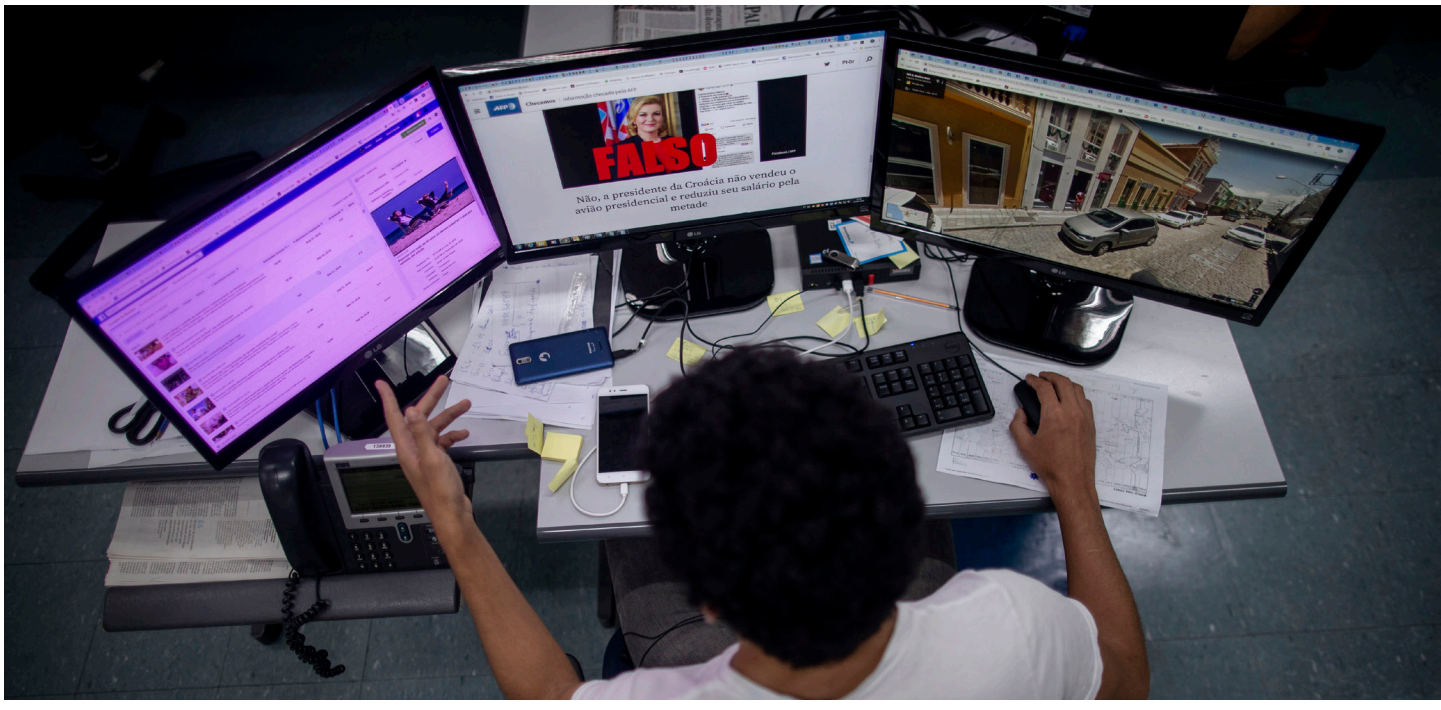
DISCUSSION PAPER

EUROPEAN POLITICS AND INSTITUTIONS PROGRAMME

30 JANUARY 2019

Disinformation and democracy: The home front in the information war

Paul Butcher



Credit: Mauro PIMENTEL / AFP

Table of contents

ABOUT THE AUTHOR

Paul Butcher
Policy Analyst for the European Politics and Institutions Programme

ACKNOWLEDGEMENTS / DISCLAIMER

The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.

Executive summary

Online disinformation is deliberately false or misleading material, often masquerading as news content, which is designed to attract attention and exert influence through online channels. It may be produced to obtain advertising profit or for political purposes, and its spread is facilitated by social media and an anti-establishment current in European politics that creates a demand for alternative narratives.

Its threat to democracy lies in its capacity to influence public opinion on the basis of falsehood. Operating mostly on independent websites outside the reach of traditional media's regulatory framework, this type of content does not need to adhere to standards of accuracy or truthfulness. Instead, it preys on fear, insecurity, societal divisions, and ideological polarisation and gives its readers the satisfaction of reading something that confirms their worldview, regardless of the empirical truth behind the story. In doing so, it entrenches them in their views, driving them further towards the extremes.

Efforts to fight the spread of disinformation have had mixed results. Self-regulation by online platforms such as Twitter or Facebook puts a great deal of power in their hands, with potentially negative effects on independent news outlets that depend on social media for their outreach. State regulation, meanwhile, raises concerns of censorship. There is a danger that methods intended to reduce disinformation, implemented clumsily or without sufficient regard for their effects, will actually exacerbate the anti-establishment feeling that drives disinformation in the first place.

Just as the disinformation problem can, to a great extent, be traced back to wider structural faults in the political system, the solution, too, must be partly structural. There must be a shift in commercial practices to disrupt the commercial motivations driving disinformation, make online platforms more fair, transparent and open, and reduce the pressure on media outlets to compete for attention. That means that all stakeholders carry a certain degree of responsibility in the fight against disinformation.

Introduction

Online disinformation, or 'fake news', is more than just a distracting internet phenomenon. Its effects have **profound consequences for democracy**. By influencing public opinion on the basis of false information, it undermines voters' abilities to make well-informed political choices. It can therefore be weaponised by subversive activists, feeding off widespread cynicism and partisan biases among citizens to support their political agenda. In fighting back, more traditional mainstream media and institutions of the 'establishment' such as the European Union (EU) risk inadvertently providing **ammunition to hostile narratives** eager to smear them with accusations of censorship or unfairness.

Misleading or hyper-partisan news coverage is nothing new, nor is it something that only occurs online. But its proliferation across the internet is alarming. With social media becoming a large part of the lives of millions of Europeans, co-ordinated campaigns pushing misleading or partisan messages can influence public opinion on an unprecedented scale even with limited resources. Mainstream politics has to sit up and pay attention.

Some of these malicious efforts are the work of external actors such as the Russian state, engaged in an 'information war' with the West. But many of them are home-grown.[1] **Domestic activists are also working to undermine fact-based political discourse**, especially in support of populist, far-right or anti-democratic causes, and diminishing the influence of external actors is not enough in its own right. Winning this information war means winning on the home front too.

This paper will first explore what makes online disinformation dangerous, how it supports itself, and the motives that have encouraged its spread. It will then discuss and evaluate some of the recent efforts to fight back, as implemented by national governments, EU bodies, and social media platforms. In doing so, it will identify other potential resources in the private sector. Finally, a set of recommendations will follow for each of these actors in turn, with the aim of providing some proposals for a society-wide collaborative approach.

'Fake news' and 'disinformation' > The term 'fake news' may be widely recognised in public debate, but academic and policy sources generally advise against it, recommending 'disinformation' instead.[2] While misinformation refers to material that is simply erroneous, for example due to error or ignorance, disinformation implies an intentional, malicious attempt to mislead – see Fig. 1 on page 5. In this paper, 'fake news' and 'disinformation' are used as synonyms.

Disinformation is just one of several tools that exploit social media and internet technology to the detriment of the democratic political system. **This paper will not attempt to cover targeted advertising, automated accounts ('bots'), or hacking and 'meddling' in election campaigns**. These may be used to increase the reach of disinformation, and may be facilitated by some of the same factors described here, but they are distinct techniques in their own right and are not core to the subject of this paper.

1. A threat to democracy?

Only a few years ago, the internet was widely seen as a force for good in supporting democracy. The Occupy movement and the Arab Spring – which became known as the 'Facebook Revolution' – were hailed at the time for demonstrating social media's power to give ordinary citizens a voice and even effect real change.

But a number of high-profile political events in the past few years have shaken our confidence in the internet's democratic potential. Starting with the double blows of the decision of the British electorate to leave the European Union in the 'Brexit' referendum and the election of Donald Trump as President of the United States, followed by elections in several European countries where radical illiberal parties put in strong showings, 'fake news' has become a matter of acute political concern for the role it may have played in influencing these outcomes. It is difficult to prove whether or not disinformation had a decisive impact, but there is no doubt that it had a wide reach: an analysis by *BuzzFeed* found that **fabricated news stories reached a greater online audience than 'real' news** in the final months of the US election campaign.[3]

In any case, disinformation has raised concerns among internet watchdogs, academics and the general public. A 2017 report on internet freedom by Freedom House concluded that "online manipulation and disinformation tactics played an important role in elections in at least 18 countries over the past year… [contributing] to a seventh consecutive year of overall decline in internet freedom".[4] A Eurobarometer survey in February 2018 found that 83% of European citizens believe that **fake news represents "a danger to democracy"**.[5]

The appeal of disinformation for illiberal politicians is that it is a convenient tool for extremist discourse to compete with and ultimately crowd out rational, informed debate.

This is unsurprising, given the prominence of disinformation in recent election campaigns across Europe. In a TV debate prior to the French presidential elections, the far-right candidate Marine Le Pen raised accusations that her liberal opponent, Emmanuel Macron, had a secret bank account in the Caribbean, referring to a malicious story that had begun circulating on Twitter only a few hours beforehand.[6] In Germany, a claim that Angela Merkel had taken a selfie with one of the men involved in a terror attack in Brussels reached twice as many Facebook users as the factual account issued to correct the rumour.[7] The Czech presidential election in January 2018 was marked by an abundance of false articles smearing liberal candidate Jiři Drahoš as a paedophile or communist collaborator, claiming that he was 'pro-immigrant' despite his opposition to migrant quotas.[8] In each case, **the disputed stories reflected poorly on 'establishment' candidates and favoured the narrative of illiberal or populist actors**.

