Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Hacking democracy: managing influence campaigns and disinformation in the digital age

Niels Nagelhus Schia & Lars Gjesvik

To cite this article: Niels Nagelhus Schia & Lars Gjesvik (2020): Hacking democracy: managing influence campaigns and disinformation in the digital age, Journal of Cyber Policy, DOI: 10.1080/23738871.2020.1820060

To link to this article: https://doi.org/10.1080/23738871.2020.1820060

Published online: 06 Oct 2020.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2020.1820060

Routledge
Taylor & Francis Group

Hacking democracy: managing influence campaigns and disinformation in the digital age

Niels Nagelhus Schia and Lars Gjesvik

NUPI (Norwegian Institute of International Affairs)

ABSTRACT

How are states responding to the threat of using digital technologies to subvert democratic processes? Protecting political and democratic processes from interference via digital technologies is a new and complicated security threat. In recent years the issue has been most prominent in terms of election security, yet the widespread usage of digital technologies allows for the subversion of democratic processes in multifaceted ways. From disrupting the political discourse with false information to inflaming and stoking political divisions digital technologies allows for a variety of ways for malicious actors to target democracies. This article compares different state experiences with interference in sovereign and contested political decisions. More specifically the article compares the Norwegian approach and experience in managing these challenges with those of Finland and the UK. Mapping both how the problem is understood, and the role of previous experiences in shaping public policy.

ARTICLE HISTORY
Received 11 February 2020
Revised 26 June 2020
Accepted 29 July 2020

KEYWORDS
Disinformation campaigns; Democratic elections; Technology companies

This paper investigates how states are responding to the threat of digital technologies being used to undermine democratic processes. While propaganda and the influencing of political decisions are nothing new, the ever-increasing use of digital technologies has made the issue of disinformation and the subverting of political discourse a pressing topic (Grigsby 2017). Following the 2016 US presidential elections and the subsequent investigation into suspected Russian interference, the subject has become a matter of critical importance on policy agendas globally. Research has tried to measure whether Russian attempts were effective, in doing so asking whether the spreading of disinformation by foreign states can potentially determine the outcome of democratic elections (Benkler, Faris, and Roberts 2018; Jamieson 2018). Since then, disinformation has become a notable feature of several high-profile political events, including the 2017 French presidential elections (Bulckaert 2018) and the 2019 elections to the European Parliament (Bendiek and Schulze 2019). Furthermore, the existence of false and falsified information has become a societal issue beyond the narrow topic of elections. A full 15% of Twitter users in 2017 were estimated to be bots (Prier 2017), while the use of internet

CONTACT Niels Nagelhus Schia nns@nupi.no

technologies to propagate false claims and narratives has been linked to such issues as climate change scepticism/denial (Leiserowitz et al. 2013) and radicalisation (Sablina 2019), and been used as a political tool for altering narratives around incidents as diverse as the Salisbury poisoning (EU vs Disinfo 2019) and the Hong Kong protests (Facebook 2019). The 'normality' of disinformation has been accepted to such an extent that a UK parliamentary committee described it as an expected part of modern political life (Digital, Culture, Media and Sport Committee 2019).

False and misleading information, and its ability to spread rapidly online, has been described as a societal vulnerability and a threat to democracy. While some uncertainties remain, especially as to the extent to which disinformation is effective (Benkler, Faris, and Roberts 2018), the possible consequences are indeed grave. States grappling with this challenge are currently implementing policies that aim to prevent disinformation from propagating too widely in their societies. In this paper, we compare the extent to which Finland, the UK and Norway envision the role of 'ordinary citizens' in building and maintaining resilience against disinformation and influence campaigns. The paper builds on desktop studies, complemented by semi-structured interviews with 21 policymakers, stakeholders and independent experts from Finland, the UK and Norway, in order to map existing and planned policies. We begin by offering some background on, and definitions of, the issue of disinformation. We then proceed to map out the approaches of the three states, examining their shared features and/or diverging practices, and the extent to which policies mainly target individual citizens.[1]

Background, definitions, literature

Disinformation has been described as 'the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain' (Digital, Culture, Media and Sport Committee 2019). In international politics, it is increasingly used as a tool for altering perceptions on a particular issue or subverting the political discourse by inserting false information (Digital Forensic Research Lab 2018).

