MONOGRAPH

Fake news, disinformation and the democratic state: a case study of the UK government's narrative

Noticias falsas, desinformación y el estado democrático: un estudio de caso de la narrativa del gobierno del Reino Unido

Notícias falsas, desinformação e o estado democrático: um estudo de caso da narrativa do governo do Reino Unido

Julian Richards
Director, Centre for Security and Intelligence Studies (BUCSIS)
(University of Buckingham)
http://orcid.org/0000-0003-0613-4264
United Kingdom

Reception date: 28 August 2020
Review date: 14 November 2020
Accepted date: 9 December 2020
Published: 1 January 2021
To cite this article: Richards, J. (2021). Fake news, disinformation and the democratic state: a case study of the UK government's narrative, *Icono 14, 19*(1), 95-122. doi: 10.7195/ri14.v19i1.1611

MONOGRAPH

Abstract

From the 2014 referendum in the UK on Scottish independence, a number of political leaders in the West have accused the Russian government of industrial-scale organised disinformation, designed to undermine the democratic process. A number of allegations have also suggested that the Kremlin has been providing financial and other aid to far-right groups in the West to disrupt the political process. In this analysis, the case study of the UK is taken in the period 2014-20. An examination is taken of current research on the scale and effect of organised Russian disinformation strategies; and the emerging official narrative in the UK government about how to deal with the problem. This narrative reveals a complex interplay between defending democracy, while maintaining a "hands-off" approach and ensuring that tech business is welcomed.

Key Words: *Intelligence; Disinformation; Democracy; Hybrid; Russia*

Resumen

Desde el referéndum de 2014 en el Reino Unido sobre la independencia de Escocia, varios líderes políticos de Occidente han acusado al gobierno ruso de desinformación organizada a escala industrial, diseñada para socavar el proceso democrático. Varias acusaciones también han sugerido que el Kremlin ha estado proporcionando ayuda financiera y de otro tipo a grupos de extrema derecha en Occidente para interrumpir el proceso político. En este análisis, se toma el estudio de caso del Reino Unido en el período 2014-20. Se examina la investigación actual sobre la escala y el efecto de las estrategias organizadas de desinformación rusas; y la narrativa oficial emergente en el gobierno del Reino Unido sobre cómo abordar el problema. Esta narrativa revela una interacción compleja entre defender la democracia, mientras se mantiene un enfoque de "no intervención" y se garantiza que los negocios tecnológicos sean bienvenidos.

Palabras clave: *Inteligencia; Desinformación; Democracia; Híbrido; Rusia*

Resumo

Desde o referendo de 2014 no Reino Unido sobre a independência da Escócia, vários líderes políticos do Ocidente acusaram o governo russo de desinformação organizada em escala industrial, destinada a minar o processo democrático. Uma série de alega-

ções também sugeriu que o Kremlin tem fornecido ajuda financeira e de outra natureza a grupos de extrema direita no Ocidente para interromper o processo político. Nesta análise, o estudo de caso do Reino Unido é realizado no período de 2014-20. Um exame é feito da pesquisa atual sobre a escala e o efeito das estratégias de desinformação russas organizadas; e a narrativa oficial emergente no governo do Reino Unido sobre como lidar com o problema. Essa narrativa revela uma interação complexa entre a defesa da democracia, ao mesmo tempo em que mantém uma abordagem "sem intervenção" e a garantia de que os negócios de tecnologia sejam bem-vindos.

Palavras chave: *Inteligência; Desinformação; Democracia; Híbrido; Rússia*

1. Introduction

In November 2017, the incumbent British Prime Minister, Theresa May, issued a strongly-worded attack on Russia and its activities in spreading disinformation and fake news. Speaking at the Lord Mayor's banquet in London, May accused Russia of a strategy to "weaponise information" in an effort to undermine the West. She said that Russia's activities were "threatening the international order on which we all depend" (Mason, 2017). The same narrative was repeated a few weeks later during a visit to Poland to bolster the political and military relationship between Warsaw and London (RT News, 2017).

Not normally one for such undiplomatic language, May's words underlined the fact that there has been no love lost between Britain and Russia in recent years; a situation hardly helped by the Skrijpal poisoning in early 2018.

Russia's response to the accusation of disinformation has been the unsurprising one of denial and doubt. As the state-backed news agency, RT News reported on the occasion of Theresa May's visit to Poland, "the British government is convinced that Russia interfered in the 2016 Brexit referendum, but has failed to produce any evidence to back up the claim" (RT News, 2017).

The objective of this paper is to critically address two questions: what evidence exists to accuse Russia of such a comprehensive strategy of undermining the political order through disinformation? Subsequently, how is the UK government articulating its response to the problem of organised Russian disinformation?

To address this objective, I review recent research on whether and how the supposedly malicious state actor of Russia has been conducting disinformation in the UK to disrupt the democratic process, including interference with votes, and alleged connections with extreme right-wing (XRW) organisations. An analysis is then undertaken of how this one particular Western state is conceptualising and narratising its response to the problem of malicious disinformation. This reveals a complex interweaving of "defending democracy", while still being seen to support freedom of speech, and not doing anything to harm the country's attractiveness as a centre for high-tech, internet-related business.

2. Material and Methods

In this analysis, the UK government's emerging narrative on organised Russian disinformation is viewed through the lens of a set of documents and commentary produced by the Digital, Culture, Media and Sport Committee of Parliament (DCMS) on "Disinformation and 'fake news'", which resulted from a formal inquiry launched in January 2017. The inquiry was triggered by growing concerns over potential interference in elections in democratic states, including the 2016 Brexit referendum and presidential elections in the US. The committee presented its final report to parliament in February 2019, and the government formally responded in May of the same year.[1] At around the same time, the DCMS committee and Home Office launched a white paper consultation process on "online harms", covering not only disinformation but the wider gamut of risks to society in the online space. (The process was triggered primarily by the death of a young person after viewing self-harm videos on the internet (DCMS and Home Office, 2020).) This was followed in July of the same year by the publication of a report by the parliamentary Intelligence and Security Committee (ISC), entitled simply "Russia", which looked at the range of alleged hostile activities by Russia against the UK and their security implications (ISC, 2020). The government formally issued its response to this report on the same day (HMG, 2020). Brief reference is also made to the parliamentary Defence Committee's inquiry into "hybrid threats" underway during 2019 (Defence Committee, 2019a, and b), although it should be noted that this inquiry has not proceeded beyond the evidence-gathering stage at the time of writing following the election of December 2019.