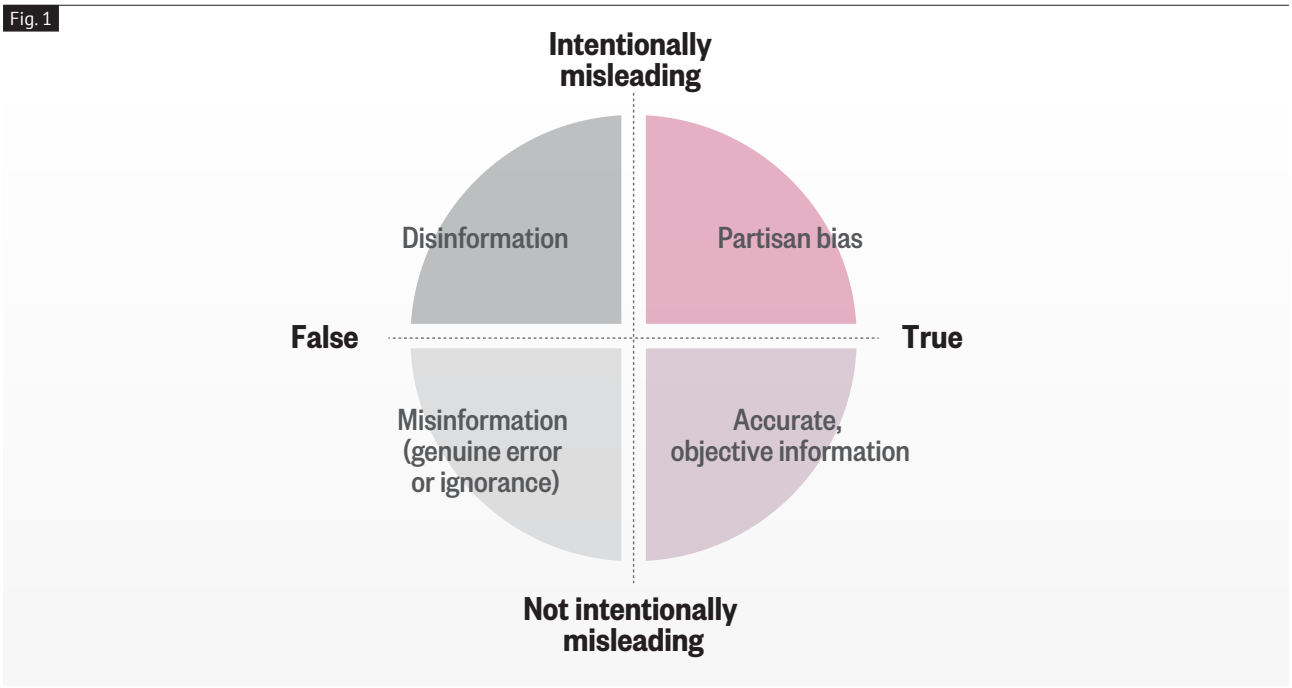
The appeal of disinformation for illiberal politicians is that it is a convenient tool for extremist discourse to **compete with and ultimately crowd out rational, informed debate**. In a media environment where revenue depends to a great extent on the number of clicks an article can generate, there is demand for ever more dramatic or sensational headlines as news outlets compete for readers. Content that triggers a strong emotional response is prioritised over sensible, fact-based reporting. In this way, the low standards set by fake news cross over into mainstream journalism as well, with negative consequences for the public debate all around.

When it requires too much effort or expertise to tell the difference between fact and fiction, a common response is to turn away from politics altogether. Such disillusioned citizens may even come to lose faith in democracy itself.

It can also contribute to political apathy by sowing doubt and confusion to such an extent that citizens, overwhelmed and unable to say for sure what is really true, simply **retreat from politics**. This is what the RAND Corporation has described as the "firehose of falsehood" technique, used to great effect in Putin's Russia and now being exported to serve Russia's interests abroad: a "challenge to the very notion of an independent accounting of facts", in which all news becomes perceived as potentially fake, and politics too complicated to be worth following.[9] When it requires too much effort or expertise to tell the difference between fact and fiction, a common response is to turn away from politics altogether. Such disillusioned citizens may even come to **lose faith in democracy itself**.

So disinformation aims to undermine the very notion that there can be such a thing as a reliable fact, which is the basis of any healthy democracy. Democracy is about making choices: this requires a well-informed debate. The idea of 'truth' is needed to hold politicians accountable. These roles – keeping the populace informed and holding power to account – are among those traditionally played by the media, and the internet is perhaps the most important part of the media today. **The proliferation of unreliable information on the internet is therefore a challenge to one of the structural pillars of democracy**. This means disinformation is more than just a moral problem; it is actively undemocratic. It follows that democratic societies should be concerned enough about its effects to take action against it.

Fig. 1



2. The business model of falsehood

The European Commission's definition of disinformation — "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit"[10] — captures **the two main motives that drive its creation and distribution**. First, the **commercial motive**: to obtain advertising revenue or market share, typically by attracting readers with sensational claims. Second, the **political motive**: to shape public opinion according to particular interests. Both present a political problem, and the line between the two is often blurred, especially when profit-driven disinformation becomes 'useful' to political actors.

These motives are facilitated by **two factors that have worked to increase disinformation's reach** in recent years. First, advances in **technology**, particularly social media, have had a transformative effect on the media environment. In particular, it has massively increased the reach of information that can originate anywhere, not just from professional newsrooms or 'trusted' sources. Second, the increase in support for **anti-establishment, anti-EU political actors** over recent years would suggest that there is an increased demand for information that supports 'alternative' discourses. The following section will explore these factors in more depth.

2.1 THE NEW TOOLS

Tabloid journalism (exemplified by newspapers such as *Bild* in Germany or The Sun in the UK) has been making money from sensationalism for years. Sensationalist coverage is not necessarily fake news, but in the absence of regulation or scrutiny the distinction between them can easily become blurred, especially for online-only outlets with no paper edition. Meanwhile, **the shift in consumption habits in the internet age has had serious repercussions on public exposure to 'unscrupulous' journalism**. The original tabloids existed in a public sphere where their stories could be challenged by other newspapers on the rack; today, it is more and more likely that readers will never be exposed to other takes at all.

Where once there was a single public space dominated by competitive media, there is now a multiplicity of individualised information spheres.

For those who get the majority of their information from social media (more than half the population in most European countries[11]), the 'echo chamber' effect may severely restrict the type of news content they see. Most social media platforms work by presenting users with content similar to that they have already liked, with the result that they are only shown a narrow selection of views. **Where once there was a single public space dominated by competitive media, there is now a multiplicity of individualised information spheres**.

What is more, the commercial structure of online journalism encourages sensationalism. Online advertising prioritises page views above all else: **a webpage that receives a large number of clicks is more profitable than one with a more restricted audience**, regardless of what appears on the page. This has changed the way

that online news sources present their content — witness the shift towards 'clickbait' headlines that perform well on social media (see box) and the increased prominence of features that encourage readers to 'share' the article and contribute to its wider dissemination. But for those with fewer scruples or with no reputation to protect, advertising is an easy way to make money, provided you have a knack for writing attractive headlines.

Clickbait > Headlines that, instead of summarising the topic of the article, provide a teasing and often emotionally manipulative preview designed to pique the reader's curiosity and encourage them to read something they might otherwise skip. Common examples use phrases like "You won't believe what happened next", "This simple trick…", or "Top 10 most unbelievable facts (Number 9 will shock you)". The articles themselves are often low-effort material with little original content: the aim is merely to attract the click. However, so-called 'respectable' news outlets, such as the BBC, have also adopted 'clickbait'-style headlines in an effort to attract younger readers who are used to less traditional news sources.[12]

These clickbaiting techniques often blur the lines between news and entertainment, fitting into a social media environment where there is no distinction between updates posted by friends, amusing material, and serious news. While a newspaper may divide its content between reporting, opinion, and a human interest section, the social media newsfeed puts everything together. The only important thing is that each piece of content, be it a friend's holiday photos, a funny video, or a serious news article, **invokes an emotional response**. The most successful 'fake news' works eliciting the desired emotional response from a certain group of people – and outrage, fear or envy are generally easier to evoke than more positive emotions.

While a newspaper may divide its content between reporting, opinion, and a human interest section, the social media newsfeed puts everything together. The only important thing is that each piece of content, be it a friend's holiday photos, a funny video, or a serious news article, invokes an emotional response.

'Fake news' online seems to have its origin in satirical news sites, with some authors originally writing parody material before finding that hoax articles were more likely to go viral and bring in ad revenue. According to a report by BuzzFeed, most fake news stories in the first half of 2016 were about crime or medical anomalies, often aiming to shock or amuse; it was only in the second half of the year that the US presidential election revealed the fertile market for misleading political articles.[13] In other words, **even much politically-themed disinformation is motivated not by politics so much as by money**.

As a striking example, many of the 2016 US election's most-read fake news stories were not produced in America at all, but by students in the Macedonian town of Veles.[14] Dozens of tech-savvy teenagers registered websites with names such as *USA Daily News* and *USConservativeToday.com* to take advantage of the huge audience for articles claiming, for example, that Pope Francis had endorsed Donald Trump for President, or that Hilary Clinton sold weapons to ISIS. The hosts of these websites had no stake in the election and no political motives: they were motivated purely by the thousands of euros they could earn from stuffing their webpages with advertising and sharing them within partisan Facebook groups. Reporters who covered the Veles 'fake news boom' found that some of these teens were earning thousands of euros every day during the height of demand in 2016.

Where there is an eager audience and a monetary award, a parasitical fake news industry is virtually inevitable.

In a country where the average income is €350 a month, the appeal of running a fake news 'business' is clear. But there are writers making money from disinformation in the US and EU too. One fake news entrepreneur, running a network of sites and commissioning writers from all over the world, implied he was making up to $30,000 a month, proving how profitable disinformation can be.[15] In an age of precarious work and high youth unemployment, disinformation is an attractive endeavour for technically literally young people.

If European politics has not yet been the target of a cottage industry on this scale, it is probably only because of the smaller potential audience for articles in languages other than English. **Where there is an eager audience and a monetary award, a parasitical fake news industry is virtually inevitable**. The Veles example proves that, with the tools provided by social media, disinformation can be a profitable endeavour for anyone, not just organised newsrooms or state propaganda departments.

What is more, this kind of material can be written and published anonymously, meaning **its creators are in no way accountable**. In the case of 'traditional' journalism, it is at least always clear who wrote the article, who edited it, and who approved its publication. Such accountability is missing in the case of online self-publishing. Factor in unprincipled actors with a political message to push, and the result is a chronic stream of harmful disinformation.

But the possibilities provided by social media and advertising revenue are only part of the story. The ease with which disinformation can be made and spread does not in itself explain why the majority of disinformation is directed against the established political order, or why it finds such a receptive audience in the first place.