The growing use of disinformation in international politics as a consequence of digital technologies has been extensively chronicled elsewhere (Badawy, Ferrara, and Lerman 2018; Bartles 2016; Bradshaw and Howard 2018a; Connell and Vogler 2017; Darczewska 2014; Franke 2015; Howard and Bradshaw 2019; Jamieson 2018; Kragh and Åsberg 2017; Moore 2018; Morgan 2018; Pope 2018; Splidsboel Hansen and Jensen 2016; Stukal et al. 2017; Ziegler 2018). While there can be no doubt that disinformation exists, its effect on political discourse is a far more controversial topic. Several researchers have criticised the idea that state-backed disinformation can effectively alter perceptions (Benkler, Faris, and Roberts 2018; Guess et al. 2019). Instead, they hold that the core of the issue lies within national politics (Benkler, Faris, and Roberts 2018) or in traditional media (Marwick and Lewis 2017; Steensen 2019); or they argue that attempts by other states to spread disinformation are limited, and far less worrisome than comparable efforts by domestic actors (Bastos and Mercea 2019; Nyhan 2019).

Rather than focus primarily on the ability of hostile states to shape domestic political opinion, a related literature has instead highlighted the broader negative societal effects of large, advertisement-driven internet platforms and online communication (Herpig,

Schuetze, and Jones 2018; Kumar, West, and Leskovec 2016). These authors point to the growing (mis)use of social media, enabled by the business model of large tech platforms, as well as shifts in the business models of traditional media (Allcott and Gentzkow 2017; Allcott, Gentzkow, and Yu 2019; Bastos and Mercea 2019; Crain and Nadler 2019; Eady et al. 2019; Kim 2018a, 2018b; Kim et al. 2018; Marwick and Lewis 2017; Robinson 2018; Sablina 2019; Woolley 2016). While these platforms may have had some success in limiting the spread of disinformation (Allcott, Gentzkow, and Yu 2019), the long-term effects of their broader business models remain to be seen. The main challenges here have less to do with immediate attempts at swaying public opinion, and more to do with the splintering of a shared public discourse, leading to new forms of political organisation with uncertain consequences, irrespective of whether the source of polarisation is foreign or domestic (Eady et al. 2019; Farrell and Schneier 2018; Lin 2019; Patel 2019). In turn, the policy problem is not so much the spread of false information or propaganda by state actors, but the changing dynamics of communication and the growing power and influence of global digital platforms (Gillespie 2015; Gorwa 2019b; Just and Latzer 2017; Kenney, Bearson, and Zysman 2019; Mozur and Scott 2016; Tufekci 2018; Zuboff 2015, 2019).

Various features of the shift towards digital communications shape how information is shared and spread. An obvious starting point is the way in which the internet makes distance irrelevant, putting actors all over the world in touch with one another. Related to this, new forms of media (which might not always adhere to established standards of journalism) are reaching larger audiences (Kalsnes 2019). This allows for more direct forms of communication, which can bypass the media's traditional 'gatekeeping' role and thus be exploited to push false news stories. A further key feature of the internet is the anonymity it offers to those wishing to conceal their true identity. A defining element of online communication has become the presence of 'trolls' – actors debating with malicious intent. The anonymity of the internet has been linked to polarisation and the expression of more extreme opinions, but there has been little research as to the causal relationship (Benkler, Faris, and Roberts 2018). Regardless, anonymity enables users to mask who they really are, which may in turn lend undeserved credibility to hostile actors.

Though these challenges are common to all communications on the internet, several key features specific to social media have enabled the rapid spread of disinformation. One of these is the automated selection of content with which users interact. This is particularly so for social media platforms employing algorithms that promote content with high user interaction, as polarising content is designed to increase the likelihood of user engagement (Bradshaw and Howard 2018b). The classic example is the ability of automated accounts – 'bots' – to re-tweet or 'like' tweets in order to push fringe content into the mainstream (Gorwa and Guilbeault 2018). Creating falsified interest in fringe opinions may contribute to such opinions entering mainstream discourse or gaining legitimacy among a broader public (Bradshaw and Howard 2018a; Howard and Bradshaw 2019). A classic instance was the Russian meddling in the US 2016 presidential election, where automated accounts promoted both white supremacist and Black Lives Matter content, sharpening polarisation on both sides of the debate (Bradshaw et al. 2019).