Media reactions to these reports were varied. The DCMS's final report had the misfortune to be published at the same time as a major political crisis in the Labour Party, relegating it much further down the news agenda than might otherwise have been the case (Ball, 2019). The Online Harms White Paper consultation process has also attracted little media attention thus far other than in specialist digital industry circles. To the government's chagrin, the same could not be said of the ISC's Russia report. This was published to a fanfare of criticism of the government for failing to take the problem of Russian interference seriously, and a clear insinuation that a clamour to welcome Russian money into London is clouding the willingness of the establishment to grip the problem (ISC, 2020b). The release of this report led to much wider national and international commentary than with the previous two examples, much of it critical not only of the UK but of Western states more generally for failing to accord due priority to tackling hostile Russian activity.

At this stage, it is worth defining a few key terms central to the debate. "Fake news" has become a much-used term, particularly following the election of President Trump in 2016. The concept implies deliberately falsified stories and reports, while "disinformation" arguably goes wider into a range of disrupting activities. The ISC's Russia report defines disinformation as "the promotion of intentionally false, distorting or distracting narratives"; and related "influence campaigns", which encompass a wider range of activity such as illicit funding or "hack and leak" activities (ISC, 2020a: 9). In this way, disinformation activities do not just involve completely false information, but can also encompass inflammatory or disruptive commentary on existing events.

"Trolls", meanwhile, are malicious actors in social media who generate and promulgate disruptive messages. These can be human actors; automated actors ("bots"); or a combination of the two in the shape of humans using algorithmic mechanisms to spread disinformation ("cyborgs"). Evidence is emerging of organised groups, known as "troll factories", such as the St Petersburg-based Internet Research Agency (IRA) conducting industrial-scale disinformation (Booth, Weaver, Hern, Smith and Walker, 2017). Some disinformation activities involve generating a seemingly authentic debate between two opposing views, in which one of the participating actors

is false ("sock puppets"). Completely false grassroots social media communities can also be generated: a process called "astroturfing". These processes underline the fact that not all disinformation is "fake news" as such: the general aim appears to be to create environments of confusion, doubt and division, using a complex combination of false, biased, emotive and inflammatory commentary.

2.2. Disinformation in the UK : the evidence base

The review period in question in this analysis begins with the Scottish independence referendum of September 2014, when some of the organised disinformation activities with which we have become more familiar in recent years began to manifest themselves. Polls before the vote had suggested a close-run situation, but the eventual outcome was a vote for Scotland to remain in the UK with 55.3 percent, against 44.7 favouring independence.

As soon as the First Minister of Scotland and leader of the Scottish Nationalist Party (SNP), Alex Salmond, publicly accepted the verdict on 19 September 2014, claims of electoral malpractice began to circulate online (Nimmo, 2017). A key source of analysis of the alleged Russian disinformation activities in this period was a comprehensive report by Ben Nimmo of the Atlantic Council's Digital Forensic Research Lab (DFRL), which the UK government has taken as its key source of commentary on interference with the Scottish vote (see DCMS, 2019a: 71).

Just under two years after the vote, the Brexit referendum confounded the pollsters with a narrow margin in favour of leaving the EU. The shock of the result led many to raise allegations of electoral manipulation. Interestingly, these included not only claims of Russian disinformation and influencing operations, but also problems closer to home in which the victorious "Leave" campaign was accused of flouting electoral regulations on funding and messaging (BBC, 2018). It also became apparent that a Canadian data mining company called Aggregate AIQ had a potentially pivotal role in assisting the Leave campaign by targeting carefully engineered messages at traditionally reluctant voters. There is no credible suggestion this company had anything to do with Russian interference.

Following the vote, a number of allegations arose concerning potential illicit funding by Russia for the Leave campaign, some of which culminated in the launching of an investigation by the National Crime Agency (NCA) into funding for the campaign from the millionaire businessman, Arron Banks. This investigation formally cleared Banks of Russian-related wrongdoing in September 2019, stating that the NCA had "found no evidence that Mr Banks or his companies had received funding from 'any third party'" (Electoral Commission, 2020).

Other allegations also suggested links between the Kremlin and right-populist or XRW organisations in the UK to influence the vote. The former leader of the UK Independence Party (UKIP) and subsequently of the Brexit Party, Nigel Farage, has been a regular commentator with the Russian state-backed media company RT News, frequently criticising the democratic credentials of both the UK and the EU. He has also been very careful to never criticise democracy in Russia (Wintour and Mason (2014)). The former leader of the more extreme British National Party (BNP), Nick Griffin, was once invited to observe Russian parliamentary elections in 2011. (Unsurprisingly, he described the polls as "robust, transparent and properly democratic" (BNP, 2011).) More recently, the founder of the English Defence League (EDL) and periodic influencer of XRW opinion in Britain, Tommy Robinson, has also been fêted in Moscow and said nice things about Russia and its political system (Free Russia Forum, 2020). There is evidence that Robinson has been used by Russian disinformation actors as a conduit for influencers on divisive issues such as terrorism and anti-Islamic sentiment in the UK (Innes, 2017). This involves a process whereby Twitter accounts with large numbers of followers can be targeted for messages (known as "@-ing"), thus substantially increasing the readership of such messages. Meanwhile, Paul Golding, the leader of the XRW group, Britain First, was invited to speak in the Russian Duma in 2019 alongside a number of other ultra-nationalist European leaders (Carroll, 2019). That such an extreme figure with a number of convictions for assault should be received at the top table of Russian politics, seems surprising to say the least.

3. Result

3.1. Russian interference: evidence and effect?

Taking all of the above evidence into account, it could be said that there is something of a mixed message concerning how much organised disinformation has been going on in the UK, and – perhaps more importantly – how much of a real effect it has had on the democratic process.