2.2 THE NEW DEMAND

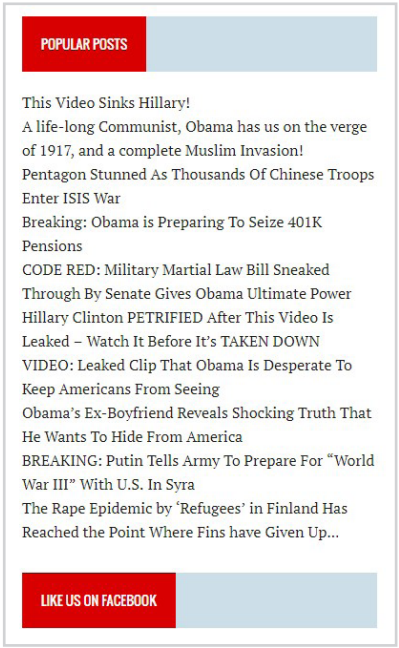
Many of the Veles teenagers' fake articles were somewhat implausible stories designed more to attract attention than to actually convince. But in the hands of actors with political motives, their techniques can be used for more insidious purposes. **The activity in Veles attracted the attention of American conservative activists who wanted to see Donald Trump in the White House**, and there is evidence to suggest that, as polling day neared, they worked more and more closely together.[16] What had begun as a money-making exercise became a tool for unscrupulous political activism.

Similarly, 'alternative' media outlets, such as *Sputnik News* or *Breitbart* (see box), feed a very real demand for anti-establishment news content. But at the same time they may also seek to use this anti-establishment sentiment to **shift public opinion in Europe according to the interests of a political actor**: in the case of Sputnik, the Russian state; for Breitbart, the international 'alt-right'. When this motivation to feed a particular ideology eclipses the commitment to accurate information, the result is disinformation.

Sputnik, Breitbart > These are some of the biggest 'alternative' online news outlets. Not all the stories they publish are 'fake news', but they are heavily partisan and prioritise sensationalist headlines over accurate information. Sputnik is owned by the Russian government and aims to promote Russian interests abroad, much like RT (formerly Russia Today), which mainly operates as a television channel. Breitbart, meanwhile, is an American outlet associated with the 'alt-right'. Its former editor, Steve Bannon, served as an advisor to Donald Trump and is now working to establish a foundation in Brussels to support the European far-right. Countering the mainstream media with 'alternative' messaging is a central part of his political strategy.

Frustration with mainstream news, caused by the perception that it is partisan or unfair to a particular cause, is a ripe source of opportunity for news outlets with less commitment to factual objectivity. Many of these outlets enthusiastically take up causes that are divisive or controversial in Europe, especially those with potential to threaten the stability of the EU, such as Brexit or the crisis in Catalonia. In many cases, **they do so quite openly**, touting their 'alternative' credentials as a means to draw in viewers who feel their political views are not treated fairly by other outlets. RT (formerly known as Russia Today), for example, makes no attempt to hide its links to the Russian government, and its business model depends on the idea that it offers an "alternative view of global events". RT claims that, although its broadcasting may be biased, so is that of Western channels such as the BBC or CNN (which, in reality, are independent and not subject to a state-defined editorial line like RT). Its slogan is "Question More" – implying that, by watching RT, viewers will learn to perceive biases in other outlets (and thereby distrust them). The fact that RT continues to attract an audience (43 million viewers in 15 European countries[17]) at least partly because it is perceived as being "honest about lying"[18] – unlike other, supposedly equally biased outlets – demonstrates that **there is an existing undercurrent of dissatisfaction with mainstream news** that is open for exploitation.

To an extent, this frustration may be caused by external factors beyond the media's control. The proliferation of online news sources has exposed the public to a greater variety of views, making them more demanding of appropriate balance in the traditional media. But **the media's response to the changing environment has not always been to prioritise dependability and credibility**. Faced with competition from sensationalist 'clickbait' headlines online, standards have been slipping for many news organisations anxious to maintain their readership. An editorial line is one thing, but one-sided



Some dedicated fake news websites are obvious fakes, such as USConservativeToday.com (left). But some are more cleverly put together. During the 2017 French presidential election, a page-for-page copy of Le Soir appeared under the URL lesoir.info (right) – it contained a single false story about the funding behind Macron's campaign, and was widely shared on social media.

coverage frustrates readers who are able to see, via social media or other channels, that there is clearly another side to the story. **In some cases, by being excessively partisan themselves, mainstream news sources have contributed to a situation where partisan loyalty has undermined objectivity**.

Not all fake news stories are necessarily anti-establishment in nature or viable to be used by populist or extremist politicians to support their own narratives. But the **topics that dependably elicit a strong response are often those where populist discourse has already established a strong presence**, such as immigration, terrorism and allegations of corruption or misconduct by mainstream politicians. This in itself reveals that the spread of disinformation stems from a lack of trust in the 'mainstream', represented by the media and government parties, and as political polarisation increases, so does demand for appropriately partisan news content.

In some cases, by being excessively partisan themselves, mainstream news sources have contributed to a situation where partisan loyalty has undermined objectivity.

Disinformation's success therefore owes a great deal to the prevailing political mood, particularly the increasing support for populist parties. What is more, the techniques of social media content play into their hands. Populists have carved out a niche in the political spectrum through provocative discourse and attempting to monopolise the debate on a handful of issues; a media environment where sensationalism trumps measured discourse provides the perfect storm to push their messages. It also plays into the hands of those who seek to promote an 'us versus them' narrative, entrenching polarisation. Meanwhile, the fact that most disinformation is directed against the 'established' political order means that, in spreading its message and pushing people towards more extreme political opinions, **it also creates a more favourable environment for itself**. Dissatisfaction with mainstream politics, polarisation, populist political actors and disinformation are all linked to one another and mutually reinforcing, creating a vicious cycle that is difficult to break.

This has made disinformation a favoured technique of extremist activists, sometimes coordinating their efforts in chat rooms or messaging apps to ensure that their content reaches as wide an audience as possible. Such organised campaigning is carried out almost exclusively in support of illiberal parties like the AfD in Germany[19] and the Front National (now Rassemblement National) in France, and while it may not be part of these parties' official campaigns or sanctioned by their leaders, the aim is to upset the established order and shift the narrative in their favour. As with Le Pen's comment about Macron's supposed Caribbean bank account (see section 1.1), populist leaders have demonstrated that they are perfectly willing to make use of this underground, unofficial support and spread disinformation more widely, giving it a gloss of legitimacy for their less extreme followers.

Dissatisfaction with mainstream politics, polarisation, populist political actors and disinformation are all linked to one another and mutually reinforcing, creating a vicious cycle that is difficult to break.

In many cases, this organised activism is supported or abetted by other actors with an interest in weakening the European liberal democratic system. Notably, the Russian state has provided support to AfD activists and worked to spread subversive messaging all over Europe.[20] This is a serious threat, but it should be put into perspective. A great deal of Russian online activity in Europe and the US consists of **amplifying existing divisions**. Concern over the role played by the Russian state in influencing Western elections often obscures the fact that this 'meddling' consists of political messaging that is eagerly accepted by parts of the electorate. Russian meddling is not mind control; if their ads or fake articles are successful in shifting European or American public opinion, **which is a domestic problem as much as it is a state security issue**.

Disinformation is not merely a *cause* of political polarisation, populist support, and anti-establishment feeling; it is also a *symptom* of a political system that already finds itself on shaky ground. Motivated by profit and political interest, and facilitated by social media and an eager audience, **disinformation is likely to continue to be a prominent issue** until this underlying problem is addressed. It is beyond the scope of this paper to venture solutions to this disillusionment with liberal democratic 'mainstream' politics, but it must be borne in mind that any efforts to counter disinformation will ultimately only be successful if there is at least as much effort directed to fixing the fundamental causes.

Nevertheless, there are certain things that can be done to stem the flow of disinformation. The following section will explore some of the efforts that have been made to resist disinformation, the challenges those efforts have faced, and the risks these kinds of approaches entail.

Disinformation is not merely a *cause* of political polarisation, populist support, and anti-establishment feeling; it is also a *symptom* of a political system that already finds itself on shaky ground.

3. Existing measures and their challenges

To a great extent, the debate so far about how to resist disinformation has focused on policing content on social media platforms. There are typically two approaches to this task: **self-regulation** by the platforms themselves, and **governmental regulation**, which may take place at the level of national governments or at the EU level. This section will analyse both in turn, before going on to consider the efforts of private sector actors which have largely been side-lined in the public debate so far. For each actor, it will also consider the risks or disadvantages of existing measures, with an eye to ascertaining more promising areas to direct future efforts. Finally, it will consider the principles and strategies behind the EU's efforts.

3.1 ONLINE PLATFORMS AND SELF-REGULATION

Once seen as the most obvious route to a healthy online space, self-regulation – that is, the efforts of social media companies to police their own content and fight against the spread of disinformation on their services – is now widely seen as ineffective or insufficient.[21] **The public mood has turned against the platforms, which are often perceived as not taking the problem seriously enough**. When Mark Zuckerberg, CEO of Facebook, initially dismissed claims that activity on the platform could have influenced the outcome of the US presidential election, calling it "a pretty crazy idea", he received a lot of criticism for being complacent.[22] Meanwhile, multiple scandals have further reduced public trust in social media, such as the March 2018 revelations that political consultancy Cambridge Analytica had made use of the data of up to 87 million Facebook users, acquired without permission. Facebook's appearances in parliamentary hearings did little to reassure policymakers and the public in the US and in Europe that it was doing enough, and later leaks revealing its business practices, including hiring a firm to investigate the financial interests of George Soros, a prominent critic, have been disastrous PR for the company. In this climate, it is little surprise that social media companies find themselves under intense scrutiny.

However, the platforms' continued efforts to improve their systems and their moderation efficiency should be recognised. In the last few years, social media companies, particularly the 'big three' of Facebook, Google and Twitter, have become aware of their roles in facilitating online disinformation and are willing to cooperate in combating it, not least for the sake of their own reputations. Where once they saw themselves as simply vehicles for user-generated content, with little responsibility for what is posted by users, **the social media giants are now becoming more sensitive to their unparalleled public roles and the corporate and social responsibility they require**. Accordingly, they have increased their self-regulation efforts, such as by hiring more moderators and experimenting with changes to their algorithms.

Social media platform > In the context of social media, a 'platform' is the application or interface where users interact with content and with each other. Social media platforms can take a variety of formats, but this paper is concerned chiefly with networks that link users with public content on a text-based 'newsfeed', such as Facebook or Twitter. Disinformation can also spread on platforms dedicated to sharing video or image content (e.g. YouTube, Instagram) or private messaging apps (e.g. WhatsApp, Snapchat), but these are outside the scope of this paper.

Algorithm > Most social media platforms choose which content to display to users by means of a formula which takes into account what the platform knows – or can learn – about the user to suggest content he or she may find interesting. This is the same technology that provides suggestions and similar items on retail websites, and has a similar purpose: to maximise user engagement with the site, potentially leading to more income, in this case via advertising. For this reason, a platform's algorithm is often the key to its success and a cornerstone of its business model.

Where once they saw themselves as simply vehicles for user-generated content, with little responsibility for what is posted by users, the social media giants are now becoming more sensitive to their unparalleled public roles and the corporate and social responsibility they require.