Beyond pushing fringe opinions into the mainstream, the massive amounts of data these digital platforms possess enable more specialised and individualised content: 'microtargeting'. Unlike traditional media, where communications to one group of citizens

inevitably reach other groups as well, thereby helping to hold politicians to account, communications on social media can be targeted at the level of the individual. Thus, politicians or other actors can promise two opposing solutions to different groups of voters, without confrontation (Heawood 2018). The most-cited example of this kind of practice is the real-time bidding feature of Facebook's advertising system, whereby potential advertisers can target a defined subset of users for any ad they want to promote on the platform. As users scroll through Facebook, they are shown ads that match their subset of users – with no information as to what *other* users are seeing (Olejnik 2016; Olejnik and Castelluccia 2016).

While efforts have been made to curtail the misuse of microtargeting and real-time bidding in election campaigns, they have so far enjoyed only modest success. In 2019, Facebook introduced the Ad Library and asked all political parties to mark their advertisements so they could be stored and accessed (Facebook 2020). This, however, has not been without problems – in the 2019 Norwegian municipal elections, for example, parties inadequately marked their advertisements as 'political', thereby undermining the usefulness of the tool (Johansen and Hager-Thoresen 2019). Furthermore, the clampdown on political ads has had unintended side-effects. Several respondents to our study referred to the 2019 European parliamentary elections, where Facebook implemented a policy banning those outside the target country from purchasing political advertisements. Though implemented with good intentions, the policy ultimately prevented EU politicians in Brussels from campaigning in their respective countries, as they were flagged as 'foreign' actors.

This points towards the larger societal complications caused by the structural change in political communication. Big data analytics and algorithmic governance have increasingly become a new form of governance in societies (Gorwa 2019a, 2019b), opening up new spaces of knowledge and control that did not previously exist, the implications of which are only now becoming evident (Amoore and Piotukh 2015). While bots, trolls and political advertisements may be short-term problems solvable by digital platforms in cooperation with governments globally, a far more fundamental challenge is the changing power dynamics between the two (Helberger, Pierson, and Poell 2018). Who has the power to determine the limitations of political discourse? What information is presented to individuals? What are the limits of free speech? Such decisions are increasingly being made by global corporations rather than societies (Gillespie 2015). Moreover, an absence of transparency and lack of access to the data provided by the digital platforms constrains researchers seeking to study the implications of this shift (Walker, Mercea, and Bastos 2019).

This paper builds on interviews conducted between July 2019 and June 2020. The data from these interviews were combined with a cross-checking of data and narratives with a wide range of informants. Our enquieries were inspired by anthropology and what has been called 'polymorphous engagement' (Gusterson 1997, 116). This involves a combination of methods such as formal interviews, document study and observation. Most of our interviews and focus groups were conducted face-to-face in Oslo, London and Helsinki, but we have also conducted interviews on Skype and Microsoft Teams. Our interviewees were selected through a network method. We already had knowledge of stakeholders through previous projects and work; when contacting and interviewing these we always asked for recommendations for other stakeholders to contact. We also

made sure to talk with key ministries in the three countries, as well as major digital platforms and their activities in the three countries, such as Facebook. The case countries were chosen because they are all very digitalised countries with very similar political situations, although with key differences. UK is one of the world's great powers and thus presumably more vulnerable to such attacks, Finland is closer to Russia and is an interesting case in this context. Norway was a logical departure for this investigation, since both authors are working in this country, but it is also interesting as a case-country because it had a political election during our investigations.

While significant questions remain about the future role of disinformation, the trend towards weaponizing information for political gain continues to give grounds for concern. Effective policies are therefore increasingly important for domestic and national security purposes. To this we now turn.

Country approaches: Finland, the UK, Norway

Liberal democratic states may find dealing with disinformation particularly challenging, with societal values such as freedom of speech and the security of democratic processes framed as conflicting, but not necessarily mutually exclusive (Farrell and Schneier 2018). As argued above, the change in communication technologies since the turn of the millennium has altered the form and nature of political discourse and debates. With the negative side-effects of this development becoming increasingly evident, states have set about implementing measures to combat disinformation in their societies.

Finland

Of the three countries examined here, Finland had the most long-term dedicated approach to disinformation, dating back to 2014 and the Russian annexation of Crimea. The issue of disinformation is not understood narrowly as 'foreign' influence, but encompasses such issues as extremism, trolling and online harassment. While Finland has received praise for tackling disinformation campaigns that have targeted the country (Mackintosh 2019), it would be premature to conclude that it is more exposed to disinformation than similar countries. The steps Finland has taken should also be seen in the context of its historical and geopolitical relationship with Russia. However, existing strategies and reports, policy documents, and our interviews, do indicate that the Finnish authorities regard the issue of disinformation – especially disinformation of Russian origin – as more pressing than their counterparts in Norway, and possibly the UK (Ahonen 2018; Riiheläinen 2018).