On the one hand, it cannot be denied that some degree of organised disinformation, a significant proportion of it conducted at the hands of the IRA in St Petersburg, has been going on. Indeed, there may have been much more than has been picked up, and it may be becoming ever more sophisticated and difficult to spot, especially where it uses humans or cyborgs rather than bots (Llewellyn, Cram, Hill and Favero, 2019: 1161). As with so many issues connected with this debate, the nature of the IRA's direct connection with the Kremlin is murky. The organisation is owned by Yevgeny Prighozin, a catering mogul who certainly knows Putin well, and who has become the subject of US sanctions for alleged interference in elections (BBC, 2019). Exactly how far Prighozin and the IRA are directly tasked by, or connected with, Putin and Russian government policy, however, remains a matter of speculation.

A report by Cardiff University's Crime and Security Research Institute examining Russian influence operations in and around a series of terrorist attacks in the UK in 2017, was robust in its conclusions. The report identified "systematic use of fake social media accounts" by Russian disinformation agents in an attempt to "engineer social division" at a scale that "is considerably more extensive than has been reported to date" (Innes, 2017: 1). Following the terrorist knife attack on London Bridge, for example, researchers identified 140 messages promulgated by fake social media accounts, which accounted for more than 57,000 reposts (Innes, 2017: 2). One of the more infamous episodes involved the tweeting of an image of a Muslim woman walking past a stricken policeman on London Bridge by the fake SouthLoneStar account, which has been linked with the IRA and was previously used for disinformation during the 2016 US presidential elections. The inflammatory and Islamophobic message that accompanied the tweet was picked up by two

mainstream media outlets in the shape of the Mailonline and Sun websites (the former of which claimed in 2012 to be the most widely-read newspaper website in the world, with over 45 million users; Daily Mail, 2012), before it was revealed as being bogus and completely unfounded in its allegations (Booth et al, 2017).

By using techniques such as "@-ing" of Twitter users with large followings; astroturfing supposed grassroots movements; or being picked up by more mainstream media channels as the above example illustrates, disinformation agents can utilise what a 2016 report by the RAND Corporation called the "firehose of falsehood propaganda model" (Paul and Matthews, 2016). In this model, the rapid and extensive promulgation of false or disruptive messages on social media can exploit cognitive tendencies to accord more respect to messages that are seen often; are reported by multiple sources; or are seen to be shared extensively. By using "high-volume and multichannel" methods enabled by troll factories, disinformation agents can ensure large numbers of people take on-board disinformation at rates faster than subsequent denials or debunking can mitigate (Paul and Matthews, 2016: 2-3). In a sense, once the messages are out, the damage is done.

It can also be reasonably postulated that the aim of such disinformation strategies is not necessarily to directly support one side or the other in an election or debate, but to create a general fog of uncertainty and doubt about "truth", thus undermining the liberalist norms in Western democratic society. In many ways this connects with the strategy adopted by right-populist and XRW organisations, which dismiss established and mainstream Western media channels as purveyors of "fake news" in the grips of conspiratorial liberal elites. This, in turn, sows doubt in the populace about which items of news are reliable and which are not. As one witness to the Defence Committee's 2019 inquiry into hybrid threats noted:

> It doesn't really matter whether something is fake or not; what matters is that people think it's fake. That really damages their trust in our institutions. (Defence Committee, 2019a).

In their detailed analysis of IRA activity, Dawson and Innes (2019) noted a high degree of "narrative switching" in specific disinformation accounts they were

following. In the case of one particular Twitter account commenting on German politics for example, messages clearly switched over time between pro-Merkel and pro-AfD commentary: two very opposing positions (Dawson and Innes, 2019: 6). Commenting on the publication of the ISC's report on Russia in the UK, Owen Matthews drew parallels with the "useful idiots" policy of the Cold War, in which the Soviet Union duped sympathetic commentators in the West to do their propagandising for them. The effect, claims Matthews, is to "bring discord in place of harmony" (Matthews, 2020: 11).

The alleged interference in the 2014 Scottish referendum included the circulation of a video framing the failure of the independence bid as part of the wider "elite New World Order" conspiracy against the will of the people; allegedly viewed over 800,000 times (Nimmo, 2017). Another key message concerned what became known as the "Boom!" video. This comprised a short clip alleging to be a clear and incontrovertible example of ballot-box interference during the Scottish referendum, but which turned out to be footage from Russian elections in 2012 (Nimmo, 2017). Also influential was a report by a Russian election observer from Moscow's Public Institute of Suffrage attending the Scottish referendum, who claimed that the vote "did not meet international standards" (Harding, 2014). The comment was reported in sections of the international press, and led to a number of calls for a revote, including a "Rally for a Revote" petition through the Change.org online organisation. Nimmo notes that this petition achieved a "remarkably high" number of votes, which "raises the question of whether an attempt was made to artificially amplify the signatures" (Nimmo, 2017).

An extensive analysis of Brexit-related Twitter activity by Llewellyn et al (2019), also quoted in the government reports under scrutiny in this analysis, found that a number of Twitter accounts believed to be related to the IRA, which were active in disinformation activities during the 2016 presidential election in the US, had also been involved in promulgating disruptive information around the time of the Brexit vote. 419 such accounts were found amongst a set of 2752 released by Twitter in 2017 in response to the US Congress investigation into the 2016 polls, and the time-lag between the activity and subsequent analysis suggests there could have been much more disruptive activity going on at the time (Llewellyn et al, 2019:

1152). The study noted that the activity was "consistent with known Kremlin disinformation approaches, and 'active measures'" (Llewellyn et al, 2019: 1162).

However, the same study noted that the amount of observed commentary on Brexit by identified troll accounts was relatively small, and that most of the activity was after the actual vote itself. Indeed, on the Brexit referendum polling day, the amount of activity by identified troll accounts within the sample set of over a million tweets represented just 0.037 percent of overall activity (Llewellyn et al, 2019: 1153). The conclusion to be drawn may be that such trolling activity was not designed to alter the outcome of the vote itself, but had a more strategic purpose of laying the groundwork for longer-term astroturfing campaigns about political views in the West in general (Bastos and Mercea, 2017).

These small figures accord with other recent research on disinformation-linked activity on social media. In their analysis of "fake news" on Twitter during the 2016 US presidential campaign, for example, Grinberg, Joseph, Friedland, Swire-Thompson and Lazer (2019: 377) found that "the vast majority of fake news shares and exposures were attributable to tiny fractions of the population".