Any future anti-disinformation strategy must surely include rigorous self-policing as part of its general approach. But self-regulation has not always been successful, and it carries many pitfalls.

There are simple problems facing the most obvious anti-disinformation measures. Users can flag or report suspicious content, but there is no way of preventing users from abusing this in an attempt to have genuine content taken down, for example if they disagree with it politically. Fact-checking services can work full time to debunk fake stories, but it is impossible to guarantee that a 'debunking' article will reach the same users as the original inaccurate story. What is more, the time and effort required to discredit a false story is excessive in comparison to the effort required to make something up in the first place: in the time it takes to disprove one false article, several others may have appeared in its place.

With more than two billion active users, Facebook is the largest social media platform by some distance, so it makes sense to explore some of its measures in more detail. From partnering with fact-checkers to flag disputed information, through polling its users about

which news sources they trust, to changing its news feed algorithm to prioritise content posted by friends over that posted by interest groups, the disinformation scare has led Facebook to experiment with the very way it presents its content. But some of its efforts have backfired or had other unintended consequences.

The time and effort required to discredit a false story is excessive in comparison to the effort required to make something up in the first place: in the time it takes to disprove one false article, several others may have appeared in its place.

Facebook's tweaking of their newsfeed algorithm has, in some cases, had disastrous effects for the reach of 'independent' news outlets (that is, alternatives to government- or business-owned mass media), particularly in countries where these strongly depend on social media. An experiment carried out on their Slovakian users, for example, whereby all publisher-posted content was moved from the default view to a separate feed, resulted in a 400% drop in user interactions (i.e. likes, comments, shares, and clicks) overnight for major Slovakian news sites.[23]

Changing the algorithms to reduce the importance of news articles equates to throwing out the baby with the bathwater: **it reduces the disinformation problem, but at the cost of also reducing the reach of 'real' news**. This does nothing to improve the standards of information available to users, but rather diminishes social media's huge potential for the news media landscape. What is more, Facebook's technique of trialling new features only in certain markets means that **the browsing experience can vary significantly between countries**, making it difficult to know if we are all seeing the same thing when we log on. As a result, different countries' experiences in fighting disinformation on the platform are not necessarily comparable.

Like many other platforms, Facebook is constantly compiling data about its users' habits and using this information to improve its user experience and business model. But **the company's analysis and research findings are not made public**. For example, Facebook once experimented with a system of flagging disputed news stories, but withdrew the feature after its analysis suggested **this was causing more harm than good**, entrenching people in their beliefs rather than encouraging them to seek out more reliable information.[24] This seems to be a finding with important implications, and would be of great interest not only to anti-disinformation campaigners but also to political scientists, psychologists, and many other researchers. But **many online platforms, including Facebook, consider their algorithms and research data to be business secrets and do not allow researchers to access this potential goldmine of information for fear of losing their competitive edge**. The result is that each platform is fighting its own battle against disinformation and not sharing findings with other stakeholders.

In any case, Facebook's headline-grabbing initiatives in this field are partly a result of its extraordinary position in the online sector. **Its enormous resources and market-dominant position mean that it is able to implement potentially loss-making changes that are out of the reach of smaller, less affluent companies**. In the last two years, Facebook has changed its business model to start prioritising the *quality* of user experience over the *quantity*, aiming to *reduce* time spent on the platform – a luxury not available to all online media, most of which are engaged in a frantic competition for user attention and clicks. The fact that Facebook's changes are so far the most significant concrete measures taken against disinformation is itself revealing of the extent to which we rely on the algorithms of a few monopolistic services.

This domination of the online space by a handful of commercial actors raises concerns relating to the freedom of information. Entrusting social media platforms with the ability to decide what information is shown to their users carries the risk of **the 'privatisation of censorship'** – arguably worse than state censorship, which can at least be challenged politically. Facebook does not seek to remove false material from the platform entirely, claiming that to do so would be "contrary to the basic principles of free speech" and that fabricated information does not necessarily violate its terms of use or community standards.[25] Instead, it merely aims to 'demote' suspicious content so that it is less prominent on the newsfeed and its reach is restricted (see image). But this principle does not hold water: **whether material is removed completely or merely prevented from reaching the audience it would otherwise reach, the result is still censorship**. By stopping short of removing suspicious content outright, Facebook avoids having to define what it considers to be fake news. It thereby also avoids having to process appeals: users will never know for certain if their content is being 'demoted'. The platform is therefore able to exercise blanket censorship on anything that could potentially be harmful, without needing to justify its individual choices.

Whether material is removed completely or merely prevented from reaching the audience it would otherwise reach, the result is still censorship.

This is one of the concerns that has led to distrust of self-regulation, and part of the reason why state regulation has become more attractive to policymakers. However, **self-regulation and state regulation do not exist in isolation from one another**. Stuck between the hammer of public scrutiny and the anvil of private censorship, social media platforms have a difficult enough job even without political activists seeking to game their systems.

As governments increase the pressure, the platforms often err on the side of caution by adopting stricter standards than they otherwise would in order to avoid fines. As the following section will demonstrate, state regulation carries no fewer dangers.

3.2 THE GOVERNMENTS OF EU MEMBER STATES

As disinformation has become a matter of public concern, EU member states have taken a variety of approaches to legislate against it. In Italy, for example, the government set up a website allowing people to report false stories to the police. In Ireland, a bill was proposed to criminalise the use of bots (automated social media accounts) to spread disinformation, while Denmark and Sweden have taken steps to include disinformation in their existing media literacy campaigns.[26] But the most noteworthy efforts to legislate against disinformation have come in the form of two laws in the biggest member states, France and Germany.

In **Germany**, attempts to fight disinformation largely consist of expanding existing legislation targeting hate speech and other illegal material to include 'fake news'. In **France**, meanwhile, new legislation has been tabled specifically to address disinformation. Both approaches run into the problem of how to define disinformation legally, and carry the risk that it may end up being the politicians who decide rather than the courts.

The **German approach** bundles disinformation into a new hate speech law (it entered into force in April 2018) that allows for **fines of up to €50 million for social media platforms that fail to remove hate speech and illegal material within 24 hours.**[27] The French law focuses on transparency, requiring social media to reveal the sources of news content and advertising, but it also allows for sites that host fake news stories to be shut down following a judicial procedure. Specifically, during election campaigns candidates can sue for the removal of contested news stories, requiring courts to rule on whether the reports are credible.

Both laws run into problems of time. The 24-hour limit of the German law is enormously ambitious, given that a report in 2017 found that Facebook managed to remove reported content within that time limit in just 40% of cases. For comparatively understaffed Twitter, it was only 1%. Even then, **24 hours is still a long time, given that social media content can go viral in minutes**. The French law's focus on election periods, presumably drawing from the experience of the 2017 presidential elections (when Emmanuel Macron's campaign was a target of disinformation), neglects that political opinions and voting intentions are not formed solely during election campaigns, and scrutiny must continue to be applied even when the stakes are perceived to be lower. Applying different standards during election periods is political ammunition for opposition activists to cry censorship.

To date, these laws have hardly been used, perhaps demonstrating that they are unwieldy and ineffective in practice. Critics have suggested that **their real power lies in their chilling effect**: even if the regulations themselves stop short of censorship, it is likely that the platforms themselves may be overzealous in their implementation of the rules, blocking more content than is strictly necessary in an effort to avoid fines and bad publicity. Especially when under time pressure (as with the German 24-hour rule), it is safer for the platforms to err on the side of caution than to risk enormous fines. In other words, **the distinction between state regulation and self-regulation is not always so clear-cut**, and self-censorship may be the result even when measures stop short of state censorship.

It is no surprise that member states with tough existing laws regarding hate speech, such as Germany, have been the readiest to legislate against disinformation, while countries with proudly liberal free speech traditions, such as the Netherlands, have sought to defend these traditions (see section 3.4 for more information on how the debate has unfolded in the Netherlands). Effectively, this is a new chapter in the long struggle between free speech and censorship. A common thread in that story has always been the actions of political actors, including governments, who deliberately make use of censorship to suit their own interests. **Fighting disinformation is an excellent excuse for governments of a more authoritarian nature to implement crackdowns on**

media freedom more widely, or to allow disinformation of their own to circulate while suppressing independent media. According to Péter Krekó of the Political Capital Institute in Budapest, the Hungarian media landscape today features very few underground 'fake news' outlets precisely because the mainstream media, largely in government hands, produces fabricated material in the same vein, while opposition media is shut down.[29] In the Czech Republic, President Milos Zeman bypasses the mainstream press in favour of 'alternative' media websites, lending them legitimacy.[30]

Even if the regulations themselves stop short of censorship, it is likely that the platforms themselves may be overzealous in their implementation of the rules, blocking more content than is strictly necessary in an effort to avoid fines and bad publicity.

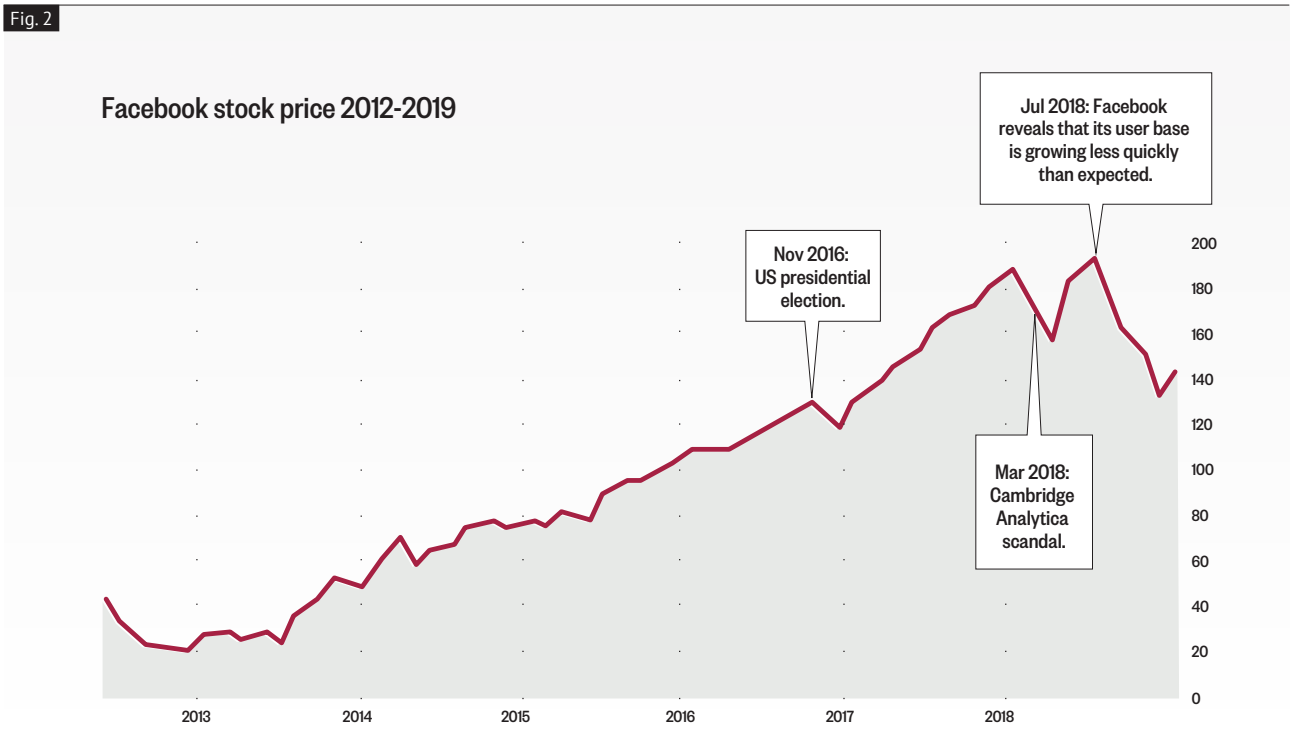
In fact, governments in general are the wrong agents for effectively fighting disinformation. State regulation can be just as counter-productive as self-regulation, with the additional danger that it risks encouraging the very anti-establishment feeling it seeks to counter. Fortunately, there is a third option. Structural resistance to disinformation can be built up through the efforts of civil society, NGOs, and the private sector, as will be described in the following section.