Finland's main protection against disinformation has been identified as its high levels of media literacy and trust in government, along with the general resilience of the population. Greater emphasis has been placed on preserving these features of Finnish society, anchored in the concept of comprehensive security, than on creating new policies. Efforts have been mainly domestic and have included long-term strategies as well as more immediate remedies. The focal point of policies has been building resilience to disinformation through raising awareness among the general public and the media, improving collaboration in the public sector, and encouraging critical thinking and reflection through the educational system. Regarding improved collaboration, our respondents

mentioned the establishment of the 'influence network' – consisting of various ministries and coordinated by the office of the prime minister – as important for detecting and responding efficiently to incidents. This system promotes better information sharing between various public bodies, between security services and other parts of the government, and between the government and the general population.

Attention given to the issue of disinformation peaked in connection with the 2019 elections, with the security of the electoral process placed under scrutiny and the mitigation of potential risks attempted (Justitieministeriet 2019). As the Finnish electoral system is largely manual, with paper ballots, manual counting, and long-term storage of votes after an election, the digital risks posed by a general election itself are considered low. Even so, communicating the security and resilience of the electoral system was stressed as vital to combat misperceptions, with one example targeting the broader population being the launch of a government initiative in the run-up to the 2019 elections that utilised various celebrities and public figures (Government Communications Department 2019). Unlike the UK and Norway, Finland did not have a fact-checker approved by IFCN, the global fact-checking network, though this was not seen as a significant issue by respondents (IFCN 2020).

The importance of social media platforms is substantial and growing in Finland. The government has adopted a collaborative approach with the major tech companies regarding possible attempts to influence the political discourse (Justitieministeriet 2019). However, multiple respondents complained about the inadequacy of this approach. Attempts at reaching out and taking initiative from the government side had been met with indifference or no response from at least one social media platform. It could be argued, and some respondents made the case, that the power imbalance between a global corporation and a small country like Finland is manifesting itself in a lack of attention to Finnish problems and perspectives. As a result of the disappointments in collaboration, our respondents explained that Finland has chosen to pursue regulation of digital platforms within the EU. This is because EU-wide regulations – backed by the union's market power and regulatory clout – are regarded as being far more likely to succeed than regulations at the level of individual states.

The UK

As in Finland, efforts undertaken in the UK have not involved any radical realignment of policy. Rather, authorities have been striving to establish more coherent and collaborative approaches across government sectors, alongside raising awareness within government and the general populace. Our respondents described the 2018 Skripal poisoning case and the false narratives spread in its wake as a learning experience highlighting the necessity of proactive and consistent communication. Government entities have chosen a two-pronged approach: firstly, to communicate potentially divisive issues before misperceptions take hold, and secondly, to have contingency plans in place for unforeseen incidents.

As a result, different agencies, offices and departments are taking the lead on different initiatives, including The National Cyber Security Centre (NCSC) which, in addition to its broader role in fostering cyber security, has mainly advised candidates and parties on cybersecurity, performed audits and held exercises (National Cyber Security Centre

2019). The Cabinet Office has established a Rapid Response Unit (RRU) which takes the lead in actively responding to false narratives and issuing corrections (Feikert-Ahalt 2019). By quickly establishing and promoting a counter-narrative, the goal is to target evolving conversations and get verified facts and narratives to be visible in these conversations, if needed, paying for Facebook ads to ensure that the relevant people are reached.[2] This has been the case recently for Covid 19 misinformation.[3] The Foreign & Commonwealth Office (FCO) has been involved in initiatives to tackle disinformation abroad and the Department for Digital, Culture, Media and Sports (DCMS), in response to Coronavirus, has established another Rapid Response Unit coordinating the tasks of different UK agencies. In addition, the department, as the responsible government body for regulating tech companies, has played a part in the evolving discussions on regulating platforms resulting in the report published by the DCMS committee.[4]

Finally, another major area of focus has been on raising awareness among the broader citizenry, along with such initiatives as the SHARE checklist, aimed at improving the public's ability to reflect critically on online news (HM Government 2019b). Similarly, efforts to incorporate critical thinking into education are linked to the spread of disinformation and false news articles (Cockburn 2019). This is not an exhaustive list of all government initiatives and efforts of relevance to digital democracies, but it covers the most significant in addition to outlining the range of stakeholders involved and deemed relevant.