Similarly, analysis of fake news during the same elections on the Facebook platform by Guess, Nagler and Tucker (2019) provides a further level of detail on the structural factors within different communities coming into contact with disinformation. These findings suggested that slightly more conservative voters (Republican in the US context) and slightly more users in the older age bracket (65 years and above in this particular study) were more likely to recirculate fake news stories they encountered than other groups. This last point may have some implications for policies targeting digital literacy across the population, but it should be noted that the overall sharing of fake news stories "was a rare activity" compared to overall traffic flows during the election (Guess et al, 2019: 1).

This point reminds us of the question of "echo chambers" and "filter bubbles" and the effect they have on wider political opinion. A normative hypothesis may be that, if people tend to restrict their interactions with largely like-minded people and sources, then the wider effect of disinformation will be relatively con-

tained within closed groups. But again, research sows potential doubt. Bakshy, Messing and Adamic (2015: 1130-1) found that social media users' friends lists were more important in defining their online interactions than political views per se, and these could introduce much diversity to the items being shared and viewed (depending, of course, on the nature of one's friends).

Research by Flaxman, Goel and Rao (2016) on a sample set of US-based web users added to the uncertainty. In this research, two seemingly counterposed theories were supported by the dataset. On the one hand, there was evidence of "higher ideological segregation" in the items selected from social media and web-browsing than was the case with direct visits to established news sites, suggesting an echo-chamber effect. At the same time, the social media and web-based channels accessed in this way were more open to diverse political views than the news sites, suggesting that such users were more likely to be exposed on those channels to diverse perspectives (Flaxman et al, 2016: 318). This last point adds weight to the sense that disinformation in the online environment may have less overall effect than is sometimes supposed, and is a small part of the total landscape.

The official UK government reports under scrutiny in this paper support the view that evidence for organised disinformation is sometimes scanty and uncertain. The government's official written response to the final DCMS report on "Disinformation and 'fake News'" notes that "there is no evidence that Britain's elections or referendums have been compromised by foreign interference", even if "it is right that the Government safeguards against future risks" (DCMS, 2019b: 16). Meanwhile, the ISC's "Russia" report, while being very critical of the government's approach to the issue, confined itself to evidence of disruptive activity being undertaken around the time of key votes, but admitted that "the impact of any such attempts would be difficult – if not impossible – to assess, and we have not sought to do so" (ISC, 2020: 12). This accords with analytical judgements above, suggesting that, while there is reasonably clear evidence of organised disinformation being undertaken by certain actors, the extent and effect of that that activity is very difficult to determine and may have much less impact than is sometimes suspected.

Similar uncertainty revolves around the issue of direct support to populist and XRW organisations and leaders. There is a general concern in the UK, highlighted in the ISC "Russia" report, about the prevalence of Russian oligarchs with connections with the Putin regime who move very considerable amounts of money through London. Indeed, the NCA is engaged in a number of investigations into "illicit financial activity" in the capital (ISC, 2020: 16). We have also seen how right-populist and XRW leaders, such as Nigel Farage, Nick Griffin, Tommy Robinson and Paul Golding, have had flirtations with Russia and the Kremlin in the shape of media interviews, visits (official and otherwise) and social media commentary in which Russia is portrayed in a comparatively much better light than supposedly elitist Western regimes.

On the financial front, despite frequent allegations of Kremlin links, there appears to be very little hard evidence of Russian government money directly funding such leaders and organisations. Indeed, one of the very few verified examples of financial connections between Russia and Western European XRW organisations concerns a loan of nine million euros made to the Front National (FN) in France by the First Czech Russian Bank, in the run-up to the French presidential elections in 2014 in which the FN's Marine Le Pen reached the final stage (Sonne, 2018).

The uncertainty is not to say that such financial connections are not real, and detailed investigative journalism by the likes of the Guardian's Carole Cadwalladr frequently suggest there will, in time, be a pot of Russian gold to be found at the end of the rainbow concerning such parties as UKIP (Cadwalladr, 2018). But very little of clear substance has yet been established. This may be because logic suggests the Kremlin would not want to be seen to be openly financing XRW parties that are clearly unpalatable to the majority of the Western electorate. At the same time, the fundamental problem with attribution of hostile influence operations to specific state actors such as the Kremlin, and the particularly complex way in which supporters and sympathisers of the Putin regime may act in its interests without being directly tasked with doing so, mean that allegations of illicit Russian funding of XRW organisations remains a subject worthy of investigation.

3.2. The government's narrative in response

On conducting a narrative analysis of the three key governmental publications under scrutiny, it can be argued that the following three key themes emerge.

3.3.1. Theme 1: Defending democracy

All of the publications under scrutiny frame the potential problem of disinformation as a serious one not only for particular states, but for the very "fabric of democracy" (DCMS, 2019a: 5). Their commentary falls under a wider cross-parliament research project, announced in July 2019 and involving the House of Lords and the Cabinet Office, called the Defending Democracy Programme. This plans to look at ways to "protect and secure UK democratic processes", including the need to "promote fact-based and open discourse, including online".[2]

In the DCMS Inquiry's final report, democracy is mentioned nine times. On two occasions, this refers to a Canadian parliamentary committee report published the previous year, entitled "Democracy under threat: risks and solutions in the era of disinformation and data monopoly" (House of Commons, 2018). The title and content of the Canadian report mirror a key focus subsequently identified in the DCMS report, namely that the risk to democracy is perceived to arise not only from the actions of hostile disinformation agents themselves, but also from the role of the major social media service providers on whose channels the disinformation is promulgated, such as Twitter and Facebook. This is an important point to which I return below in the second theme. In the meantime, the risks to democracy from disinformation are highlighted as emerging from a general slide towards polarisation of public debate, which "reduces the common ground on which reasoned debate, based on objective facts, can take place" (DCMS, 2019a: 5).