3.3 THE ANTI-DISINFORMATION SERVICE INDUSTRY

NGOs have a strong interest in fighting disinformation, and many are already working in promising directions. Examples include the media literacy work of the European Association for Viewers' Interests (EAVI), watchdogs such as AlgorithmWatch, and networks of non-profits working on fact-checking and other services, such as the Poynter International Fact-Checking Network. This is a welcome resource for expertise, ideas and practical suggestions that are not handicapped by the distrust that often surrounds government, EU or Big Tech company efforts. According to the 2018 Edelmann Trust Barometer, trust in NGOs is higher than that in government or media (though still low at only 53% globally).[31]

But non-profit motives are not the only motives for defending against disinformation. Building an infrastructure that is resistant to disinformation is possible in the private sector too, **because disinformation is also harmful to business models**. In other words, **in addition to any moral or political incentives, there is a *commercial* motive to fight disinformation, with the potential to counteract the commercial motive to create it**. Private companies concerned about their public image have a major interest in not being affiliated in any way with deceptive, misleading or malicious sites. Many companies are concerned about where their ads appear online, and are willing to pay extra to ensure they will not be shown on inappropriate pages. For example, well-known companies such as Kellogg's, Lego and the Vanguard Group no longer advertise on controversial news platforms such

Fig. 2



Data source: Macrotrends, "Facebook – 7 year stock price history", https://www.macrotrends.net/stocks/charts/FB/facebook/stock-price-history

as Breitbart or The Daily Mail, and Unilever recently announced that they will pull all their advertising from Facebook and Google entirely unless they can guarantee their ads will not be listed alongside undesirable content.[32]

Online advertising today is mostly automated: rather than choosing where they want their ads to appear, companies rely on Google AdSense or similar systems to provide targeted ads to particular users. This means the ads could appear on any site, as long as it has not been blacklisted, and the **companies in question are often unaware of where their ads are being shown**. Most sites containing pornography or illegal content are already on the blacklists, but others – such as fake news hosts – must be specifically requested by the advertising client if they wish to boycott them.

Some digital advertising agencies and consulting groups have carved out a niche for themselves in the marketplace by offering services with this social responsibility in mind. For example, NetSuccess, a Slovakian online advertising and marketing agency, provides their clients with the tools to "prevent your brand from being associated with controversial content".[33] As disinformation in Europe, unlike the US, can be in any of the EU's 24 official languages (not to mention regional or minority languages), the local expertise of commercial interests from all corners of Europe is an excellent resource to catch more than just the most widespread English-language fake stories.

Perhaps the massive public response to recent social media scandals (Facebook's stock prices fell 16% after the Cambridge Analytica revelations and have fallen still further since then – see Fig. 2) will help to turn the tide of commercial interests when it comes to online disinformation. From advertising revenue incentivising sensationalism, to services protecting brand images, the private sector has enormous power to affect change in the digital media sphere. So far, we have mostly seen this power used for bad, but its positive potential should not be overlooked.

But no single sector can defend against disinformation alone, and an effective strategy will need a mutually supportive network of all parts of society, where each stakeholder plays an appropriate role. This is one reason why the national level is inadequate for tackling such a widespread problem in the online space: to prevent abuses or poor implementation at the national level, and to coordinate a wide variety of private sector actors, there must be a European level of oversight.

3.4 THE EUROPEAN COMMISSION STRATEGY

The EU level is not the highest level on which action against disinformation could take place; there is scope for further international cooperation, particularly the sharing of experience and knowledge between the US and Europe. But what the EU does offer is the possibility for structured, binding policy, regulatory oversight, and the means to enforce it. In fighting a cross-border problem such as disinformation, it is the most promising level for effective action.

The EU's efforts have been rather more cautious than those of the member states, opting to explore more systematic approaches to the issue rather than implementing headline-grabbing fines and attacks on the platforms. This is partly because the EU seeks to avoid infringing on the competences of the member states in these areas. But its systematic approach also reflects the fact that the EU, with cross-border competence, can take a bigger-picture approach with more potential for long-term success.

Following the report[34] of the High Level Expert Group on fake news and online disinformation, Digital Commissioner Mariya Gabriel led the establishment of a "multi-stakeholder forum on disinformation" to facilitate cooperation between actors, eventually resulting in the **"EU Code of Practice on Disinformation"**.[35] The Code sets out a list of commitments and principles that the signatories – which include all the main online platforms including Facebook, Google and Twitter, as well as software designers, advertisers and trade associations – agree to follow in their efforts to protect users from disinformation.

The Code's main aim is to improve the transparency, trustworthiness and accountability of the online ecosystem. For example, it obliges signatories to undertake efforts to **disrupt the advertising and monetarisation incentives** to produce disinformation, mandating transparency and increased scrutiny of advert placements – for example, advertising should be clearly distinguished from editorial content on news sites, and users should be able to see why they have been targeted with particular content. Platforms should also ensure that their algorithms prioritise 'good' content, according to set indicators of trustworthiness – which, however, are not defined in any detail. The Code recognises the **importance of access to data** for fact-checkers and researchers, and even calls on media outlets to **make it easier for people to find alternative viewpoints** in news sources to undermine the attraction of partisan fake news. Aware of the risks of censorship, the Code explicitly rules out policies encouraging the deletion of lawful content "solely on the basis that they are thought to be 'false'", citing Article 10 of the European Convention on Human Rights, which guarantees the freedom of expression and information.[36] Each signatory must prepare an annual report on its efforts, and the European Commission will undertake a review each year – indicating that the Code establishes the basis for a long-term and adaptive plan.

In this way, the Code demonstrates a laudable awareness of the driving factors behind disinformation and the risks inherent in regulatory efforts that have been described in this paper. It is clearly the result of careful consultation with a variety of experts and stakeholders, and provides an excellent starting point for a sensitive and evidence-based strategy. Its most important work lies in long-term measures to **"increase societal resilience to disinformation"** while working on

continuous evaluation and further research. This is the correct approach: restricting efforts to countering each new method of spreading disinformation means treating the symptoms and not the cause. It is the long-term underlying problem – demand for anti-establishment discourse – that must be addressed, with the aim of eventually rendering disinformation ineffectual.

There is one **major weakness** to the Code. It **remains entirely voluntary**, and although all of the relevant internet media companies have signed up to it, **signatories may withdraw at any time**. They may even withdraw only from individual commitments, while technically remaining signatories. This means **that the success – or otherwise – of the methods listed in the Code will depend to a great extent on public awareness of its existence and pressure on the signatories to uphold their commitments in full.** The document does conclude with the suggestion that "the signatories may indicate on their websites or in commercial or other communications that they have signed the code" and that they should "take all reasonable measures to make their business contacts aware of the existence of the Code".[37] But this is not mandatory, and it is unclear whether it will form part of the reporting and evaluation of the signatories' efforts.

There is one major weakness to the Code. It remains entirely voluntary, and although all of the relevant internet media companies have signed up to it, signatories may withdraw at any time.

The Code of Practice was followed in December 2018 by a comprehensive Joint Action Plan, announced by the High Representative and the European Commission. The Action Plan's main purpose is to **ensure that the Code of Practice is properly implemented in good time before the European Parliament elections in May 2019**, and to complement this with further actions on a governmental level.

It begins with some clarifications of how the Code will apply in practice: the European Commission will **work closely with the online platforms** to ensure that they comply with their commitments, while simultaneously working on **supporting media literacy efforts, fact-checkers and researchers**. Platforms must report to the Commission once a month – an improvement on the yearly timeframe foreseen by the Code. If the Code proves to be insufficient, only then will further regulatory methods be considered – but this threat remains implicit as an incentive for the platforms to cooperate fully.

One important aspect of the fight against disinformation that is recognised in the Action Plan is **the need to increase positive messaging about the EU**, given that it is frequently a target of disinformation campaigns. The Action Plan declares that the Commission and the European Parliament will step up their communication efforts on Union values and policies. More importantly, it recognises that **pro-EU communication is more effective when it comes from the member states** rather than the EU institutions themselves. Accordingly, it recommends better efforts from member state governments to communicate more effectively about the EU, particularly its values. This indicates a level of awareness that combating disinformation is not merely about tweaking algorithms or adjusting advertising regulations: it must also involve a campaign to win hearts and minds.

The anti-establishment motive of coordinated disinformation means that action taken against it by EU bodies runs the risk of further alienating Eurosceptics inclined to perceive this as censorship. The Code of Practice clearly recognises this, opting to place the burden of responsibility for tackling disinformation on the private sector and civil society rather than making the EU an actor in its own right. The Action Plan, too, provides promising ideas in this direction. But its **main thrust is a considerably increased role for security services, an area where caution is needed**.

Some ideas are unlikely to be very controversial. For example, information-sharing will be facilitated by a **Rapid Alert System**, to be set up by March 2019, which will have a contact point in each member state and in the EU institutions and will be tasked with helping to coordinate responses to malicious disinformation. But the Action Plan also foresees a significant funding boost for the EU's existing 'strategic communications' efforts, including working with the European External Action Service to extend anti-disinformation campaigns from the Eastern Neighbourhood to the member states. This has already started to happen, and has not always had promising results.

This means that the success – or otherwise – of the methods listed in the Code will depend to a great extent on public awareness of its existence and pressure on the signatories to uphold their commitments in full.

3.5 *EU VS DISINFO* AND THE EUROPEAN EXTERNAL ACTION SERVICE

European military intelligence services currently operate several institutions and agencies whose main purpose is to monitor hostile (chiefly Russian) cyber activity, including disinformation, in the Eastern Neighbourhood and the EU member states. A Commission communication on the topic refers to these as "important elements in the cooperation between EU and the North Atlantic Treaty Organisation (NATO) to improve European resilience, coordination and preparedness against hybrid

interference".[38] One of these is a debunking service by the name of 'EU vs Disinfo'. This platform has faced some controversy, for reasons that will be explored below.

EU vs Disinfo sees the fight against disinformation as an extension of the EU's common foreign and security policy in the East; in other words, it is concentrated primarily against Russian propaganda efforts, especially in Ukraine, and the Russian state media's reporting on the EU. But it also tries to address disinformation circulating within the EU that repeats Kremlin talking points, even if unintentionally.

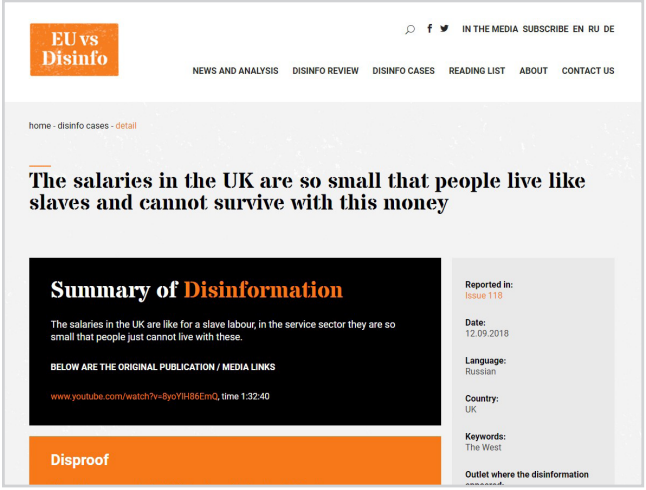
EU vs Disinfo is run by the European External Action Service's (EEAS) East Stratcom Task Force, and consists of a "compilation of cases from the Task Force's wide network of contributors".[39] Many of these contributors are NGOs and journalists, but specific information about the network's membership is not available on its website. It provides a database of disinformation cases, including where the story originated and a brief disproof. The service produces a weekly newsletter called 'Disinfo Review', which summarises recent disinformation stories that have been brought to the network's attention.

The East Stratcom Task Force has the role "to explain and promote the European Union's policies in the Eastern Neighbourhood".[40] Accordingly, EU vs Disinfo sees the fight against disinformation as an extension of the EU's common foreign and security policy in the East; in other words, it is concentrated primarily against Russian propaganda efforts, especially in Ukraine, and the Russian state media's reporting on the EU. But it also tries to address disinformation circulating within the EU that repeats Kremlin talking points, even if unintentionally.

In doing so, it oversteps its brief. **The Task Force has no domestic role, but in practice it does comment on domestic media**. The **EEAS is clearly the wrong actor for this, not least because it is not accountable in the same way the European Commission is**. Entrusting the policing of the EU's media and civic space to an EEAS platform essentially means that it falls under the brief of military intelligence, an elision that should cause as much concern as the regulatory worries expressed above.

This blurring of the boundaries also **downplays the role of disinformation that is made in Europe**, conflating Russian (state) propaganda and locally-produced material that uses similar messaging. **The fact that EU vs Disinfo was intended to deal with a specific kind of disinformation – pro-Kremlin messaging – and now finds itself trying to field the entire European media space reveals an imbalance in how the EU responds to different kinds of false material**. EU vs Disinfo's expansion is symptomatic of the steady growth of disinformation from a military intelligence issue in the Eastern Neighbourhood to a Europe-wide political problem, and while the issue has changed, the actor tasked with dealing with it has not.

In theory, this means that **the EU has a service that can call foul when a European media outlet repeats disinformation that can be linked in some way to Kremlin propaganda; but where no Russian link can be found, it must be silent**. In practice, the Task Force's definition of pro-Kremlin messaging is so wide that there does not appear to be any systematic approach to which stories it covers and which it does not. Much of the content on the database appeared in the Russian state media, but much did not, including anonymous social media material of unknown origin. Most entries relate directly to Russia in some way (common subjects in 2018 were the poisoning of Sergei and Yulia Skripal and the conflict in Ukraine), but they also cover subjects such as migration and integration in Europe. It is true that these subjects often appear in Russian messaging about the EU, but there is no way of knowing whether any individual story has Russian origins or not – especially when its coverage includes Russian "talking points" that may also be repeated by actors with no link to the Kremlin. The service's entire approach is slapdash and inconsistent, which is symptomatic of the enormous (and expanding) task it has been given.



Many of the narratives described as 'disinformation' by EU vs Disinfo are closer to partisan spin than outright falsehood. By claiming these as fabrications, the platform opens itself to the criticism of spreading 'fake news' itself, as in the Geenstijl case.

What is more, it is not clear who EU vs Disinfo's intended audience is: the punchy site design and brief story summaries would suggest the general public, while its outreach work seems to be directed towards specialists and the defence community. The tone is often derisive or dismissive rather than seeking to clarify and explain in good faith. **If the service's aim is to address those who may have been deceived by disinformation, this approach is unlikely to be successful**. Rather, it may entrench Eurosceptic readers in their views as they become frustrated by what they may perceive as patronising counter-propaganda.

When it crosses into the domestic media, EU vs Disinfo finds itself in the position where it must defend its choices. In January 2018, the Dutch online media outlet Geenstijl commenced court proceedings against EU vs Disinfo for its claim that Geenstijl and two other Dutch outlets had disseminated disinformation about Ukraine. The claim originated from a mistranslation, and Geenstijl's lawyers maintained that the articles contained only legitimate criticism of the Ukrainian government. EU vs Disinfo eventually retracted the claims, but in the meantime the Dutch parliament debated the case and passed a motion calling for EU vs Disinfo to be shut down, citing concern for its impact on freedom of speech and the lack of accountability for its claims.[41]

The tone is often derisive or dismissive rather than seeking to clarify and explain in good faith. If the service's aim is to address those who may have been deceived by disinformation, this approach is unlikely to be successful. Rather, it may entrench Eurosceptic readers in their views as they become frustrated by what they may perceive as patronising counter-propaganda.

The service's defenders cite the fact that, when the claims against the Dutch outlets were first published, **EU vs Disinfo had a very small staff and budget, meaning that mistakes were inevitable**. The solution, in their eyes, is to provide the platform with better resources, as foreseen by the Action Plan. This attitude does not take the problem seriously enough; **when passing judgement on European news outlets, the EU simply cannot afford to get things wrong**. The court case and parliament motion were a PR disaster, not least because the headline "EU anti-fake news service spreads fake news" proved irresistible to the media, mainstream and alternative alike. This demonstrates the particular vulnerability of the EU in the fight against disinformation: it depends on trust, which is in increasingly short supply.

EU vs Disinfo's greatest failing is its title. Especially given its origins as a tool of 'strategic communications' and its errors in the past, the name does little to promote the image of a fair and neutral arbiter of the truth: if anything, whether for invalid or valid reasons, it invites accusations of propaganda. It also does not fit into the initial European Commission strategy, which recommended limiting the EU's role as an actor in its own right. Combined with the lack of transparency regarding the composition of the network and the direct link to an agency whose purpose is to promote the EU (East Stratcom), **the result is a service that can do little to persuade sceptics that it is a reliable and neutral source of information**. However well-respected its role in fighting Russian propaganda in the Eastern Neighbourhood, EU vs Disinfo in its current form may be a liability in the fight against domestic disinformation. The recent scandal in the UK regarding the Integrity Initiative, an anti-disinformation charity that declared itself to be independent but was revealed to be funded by the British government, demonstrates the impact on public trust when a tool that seeks to fight against disinformation opens itself to conspiracy theories or accusations of hypocrisy.[42]

Given the role that Russian information warfare has played in seeking to influence elections across the West, it is understandable that the EU wishes to boost its defences. But **when it comes to the European domestic space, a prominent role for the EEAS and state security services may be counter-productive, playing into narratives of censorship and a culture war between 'the establishment' and 'the people'**. Certainly, the expertise and experience of East Stratcom in fighting propaganda in the Eastern Neighbourhood can be useful for domestic bodies, but European and national decision-makers should consider very carefully whether they are really the best tools in such a sensitive political environment.

Disinformation is best understood not as a security issue, but as a tool; it may be used by any actor, and resisting it effectively means not merely neutralising the actor, but building defences against the technique. There is a place for security services in the fight against disinformation, but it must work in harmony with the soft-touch comprehensive approach outlined in the Code of Practice.

Disinformation is best understood not as a security issue, but as a tool; it may be used by any actor, and resisting it effectively means not merely neutralising the actor, but building defences against the technique.

4. Recommendations

4.1 THE EU AND MEMBER STATES

As it is the highest level at which effective policy can be implemented and enforced, the EU remains the most promising level for action against disinformation: it is best placed to combat a cross-border phenomenon without the pressures of day-to-day national politics. In general terms, the **Code of Practice** and the **civil society/private sector aspects of the Action Plan** should be the priority: they err on the side of inaction, but this is preferable to clumsy or inappropriate action. There is a very real danger of making things worse.

Ultimately, the only truly effective way to fight disinformation will be to address the crisis of confidence in mainstream politics that is creating demand for alternative narratives, and this should be the first priority of any actor. In the meantime, however, **the focus of EU efforts should be to develop a supportive environment in which NGOs, civil society, the media and the wider private sector can construct the societal infrastructure needed to resist disinformation**.

- The Code of Practice is an excellent starting point, and it should remain at the heart of the European response to disinformation. Its **voluntary nature is a weakness, but compulsion would likely be counter-productive**. To keep the signatories bound to their commitments, the European Commission must therefore keep the option of regulation on the table as an incentive. **There must be consequences if signatories choose to withdraw from the Code** or specific commitments – the threat of regulatory measures that could be harmful to business practices should serve to keep the signatories committed to cooperation.

- Since it is implemented on a purely voluntary basis, the Code of Practice must be **widely advertised so that the public is aware of it** and can hold signatories to account. The Commission should insist that the reports, which signatories should submit each month, include details on their efforts to spread awareness among their users about the Code and what they are doing to meet their commitments. These **reports should be made public**, and the Commission should issue a **regular public evaluation** of how each signatory is doing, including recommendations of where improvements could be made.