The Online Harms White Paper mentions democracy slightly less often, taking as it does the primary concern of the safety of online users from harmful content. It does, however, mention the importance of "a thriving democracy and society, where pluralism and freedom of expression are protected" (DCMS and Home Office, 2020: 3). In this factor we can see a further nuance around the question of defending democracy, namely the conundrum posed to a liberal democracy in balancing control

and regulation of the online space while not reneging on the core principles of freedom of speech. Controlling organised disinformation may be needed, but not at the expense of being seen to quash and expunge unwelcome discourse and commentary.

This is one of the key problems for the government when it comes to confronting the major social media service providers, as outlined in the second theme below. One of the issues is whether such corporations should be re-classified from "platform" to "publisher" (DCMS, 2019a: 89). At the moment, holding the former status means the corporations can absolve themselves of responsibility for moderating content on their platforms, much as would be the case with a telephone company having responsibility for the content of conversations on the phone lines. If they were re-classified as publishers, the social media corporations would then need to accord to a range of statutes and regulations, as do the press and electronic media providers. But, as is the case in those areas, the government does not want to be too heavy-handed in regulating the media, lest it be seen to be becoming authoritarian. In a state that prides itself on freedom of expression, these are dangerous regulatory waters to enter.

The ISC Russia report is more direct about the threats to democracy, drawing a contrast between the lack of democracy in Russia, which allows its intelligence services to act with a degree of impunity (ISC, 2020: 1); and the democratic ideals of the UK. With that said, the ISC notes that the UK's intelligence services also have a responsibility. Here, again, is another conundrum for a liberal democracy such as Britain. Much as is the case with the risks of being seen to regulate freedom of expression too much, there are also risks in allowing the security agencies to be seen to have too great a remit in scrutinising and possibly even interfering in the democratic process. The Russia report notes that:

> Whilst we understand the nervousness around any suggestion that the intelligence and security Agencies might be involved in democratic processes – certainly a fear that is writ large in other countries – that cannot apply when it comes to the protection of those processes ..... Protecting our democratic discourse and processes from hostile foreign interference is a central responsibility of Government, and should be a ministerial priority (ISC, 2020: 11).

The ISC feels, therefore, that UK intelligence agencies absolutely should become more involved in regulating Russian disinformation, and that this is a task little different from countering Communist subversion during the Cold War. The difficulty for the democratic state in this area, however, is partly a legal and constitutional one. Ohlin (2018: 10) highlights an argument often presented by international lawyers, that freedom of speech means that anyone should be allowed to pass comment in an electoral process, even if they are not inside the country in question. Foreign media, for example, can and continually do comment on American elections or those in any number of democratic countries. So are Russia-based commentators within their rights to pass comment on US elections, even if their comments are inflammatory?

The US intelligence community, furthermore, has made a point of reminding us that, while it has a job to monitor the activities of hostile foreign actors, it is not mandated to "analyze US political processes or US public opinion" (Ohlin, 2018: 13, n49). Memories of the Watergate Scandal in the 1970s mean there is a particular aversion to US state intelligence agencies being seen to be too close to the domestic political and democratic process.

The UK government takes a similarly careful approach to the question of directing its intelligence agencies to intervene in the situation. In its formal response to the DCMS Inquiry's final report, it notes that:

> In the UK, the Government does not, and cannot, direct the police, Electoral Commission or the Security Service to investigate particular allegations. These organisations are operationally independent of Ministers and take a professional view of the necessity and proportionality of using their investigative powers (DCMS, 2019b: 17).

Interestingly, in March 2020, the government did publicly announce that an intelligence coordination group called the Joint State Threats Assessment Team (JSTAT) had been established three years earlier, within the Security Service's headquarters building in London.[3] It can be presumed this is modelled very much on the counter-terrorism Joint Terrorism Analysis Centre (JTAC), with both groups

recognising the need to coordinate strategic intelligence on complex contemporary threats across multiple agencies.

3.3.2. Theme 2: An arm's length approach?

The approach of the government of wanting to seem at arm's length from the operational decisions of the security services is part of a wider narrative of questioning exactly how far the problem of organised disinformation is a sole concern of central government. In some ways, this relates to two themes in post-Cold War security strategy more broadly. The first is a recognition that the contemporary security threat landscape is arguably much more complex and multi-faceted than was the binary confrontation during the Cold War (Richards, 2012: 11). Much of the thinking of how to respond to the picture has been spearheaded by counter-terrorism strategy, particularly since the 9/11 terrorist attacks in 2001. This has led to a "broadening" of security strategy (Gill, 2006: 30) not only in terms of the number of issues "securitised" by governments, but also of the range of stakeholders within and beyond government who are considered appropriate players in the strategy. Examples include the increasing penetration of private military and security companies (PMSCs) into post-Cold War military operations, but also, in the cyber domain, the role of private cybersecurity providers and the information and computing industry more generally.

The narrative in this strategic shift has increasingly centred around a notion of "resilience". As Coaffee, Wood and Rogers (2009: 1) describe, "the push for resilience is thus a response to existential or material vulnerability, insecurity and, ultimately, change". Initially emerging in the area of ecology, the concept is now freely used in a range of settings, from the environment to cyber security. As well as leading to a proliferation of issues to tackle in what Ulrich Beck described as "risk society" (Beck, 2006), the notion of societal resilience leads to a complex "multiplicity of subjectification processes" (Cavelty, Kaufmann and Kristensen, 2015: 8): namely, a complex interweaving of power and responsibility relations between the state and its citizens in delivering security.

Critics would suggest that this leads to a "depoliticization" of security policy (Power, 2004), in which the government can not only use repressive measures un-

der the guise of a resilient security strategy without facing much debate; but can also blame others when things go wrong.

Analysis of the UK government's response to the problem of disinformation suggests arguments for and against such a critical view. Firstly, there is clear evidence that the government sees the problem not as one for which it is primarily responsible, but one that will involve a partnership of government, citizen and private corporation. On the citizen front, there is much talk across all of the documents about digital and media literacy. The Online Harms White Paper consultation document, for example, describes a "media literacy strategy", which:

> … will ensure a coordinated and strategic approach to online media literacy education and awareness for children, young people and adults. It will aim to support citizens as users in managing their privacy settings and their online footprint, thinking critically about the things they come across online (disinformation, catfishing etc), and how the terms of service and moderating processes can be used to report harmful content (DCMS and Home Office, 2020: 9).

On the question of the involvement of corporations, there is clear evidence that the government is sympathetic to a growing chorus targeting large social media companies who may be using their size and influence to absolve themselves of responsibility for the problem of disinformation. I have argued elsewhere that, in one sense, this could be a skilful shifting of attention by the democratic state away from questions of its own involvement in massive data mining and digital surveillance, capitalising on public sentiment frequently suspicious of mega-companies and their avoidance of tax liability (Richards, 2019: 37). This could be seen in the way in which the purported founder of the internet, Tim Berners Lee, clearly shifted his critical commentary around 2018 away from a new surveillance law introduced by the UK government in 2016, towards "big tech" and the major social media corporations (Richards, 2019: 37).

In this way, the DCMS Inquiry's report clearly have what they call the "big tech companies" in the crosshairs, describing them at one stage as "digital gangsters" (DCMS, 2019a: 42).

The government's response broadly agrees, and identifies a range of forward-leaning measures against such companies, including "a statutory Duty of Care and Codes of Practice, enforced by an independent regulator" (DCMS, 2019b: 3), backed up by "the ability to levy substantial fines" for non-compliance (DCMS, 2019b: 5). There is also mention of establishing a requirement for the companies to "submit annual transparency reports and provide additional information to inform their oversight or enforcement activity" (DCMS, 2019b: 5); and a reminder that, in the Chancellor's 2018 budget, an announcement was made of a new "digital services tax" on the UK revenues of the big technology companies of two percent (DCMS, 2019b: 6).

A contrary position to government depoliticization of the threat, is that concerning the aforementioned democratic and legal arguments. The government could reasonably argue that, in a liberal democratic society, the way to deal with disinformation on social media channels is not to intervene itself in a covert or authoritarian way, but to ensure appropriate regulation and licensing of those companies operating in the UK space. This would chime with the ideological inclination of "small state" Conservativism of Boris Johnson. It could also be argued that the government would not have any legal mandate to control or shape the nature of information circulating on the internet, nor, indeed, to have any powers to control the activities of disinformation agents in foreign jurisdictions with whom there are very poor mechanisms for mutual legal assistance. In this way, the government frequently stresses the independence of the regulator (in the shape of the Information Commissioner's Office) and their codes of practice; and also references a range of other stakeholders in the process, including: the National Crime Agency (NCA) ; Competition and Markets Authority (CMA); Ofcom; the Electoral Commission and the Advertising Standards Agency (DCMS, 2019b: 2). All of these are independently managed government agencies but not direct government departments.

The answer is probably somewhere in the middle: while the UK government is clearly trying not to step into undemocratic authoritarianism in its approach to the problem, it is clearly tapping into the zeitgeist of public ire against bloated social media corporations, who have recently been under heavy fire in a number of investigations and inquiries on both sides of the Atlantic.

3.3.3. Theme 3: Welcoming tech business

The third and final theme that clearly emerges from the government publications and processes under scrutiny here is the need to delicately balance control and regulation of the tech sector, with not discouraging it from investing in the UK. For the political reasons described above, the government clearly wishes to tap into the public disenchantment with the behaviours of the major social media companies, but at the same time, it does not want to be so hard on them that they decide to take their business elsewhere.

For the UK, there is clearly a particular issue at the time of writing about post-Brexit economic strategy. The UK commenced the nominally one-year final process of leaving the EU on 1 January 2020. The preamble to the Online Harms White Paper consultation documents states:

> ..we want to make the UK the safest place in the world to be online and the best place to start and grow a digital business……By getting it right, we will drive growth and stimulate innovation and new ideas, whilst giving confidence and certainty to innovators and building trust amongst consumers. As we leave the EU, we have an incredible opportunity to lead the world in regulatory innovation (DCMS and Home Office, 2020: 2).

In this way, like many post-industrial states, the UK wishes to invest heavily in the burgeoning tech sector and to send the message that it is an attractive, and – crucially – relatively bureaucracy-free place in which to set up and grow a new tech business. The sub-text here may be a somewhat political one, that the rest of the EU may be relatively more bound by directives and regulations emerging from Brussels than a post-Brexit UK. Interestingly, the DCMS Inquiry's final report describes fairly punitive new laws in Germany and France and suggests that they have delivered "practical evidence that legislation can work" in targeting the big tech companies (DCMS, 2019a: 13). In the case of Germany, for example, a new law passed in 2018 called the Network Enforcement Act (NetzDG) levies a requirement on social media companies to remove "hate speech" on their networks within 24 hours, or be fined 20 million euros. As a result, Facebook has allegedly installed one sixth of all of its global moderators in Germany to ensure compliance (DCMS, 2019a: 13).

While these examples may seem compelling, the UK government may see opportunity in placing some clear blue water between itself and its erstwhile EU partners in these areas of legislation. It is interesting that the government response to the DCMS's point above describes its view that "a regulatory model which focused solely on liability for the presence of illegal content would not incentivise the sort of systematic improvements in governance and risk management processes that are necessary" (DCMS, 2019b: 3). Use of the word "incentivise" is significant here: it suggests an approach of working with tech companies rather than against them in a confrontational way. It also seems to be the case that the UK wishes itself to be a thought-leader in developing regulations and laws relating to the internet and associated technology industries, thus off-setting a potential post-Brexit loss of influence on the world stage.

Similarly, the Online Harms consultation process clearly revealed an anxiety about too much regulation being imposed. This presumably resulted from inputs to the consultation process from tech businesses themselves. The White Paper consultation document notes that regulation should be "proportionate"; and that fewer than five percent of businesses would actually be subject to the proposed new regulatory measures described above (DCMS and Home Office, 2020: 4). This sends the message that, where there is going to be a robust approach to regulation in the online space, it will mostly be targeted at the small number of very large tech businesses such as Facebook and Twitter. For the vast majority of other businesses, the message is that the UK will remain very much regulation-lite.