- Fighting disinformation in Europe should **take place in the civil space** to ensure that actors are democratically accountable. There is a role for military strategic communications in countering state actor interference, but excessive concern over the influence of 'Russian bots' in European democracy risks neglecting the very real home-grown threat from populists, trolls and the far-right. The European public space must be reclaimed by the **European public, not by the EEAS or state security services**, and allowing the fight against disinformation to be framed as a national or European security matter rather than a domestic challenge will only contribute to further alienating a sceptical public. This is why the Code of Practice, with its focus on civil society and the private sector, should take priority over security sector actions.

- The policy expert consensus is that EU vs Disinfo provides a valuable service in the Eastern Neighbourhood; but to avoid playing into conspiracy theories or hostile narratives **its role within the EU member states should be reconsidered**. As a platform that casts judgement on whether something is true or false, it is potentially vulnerable to these criticisms and should tread carefully. Either it should be moved from the EEAS to the Commission (or better still, to an independent body not directly affiliated with political interests) and tasked with a specifically domestic brief, or it should restrict its operations to analysing Russian state media and propaganda in Ukraine and other Eastern Neighbourhood countries. In any case, it should be rebranded to remove the reference to the EU in its name, and if it seeks to convince as well as document then it should consider using more detailed disproofs and a more professional tone.

- The European Commission should expand its horizon beyond the hosts and distributors of online disinformation, and look into what it can do to **support not only NGOs but also private sector actors** with an interest in maintaining high informational standards in public life, as these have may have access to specialist knowledge and resources out of the reach of governmental actors. **A European-wide advertising blacklist of suspicious sites**, updated regularly with input from consultants or advertising agencies across the continent, would be an excellent start to cutting off the revenue stream that makes disinformation profitable.

- If national governments seek to legislate against disinformation, such as by expanding hate speech laws, they must tread carefully. **It should ultimately be up to the courts to decide what is disinformation and what is not, not private companies or politicians**. It is true that legal prosecution is too slow to be effective in preventing content from reaching large numbers of viewers. But the response should not be to use this argument to justify clamping down on media freedom, but rather to recognise the limits of legislating against disinformation and invest efforts elsewhere.

- The EU must ensure that **it does not overlook or permit threats to media freedom implemented**

in the member states in the name of fighting disinformation. The work of the Commission should be to find an approach that all of Europe can sign up to, and it should include **monitoring member state initiatives and crying foul where necessary**, particularly when they cross the line into censorship.

- Constant research and evaluation will be an important part of any strategy. The work of the High Level Expert Group was supplemented by a Eurobarometer survey on fake news and public trust in the media. **More regular opinion polling** on the subject – perhaps as part of the regular biannual Eurobarometers – would provide a useful data source which might help researchers to track the impact of trialled methods. This would provide not only snapshots but a better vision of change and development over time. This would be particularly useful for shaping the messaging of any public awareness campaign focused on media literacy (see section 4.3 below).

- The Action Plan rightly recognises that "pro-active and objective communication on Union values and policies is particularly effective when carried out directly by member states".[43] To counteract the rising force of Eurosceptic messaging, member state governments should make serious efforts to **involve citizens more closely in European politics and decision-making**. The European Citizens' Consultations are an example of good practice in this field, and they should be repeated and built upon as described in EPC's Evaluation Report.[44]

4.2 THE SOCIAL MEDIA PLATFORMS AND THE PRIVATE SECTOR

Putting responsibility on tech companies to curate and control what is posted on their platforms will only increase the influence they have over users' lives. It could also have a greater chilling effect than state regulation and is unfair on smaller platforms that will be disproportionately affected by the burden of responsibility. But at the same time, these social media companies hold the keys to the bulk of internet users' exposure to media content, including disinformation. If they are serious about their efforts to resist disinformation – and they should be – there are several things they can do to effectively collaborate with the EU and other stakeholders:

- In the interest of social responsibility, social media platforms should **guard their algorithms and research data less jealously**. This data, currently only available to in-house analysis, could be transformative for experts and researchers if it were available more widely, as it would provide a huge amount of information on which to base policy or research. It would surely result in a 'boom' in scientific knowledge of how content spreads online and how political views are shaped by media exposure.

- If the platforms are not willing to share research data on a voluntary basis, **the European Commission should consider legislation to mandate open access to data**. This would be strongly resisted by tech companies, who consider these to be business secrets. But given the central role they play in the media and information space today, it is unacceptable that these companies can sit on huge amounts of potentially revolutionary information and not release it for public research. This may involve a seismic shift in the sector's business model, given that their algorithms would become public domain, but there are likely many in the sector who already suspect that the current level of secrecy is unsustainable due to increasing public and governmental scrutiny. There is a strong case for readdressing the balance between tech giants and their users – whose data provides their profits – with a new 'social contract'.[45] This could be implemented in cooperation with the US, where the majority of tech giants are based, to the benefit of all social media users worldwide.

- Online platforms must be **sensitive to the needs of local media ecosystems** when experimenting with new features or anti-disinformation tools. It is vital that they do not cause harm to genuine, high-quality news content in their efforts to reduce disinformation, as has happened as a result of previous experiments. Any changes to the user experience should be made **in consultation with independent media outlets, NGOs and experts**, and preferably also with the input of other stakeholders in the framework of meetings between the Commission and the signatories to the Code of Practice.

- In particular, given that the European Commission is working on a holistic Europe-wide strategy, the platforms should **refrain from trialling new features only in individual markets**. Instead, their changes should apply simultaneously in all EU member states, so that all European citizens have the same online experience. This will simplify efforts to combat disinformation in Europe by eliminating unnecessary variation between countries. If the platforms wish to experiment with new features, they should find other means to do so, such as by taking a random selection of users across the whole of Europe. This will minimise any potential negative effects on local news ecosystems.

- Mainstream news media, meanwhile, should consider their **responsibility to be fair and not unduly partisan**. Competing alongside social media content and disinformation puts traditional media under enormous financial pressure, but they should ensure their credibility is not compromised in the process of adapting to online markets. They should consider that there remains a **healthy market** for news content that is *reliable*, and that having a well-regarded pedigree as a print or broadcast outlet gives them a valuable edge over online-only competitors. **Pluralism in the media environment** means not only pluralism in ideological positions and in news formats, but also **pluralism in tone**: clickbait may be a successful way of drawing in casual readers, but there remains a market share for more serious, respectable, and

high register content, which is still perceived as more trustworthy. Not all media outlets need to follow the fashions set by the internet age.

4.3 MEDIA CONSUMERS AND CIVIL SOCIETY

In the meantime, it may be that disinformation is here to stay and is simply part of how media is consumed in the information age. The methods described in this paper may help to reduce its reach and volume, but so long as the internet remains open to all (as it should), there will be malicious material lurking where it cannot be easily opposed.

Respondents to a Eurobarometer poll on the subject considered journalists to be the actors with the most responsibility to stop disinformation, followed by national authorities.[46] But they also placed a great deal of responsibility on the citizens themselves. That is, the public largely recognises its responsibility to exercise judgement about what it reads. But the citizens must not be alone in this.

- The only truly dependable strategy to counter 'fake news' will be to **change the way we as media consumers read the news**: by raising awareness of the importance of checking and comparing sources, applying scepticism to outrageous claims, and exercising informed judgement at all times, disinformation can be reduced from a dangerous political problem to just part of the background noise of our online experiences. Better media literacy can help more people to learn how to recognise the most common disinformation techniques.

- The European Commission's focus on **media literacy and education** reflects an understanding that investing in this field will have enormous pay-offs in terms of societal resilience to disinformation. A media literacy campaign could be led by the EU, national governments, or the NGO sector. Even the tech giants may wish to contribute funds as part of their public relations work.

- To be effective, media literacy efforts should target the most vulnerable groups as a priority. The task is to help those who are not already 'digital natives' to approach online content with the appropriate tools to tell fact from fiction. That means not restricting educational efforts to schools, but running a wider **public awareness campaign designed specifically to target older generations**, who are more likely to share fake news.[47]

- Ultimately the only thing likely to shift commercial practice is public opinion and the behaviour of their customers. This is difficult when it comes to social media and online news, since for the most part users 'pay' not with money but with attention. But in this field, attention is money – and if European citizens are unsatisfied with the efforts of a particular platform or outlet, **they must express it by choosing where to invest their attention**. It may seem that social media is a monopoly of a handful of big players, but where there is demand, alternatives are always available. Users should not feel that they have no choice but to accept whatever conditions prevail on their platform of choice.

The keyword is responsibility. The platforms that host news content; the governments that set the regulations; the readers that consume news: all these have a responsibility to ensure that European democracy is not threatened by disinformation's distortion of public opinion, nor by heavy-handed responses that threaten freedom of expression.

Conclusion: Safeguarding truth for the future

While some motives driving the spread of disinformation, just as the monetary incentive posed by advertising methods, are relatively simple to counteract, the demand for anti-establishment messaging created by a crisis of mainstream liberal democracy is a symptom of a much more worrying structural cause. It also means that any attempt to fight back against the disinformation problem must be very careful not to exacerbate the Eurosceptic and populist views that have enabled it in the first place. Existing measures, such as legislation with a chilling effect or EU bodies with poorly-defined roles, run exactly this risk.

If self-regulation puts too much power in the hands of tech giants, and state efforts encourage the very thing they are intended to fight against, more promising potential can be found among other stakeholders.

If self-regulation puts too much power in the hands of tech giants, and state efforts encourage the very thing they are intended to fight against, more promising potential can be found among other stakeholders. In particular, the possibility of private sector actors such as consultancies and advertising agencies bringing their unique expertise to the fight against disinformation has been overlooked by most commentators, despite some companies already working in this sector. NGOs, too, have more to contribute.

No single measure will be enough to counteract such a wide-ranging phenomenon, however. If society as a whole is to be made more resilient to disinformation, the best way of achieving this will involve sensitive cooperation between all these stakeholders, who should be brought together in a multi-stakeholder forum convened by the European Commission. It may be necessary for some actors, notably the social media platforms, to abandon commercial principles that have served them well in the past but are now facing public opposition. They should see this not as a surrender, but an investment in a sustainable future for their business model.

The media's principal role in a democracy is to create informed, empowered and engaged citizens who can participate in the democratic system on the basis of reliable and complete information. If we can render disinformation negligible and ineffectual, by way of multifaceted changes to regulation, greater private sector responsibility and increased media literacy, the internet will remain a potent and beneficial tool in shaping the resilient media and active citizenship that lie at the heart of a healthy democracy.

It may be necessary for some actors, notably the social media platforms, to abandon commercial principles that have served them well in the past but are now facing public opposition. They should see this not as a surrender, but an investment in a sustainable future for their business model.