4. Discussion and conclusion

The supposed Russian strategy of "hybrid warfare" (Wither, 2016) has increasingly shaped Western conceptions of post-Cold War security. The narrative has been present to a certain extent long before the more recent period, with some suggesting a continuity with Soviet-era *dezinformatsia* active operations (Shultz and Godson, 1984; cited in Llewellyn et al, 2019: 1149). Meanwhile, a more recent shift towards disruptive "populist" politics in the West, has opened opportunities – potentially – for a Russia interested in undermining a combative European Union (EU) and its trans-Atlantic partners. In the area of election interference, concerns

have swirled not only around Scottish and Brexit referenda and the election of President Trump; but also the rise of Emmanuel Macron in France (Hansen and Lim, 2019); the (unauthorised) Catalonian independence referendum in Spain in 2017 (Maness, 2018); and the waning of Angela Merkel's long political career in Germany (Stelzenmüller, 2017), to name but a few.

There have also been numerous allegations concerning Russian funding for disruptive right-populist and XRW groups . It is alleged that parties such as the UK Independence Party (UKIP); the *Front National* in France; *Alternative für Deutschland* (AfD) in Germany; and numerous others have received succour and support from the Kremlin in recent years (Klapsis, 2015).

This analysis has not sought to deny that organised disinformation is taking place, or that it is not becoming more sophisticated and potentially impactful as capabilities and technologies progress. It is clearly the case that troll factories such as the IRA have been very active in spreading disruptive and inflammatory social media in recent years, not only around the times of key elections and referenda in the West, but in relation to other phenomena such as terrorist attacks and societal responses to them. Indeed, reference was made in the Defence Committee's 2019 inquiry to overt disinformation on Russian state television about the true motives of the Skrijpal poisoners, alleged in the West to be GRU agents (Defence Committee, 2019b).

The ISC suggested on the publication of its Russia report that the UK government had been woefully negligent in its approach to the question of organised Russian disinformation. A Scottish National Party member of the ISC, Stewart Hosie, said:

> The UK Government have actively avoided looking for evidence that Russia interfered [in elections]. We were told that they hadn't seen any evidence, but that is meaningless if they hadn't looked for it (Sabbah, Harding and Roth, 2020).

The problem of attribution of such hostile activity to specific Russian state direction (other than where it is very overt) is well-known. This issue aside, research reveals that there is much uncertainty about the actual impact of organised disinfor-

mation strategies on social media, with many studies suggesting that the volume of such "bad information" is relatively low compared to the general flows of information, and that the impact it has on electorates in terms of materially changing their views and voting intentions is perhaps very small indeed. This does not, of course, mean that further research is not needed. This will be especially important over time as the social media sector and its impact on society evolve in new directions.

It also appears to be the case that the specific effect of organised disinformation is not necessarily to directly change the outcome of specific elections, but to create a general fog of uncertainty and division in Western societies which can, in the longer term, have a strategic effect on politics and its evolution. Such developments also cause a generally destabilising effect in Western polities, whereby more extreme political expressions start to challenge normative, mainstream views. These are issues not to be taken lightly.

In terms of the UK government's narrative in response, the three themes drawn out (defending democracy; an arm's length approach; and welcoming tech business) are, of course, not the only themes that could be identified in the documents under scrutiny, not least as they deal with a range of issues wider than the immediate question of Russian disinformation and interference. However, the themes do shed light on the complex balancing acts and political considerations in a modern liberal democracy when confronted with the problem of organised disinformation. For the UK, there may also be a particularly context-specific factor about the state's post-Brexit future and its relationship with other European competitors such as France and Germany. On these issues also, further contextual case-study research will be needed.

References

Ball, J. (2019, February 18). The DCMS report is good and sensible and everyone will ignore it. *New Statesman*. Retrieved August 20, 2020, from https://www.newstatesman.com/politics/media/2019/02/dcms-report-fake-news-good-and-sensible-and-everyone-will-ignore-it

Bakshy, E., Messing, S. and Adamic, L.A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science, 348*(6239), 1130-1132

Bastos, M.T. and Mercea, D. (2017). The Brexit botnet and user-generated hyperpartisan news. *Social Science Computer Review, 37* , 38-54

BBC (2018, July 26). *Vote Leave's targeted Brexit ads released by Facebook*. Retrieved August 20, 2020, from https://www.bbc.co.uk/news/uk-politics-44966969

BBC (2019, November 4). *Powerful 'Putin's chef' Prigozhin cooks up murky deals*. Retrieved August 19, 2020, from https://www.bbc.co.uk/news/world-europe-50264747

Beck, U. (2006). Living in the world risk society. *Economy and Society, 35*(3), 329-345

BNP (2011). *Russian elections 'much fairer than Britain's'.* Cited in cited in Klapsis, 2015.

Booth, R., Weaver, M., Hern, A., Smith, S. and Walker, S. (2017). Russia used hundreds of fake accounts to tweet about Brexit, data shows. *The Guardian*. Retrieved August 19, 2020, from https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets

Cadwalladr, C. (2018, June 16). Arron Banks, Brexit and the Russia connection. *The Guardian*. Retrieved August 20, 2020, from https://www.theguardian.com/uk-news/2018/jun/16/arron-banks-nigel-farage-leave-brexit-russia-connection

Carroll, O. (2019, July 2). Britain First: Far-right British group invited to speak at Russian parliament. *The Independent*. Retrieved July 18, 2020, from https://www.independent.co.uk/news/world/europe/britain-first-russia-paul-golding-duma-parliament-far-right-a8984521.html

Cavelty, M.D., Kaufmann, M. and Kristensen, K.S. (2015) Resilience and (in) security: Practices, subjects, temporalities. *Security Dialogue, 46*(1), 3-14

Coaffee, J., Wood, D.M. and Rogers, P. (2009). *The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster*. Basingstoke, Palgrave Macmillan

Daily Mail (2012, January 27). Mailonline: the world's number one: We're the biggest newspaper website with 45.348 million unique users. Retrieved August 10, 2020 from https://www.dailymail.co.uk/news/article-2092432/MailOnline-worlds-number-Daily-Mail-biggest-newspaper-website-45-348-million-unique-users.html

Dawson, A. and Innes, M. (2019). How Russia's internet Research Agency built its Disinformation Campaign. *The Political Quarterly*, 1-12

DCMS (2019a). *Disinformation and "fake news": Final Report. Eighth Report of Session 2017-19*. London, House of Commons, HC 1791. Retrieved August 15, 2020, from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm

DCMS (2019b). *Disinformation and "fake news": Final Report: Government's Response to the Committee's Eighth Report of Session 2017-19*. London, House of Commons, HC 2184. Retrieved August 15, 2020, from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2184/2184.pdf

DCMS and Home Office (2020). *Online Harms White Paper – Initial Consultation Response. Updated 12 February 2020*. Retrieved August 15, 2020, from https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

Defence Committee (2019a). UK Response to Hybrid Threats Inquiry. Oral evidence, 30 April, 2019, HC 1816. Retrieved December 12, 2020, from https://old.parliament.uk/business/committees/committees-a-z/commons-select/defence-committee/inquiries/parliament-2017/uk-response-hybrid-threats-17-19/publications/

Defence Committee (2019b). UK Response to Hybrid Threats Inquiry. Oral evidence, 2 July, 2019, HC 1816. Retrieved December 12, 2020, from https://old.parliament.uk/business/committees/committees-a-z/commons-select/defence-committee/inquiries/parliament-2017/uk-response-hybrid-threats-17-19/publications/

Electoral Commission (2020). *Joint announcement by The Electoral Commission, Mr Robert Posner, Mr Arron Banks and Ms Elizabeth Bilney*. Retrieved August 15, 2020 from https://www.electoralcommission.org.uk/media-centre/joint-announcement-electoral-commission-mr-robert-posner-mr-arron-banks-and-ms-elizabeth-bilney

Flaxman, S., Goel, S. and Rao, J.S. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, 80, 298-320

Free Russia Forum (2020, April 3). *British far-right activist "Tommy Robinson" in Moscow*. Retrieved August 20, 2020, from https://www.forumfreerussia.org/en/news-en/2020-04-03/british-far-right-activist-tommy-robinson-in-moscow/ffr/

Gill, P. (2006). Not Just Joining the Dots but Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing and Society, 16*(1), 27-49

Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B. and Lazer, D. (2019). Fake news on Twitter during the 2016 U.S. presidential election. *Science,* 363, 374-378

Guess, A., Nagler, J. and Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances, 5*(1), 1-8

Hansen, I. and Lim, D.J. (2019). Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics, 25*(2), 150-171

HMG (2020). *Government Response to the Intelligence and Security Committee of Parliament Report "Russia"*. London, CP 275. Retrieved August 15, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf

House of Commons (2018). *Democracy under threat: risks and solutions in the era of disinformation and data monopoly* . 42nd Parliament, 1st session, December 2018. Ottawa. Retrieved August 15, 2020, from https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf

Innes, M. (2017). *Russian influence and interference measures following the 2017 UK terrorist attacks*. Cardiff University Crime and Security Research Institute/ CREST

ISC (2020a). *Russia*. London, HC 632. Retrieved August 12, 2020 from https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl

ISC (2020b). *Press notice: Intelligence and Security Committee publish predecessor's Russia report*. Retrieved August 15, 2020 from https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDoxMmRkZmU2MjQ4ZWEzNDI0

Klapsis, A. (2015). *An Unholy Alliance: The European Far Right and Putin's Russia*. Brussels, Wilfied Martens Centre for European Studies

Llewellyn, C., Cram, L., Hill, R.L. and Favero, A. (2019). For Whom the Bell Trolls: Shifting Troll Behaviour in the Twitter Brexit Debate. *Journal of Common Market Studies, 57*(5), 1148-1164

Maness, R.C. (2018). *Death by a thousand cuts: is Russia winning the information war with the West?* Paper presented at the 2018 International Studies Association Meeting. Retrieved August 10, 2020, from https://www.researchgate.net/publication/326926354_Death_by_a_Thousand_Cuts_Is_Russia_Winning_the_Information_War_with_the_West

Mason, R. (2017, November 14). Theresa May accuses Russia of interfering in elections and fake news. *The Guardian*. Retrieved August 10, 2020, from https://

www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news

Matthews, O. (2020, July 25). Unleash chaos: How Putin plans to make the West destroy itself. *The Spectator,* pp.10-11

Nimmo, B. (2017, December 13). #Election Watch : Scottish Vote, Pro-Kremlin Trolls. *DFRLab*. Retrieved August 15, 2020, from https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb

Ohlin, J.D. (2018). *Election Interference: The Real Harm and the Only Solution*. Cornell Law School, Legal Studies Research Paper no. 18-50

Paul, C. and Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation, Perspective, PE-198-OSD [2016]

Power. M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London, Demos

Richards, J. (2012). *A Guide to National Security: Threats, Responses and Strategies*. Abingdon, Oxford University Press

Richards, J. (2019). *Intelligence gathering, issues of accountability and Snowden*. In Hale-Ross, S. and Lowe, D. (Eds.) Terrorism and State Surveillance of Communications (pp.19-37). London, Routledge

RT News (2017, December 21). T*heresa May accuses Russia of 'weaponizing information' during visit to Poland*. Retrieved August 10, 2020, from https://www.rt.com/uk/413890-may-russia-poland-defence/

Sabbah, D., Harding, L. and Roth, A. (2020, July 21). Russia report reveals UK government failed to investigate Kremlin interference. *The Guardian*. Retrieved August 17, 2020, from https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit

Schultz, R.H. and Godson, R. (1984). *Dezinformatsia: Active Measures in Soviet Strategy*. Washington D.C., Pergamon-Brassey's

Sonne, P. (2018, December 27). A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening. *The Washington Post*. Retrieved August 12, 2020 from https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html

Stelzenmüller, C. (2017). *The Impact of Russian Interference on Germany's 2017 Elections*. Testimony delivered to the U.S. Senate Committee on Intelligence, June 28, 2017. Retrieved August 10, 2020 from https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

Wintour, P. and Mason, R. (2014, March 31). Nigel Farage's relationship with Russian media comes under scrutiny. *The Guardian*. Retrieved August 10, 2020 from https://www.theguardian.com/politics/2014/mar/31/nigel-farage-relationship-russian-media-scrutiny

Notes

[1] All documents related to the DCMS investigation can be seen at https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/

[2] For details of the Defending Democracy programme, see https://hansard.parliament.uk/commons/2019-07-22/debates/19072238000019/DefendingDemocracyProgramme

[3] See https://www.gov.uk/government/news/hostile-state-activity-assessment-body-announced