[1] Pomerantsev, Peter, "How terrorists and provocateurs are using social media against western democracies", *New Statesman*, 14 January 2018, https://www.newstatesman.com/culture/books/2018/01/how-terrorists-and-provocateurs-are-using-social-media-against-western.

[2] For example, the report of the European Commission's High Level Expert Group on fake news and online disinformation considers that the label 'fake news' "has been appropriated and used misleadingly by powerful actors to dismiss coverage that is simply found disagreeable." European Commission Directorate-General for Communication Networks, Content and Technology (2018), *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, April 2018, p.5, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271. See also https://www.politico.com/story/2017/12/08/trump-fake-news-despots-287129.

[3] Silverman, Craig, "This analysis shows how viral fake election news stories outperformed real news on Facebook", *BuzzFeed News*, 16 November 2016, https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook#.eu5VB8wq3.

[4] "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy", New York: Freedom House, 2017, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

[5] European Commission, *Flash Eurobarometer 464*: Fake news and disinformation online, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183.

[6] CrossCheck, "Did Emmanuel Macron open an offshore account?", 5 May 2017, https://crosscheck.firstdraftnews.org/checked-french/emmanuel-macron-open-offshore-account/.

[7] Toor, Amar, "Germany grapples with fake news ahead of elections", *The Verge*, 19 January 2017, https://www.theverge.com/2017/1/19/14314680/germany-fake-news-facebook-russia-election-merkel.

[8] Crosby, Alan, "Fake news kicks into high gear in Czech presidential runoff", *Radio Free Europe / Radio Liberty*, 21 January 2018, https://www.rferl.org/a/fake-news-kicks-into-high-gear-czech-presidential-vote/28987922.html.

[9] Paul, Christopher and Matthews, Miriam (2016), "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It", Santa Monica: RAND Corporation, https://www.rand.org/pubs/perspectives/PE198.html; Bauerlein, Monica, "The Firehose of Falsehood", *NiemanLab*, December 2017, http://www.niemanlab.org/2017/12/the-firehose-of-falsehood/.

[10] *A multi-dimensional approach to disinformation*, p.5. The February 2018 flash Eurobarometer on 'fake news and disinformation online' puts the term *fake news* in italics, presumably to distance itself from the label.

[11] Mitchell, Amy; Simmons, Katie; Matsa, Katerina Eva; Silver, Laura; Shearer, Elisa; Johnson, Courtney; Walker, Mason and Taylor, Kyle, "Many Western Europeans get news via social media, but in some countries, substantial minorities do not pay attention to the source", *Pew Research Center*, 14 May 2018, http://www.journalism.org/2018/05/14/many-western-europeans-get-news-via-social-media-but-in-some-countries-substantial-minorities-do-not-pay-attention-to-the-source/

[12] Moore, Matthew, "BBC online criticised for "'pathetic" clickbait'", *The Times*, 15 January 2018, https://www.thetimes.co.uk/article/bbc-online-criticised-for-pathetic-clickbait-9cfdxgf73.

[13] Silverman, Craig, "Here Are 50 of the Biggest Fake News Hits on Facebook From 2016", *Buzzfeed News*, 30 December 2016, https://www.buzzfeed.com/craigsilverman/top-fake-news-of-2016?utm_term=.erMEDqRYR#.qrj5mk929

[14] Kirby, Emma Jane, "The city getting rich from fake news", *BBC News*, 5 December 2016, http://www.bbc.com/news/magazine-38168281.

[15] Sydell, Laura, "We tracked down a fake-news creator in the suburbs. Here's what we learned", NPR, 23 November 2016, https://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs?t=1533477289290.

[16] Silverman, Craig; Feder J., Lester; Cvetkovska, Saska and Belford, Aubrey, "American conservatives played a secret role in the Macedonian fake news boom ahead of 2016", *BuzzFeed News*, 18 July 2018, https://www.buzzfeednews.com/article/craigsilverman/american-conservatives-fake-news-macedonia-paris-wade-libert.

[17] RT, "RT weekly TV audience grows by more than a third over two years; now 100mn – Ipsos", 3 April 2018, https://www.rt.com/about-us/press-releases/ipsos-market-research-rt/.

[18] Patin, Katherina, "Why has a Kremlin-controlled news network become a hit in the West?", *Coda*, 31 January 2017, https://codastory.com/disinformation-crisis/information-war/honest-about-lying.

[19] Von Hammerstein, Konstantin; Hoefner, Roman and Rosenbach, Marcel, "Right-wing activists take aim at German election", *Spiegel Online*, 13 September 2017, http://www.spiegel.de/international/germany/trolls-in-germany-right-wing-extremists-stir-internet-hate-a-1166778.html.

[20] Ibid.

[21] Machado, Gary, "Facebook and the EU, or the failure of self-regulation", *BlogActiv*, 22 May 2018, https://guests.blogactiv.eu/2018/05/22/facebook-and-the-eu-or-the-failure-of-self-regulation/.

[22] Levin, Sam, "Mark Zuckerberg: I regret ridiculing fears over Facebook's effect on election", *The Guardian*, 28 September 2017, https://www.theguardian.com/technology/2017/sep/27/mark-zuckerberg-facebook-2016-election-fake-news.

[23] Newman, Nic (2018), "Journalism, Media, and Technology Trends and Predictions 2018", in *Digital News Project 2018*, Oxford: Reuters Institute for the Study of Journalism at the University of Oxford, p. 13, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-01/RISJ%20Trends%20and%20Predictions%202018%20NN.pdf.

[24] Lyons, Tessa, "Replacing disputed flags with related articles", *Facebook Newsroom*, 20 December 2017, https://newsroom.fb.com/news/2017/12/news-feed-fyi-updates-in-our-fight-against-misinformation/.

[25] Facebook (facebook), "@oliverdarcy We see Pages on both the left and the right pumping out what they consider opinion or analysis…", *Twitter*, 12 July 2018, 18:34 UTC, https://twitter.com/facebook/status/1017477222083411968?lang=en.

[26] Funke, Daniel, "A guide to anti-misinformation actions around the world", *Poynter*, 24 July 2018, https://www.poynter.org/news/guide-anti-misinformation-actions-around-world.

[27] Scott, Mark and Delcker, Janosch, "Free speech vs. censorship in Germany", *Politico*, 4 January 2018, https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/.

[28] Young, Zachary, "French Parliament passes law against 'fake news'", *Politico*, 4 July 2018, https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/.

[29] *International Press Institute IFEX*, "Hungarian taxpayers fund unique 'fake news' industry", 16 November 2017, available at: https://www.ifex.org/hungary/2017/11/16/fake-news/ ; Euractiv, "'Fake news' another weapon in Orban's illiberal Hungary", 10 April 2017, https://www.euractiv.com/section/freedom-of-thought/news/fake-news-another-weapon-in-orbans-illiberal-hungary/.

[30] Houska, Ondrej, "Business booming in Czech fake news industry", *EUObserver*, 31 July 2017, https://euobserver.com/beyond-brussels/138638; https://twitter.com/DanielKral1/status/950747323830763520.

[31] Edelman, 2018 *Edelman Trust Barometer Global Report*, http://cms.edelman.com/sites/default/files/2018- 02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf.

[32] Picchi, Aimee (2016), "As Breibart wages 'war' on Kellogg's, advertisers flee", *CBS News*, 2 December 2016, https://www.cbsnews.com/news/as-breitbart-wages-war-on-kelloggs-advertisers-flee/; Nicas, Jack (2016), "Fake-News Sites Inadvertently Funded by Big Brands", *The Wall Street Journal*, 8 December 2016; https://www.wsj.com/articles/fake-news-sites-inadvertently-funded-by-big-brands-1481193004.

[33] See https://www.konspiratori.sk.

[34] European Commission Directorate-General for Communication Networks, Content and Technology, *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, April 2018, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

[35] European Commission, *Code of Practice on Disinformation*, 26 September 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[36] Ibid. p. 3.

[37] Ibid. p. 10.

[38] European Commission, *Tackling online disinformation: A European Approach*, 26 April 2018, p. 16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

[39] EU vs Disinfo, About, https://euvsdisinfo.eu/about/ (last accessed 26 September 2018).

[40] European External Action Service, *Questions and answers about the East Stratcom Task Force*, 8 November 2017, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

[41] Jurjens, Emiel and van den Brink, Jens, "Some problems with EU measures against fake news, Dutch Media v EU", *International Forum for Responsible Media blog*, 17 May 2018, https://inforrm.org/2018/05/17/the-problems-with-eu-measures-against-fake-news-emiel-jurjens-and-jens-van-den-brink/.

[42] Ball, James, "When free societies copy Russian media tactics, there's only one winner", *The Guardian*, 9 January 2019, https://www.theguardian.com/commentisfree/2019/jan/09/free-societies-russia-misinformation-integrity-initiative.

[43] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation (JOIN(2018) 36 final): Action plan against disinformation*, 5 December 2018, https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation.

[44] See Butcher, Paul and Stratulat, Corina (rapp.) (2018), "The European Citizens' Consultations: Evaluation Report", Brussels: European Policy Centre, http://www.epc.eu/pub_details.php?cat_id=1&pub_id=8839&year=2018.

[45] As argued in Mazzucato, Mariana, "Let's make private data into a public good", *MIT Technology Review*, 27 June 2018, https://www.technologyreview.com/s/611489/lets-make-private-data-into-a-public-good/.

[46] European Commission, *Flash Eurobarometer 464*: Fake News and Disinformation Online, March 2018, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183.

[47] Goyanes, Manuel and Lavin, Ana (2018), "The sociology of fake news: factors affecting the probability of sharing political fake news online", *Media@LSE Working Paper #55*, London: London School of Economics, http://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/WP55.pdf.

NOTES

MISSION STATEMENT

The **European Policy Centre** is an independent, not-for-profit think tank dedicated to fostering European integration through analysis and debate, supporting and challenging European decison-makers at all levels to make informed decisions based on sound evidence and analysis, and providing a platform for engaging partners, stakeholders and citizens in EU policymaking and in the debate about the future of Europe.

The **European Politics and Institutions Programme** is one of the five thematic programmes of the European Policy Centre. It covers the EU's institutional architecture, governance and policymaking to ensure that it can move forward and respond to the challenges of the 21st century in a democratic and effective manner. The programme also monitors and analyses political developments at the EU level and in the member states, discussing the critical questions of how to involve European citizens in the discussions about the Union's future and how to win their support for European integration. It has a special focus on enlargement policy towards the Western Balkans, questions of EU institutional reform, and illiberal trends in European democracries.

With the strategic support of King Baudouin Foundation
Working together for a better society

With the support of Europe for Citizens Programme of the European Union