Of the countries examined here, the UK has gone the furthest in criticising the role of digital platforms. A 2019 report by the House of Commons' Digital, Culture, Media and Sports Committee entitled *Disinformation and 'Fake News'* was highly critical of the role played by social media platforms, and outlined a list of recommendations – these, however, have not yet been implemented (Digital, Culture, Media and Sport Committee 2019). Related to this report, both the *Online Harms White Paper* (HM Government 2019a) and the *Cairncross Review of a Sustainable Future for Journalism* (Cairncross 2019) have examined the issue of disinformation and digital communications more broadly (Goodman 2019). As yet, these reviews and reports have not resulted in any new policies, but our respondents argued that this was largely because the prolonged Brexit process had delayed their development.

Norway

In Norway, the political discourse appears to have been less influenced by foreign disinformation than the other two cases, with no prominent instances of foreign influence mentioned in our interviews or otherwise identified (Kalsnes 2019). During the 2019 municipal elections, the Norwegian independent research institute of Applied Research, Technology and Innovation (SINTEF) investigated the possibilities of foreign influence, but no clear evidence was found that this was the case (Grøtan et al. 2019). Publicly available datasets on known disinformation campaigns, such as those published by Twitter in 2018, have only a marginal focus on Norwegian political issues, which strengthens the hypothesis that Norway has thus far not been exposed to the same extent as other countries (Twitter 2018). There may be several reasons for this, one being that the 2019 elections were local rather than national, and so perhaps of little interest to such campaigns. Another reason, mentioned by respondents, may be the election system itself.

The Norwegian multi-party system is such that it is rare for a single party to be given the opportunity to govern alone. This means that, most of the time, parties must work together to form coalition governments or minority cabinets, potentially making the country's election system more resilient to disinformation campaigns aimed at polarisation. A third reason may be the fact that Norway, a small country not involved in any geopolitical conflicts in recent years, does not elicit the same level of interest as larger countries involved in greater power politics.

Norwegian efforts to combat potential attempts to influence the political discourse focused on the September 2019 local (municipal and county council) elections. That summer, the Norwegian government engaged a broad range of ministries and stakeholders to initiate a 10-point plan to secure the elections. Headed by the Ministry of Local Government and Modernisation and the Ministry of Justice and Public Security, the working group took the lead in safeguarding democratic processes in the digital age. The 10-point plan focused on, firstly, improving election security, and, secondly, boosting resilience through fostering critical thinking and awareness (Kommunal og moderniseringsdepartementet 2019). Beyond election-targeting efforts, there has been a focus on building resilience, as in the UK and Finland. The working group has continued to meet regularly, establishing – as our respondents noted – an informal network of public bodies working on securing elections. This new approach has also entailed increased efforts at improving critical thinking (Utdanningsdirektoratet 2019).

Regulating social media platforms and large tech companies was not a topic mentioned by any government respondents, but was one that was frequently brought up by outside experts. In addition, attempts at fostering such debates by, for example, the Norwegian Board of Technology (NBT) were met with puzzlement by some social media platforms representatives as discussed proposals had already been implemented at an EU-level and were soon to be rolled out in Norway as well. While the issue of disinformation continues to get attention in the Norwegian context, there appears to have been limited movement in developing new policies and regulation.

Comparison and discussion

The UK, Finland and Norway emerge as broadly similar in their understanding of the issue of disinformation, as well as the efforts they have undertaken to combat it. Public statements and assessments by intelligence agencies in all three countries show that Russia is regarded as the state most actively engaged in disinformation (Karlsen 2019). However, all three countries view disinformation as a broader societal issue and have not concentrated solely on the actions of any given state. Interestingly, Norwegian and UK respondents highlighted the 2016 US election as the starting point for more focused efforts at disinformation, whereas Finnish respondents referred to Russia's 2014 annexation of Crimea and the use of disinformation during the occupation. Even so, this is unlikely to indicate radically differing understandings of the dangers posed by disinformation and its sources.

In all three countries, most respondents agreed that disinformation was as much a domestic issue as a national security one. Moreover, disinformation emanating from domestic actors is considered more effective – and thereby more challenging to combat – than foreign disinformation, primarily due to the difficulties faced by foreign actors in bridging cultural and linguistic divides. This was especially evident in the two Nordic countries, but

respondents in all three countries argued that, while physical distance has become less relevant in the digital age, cultural distance continues to affect the impacts of foreign disinformation.

Another feature common to all three countries is a concern that elections are particularly vulnerable, with efforts at securing elections focused on both their security and in bolstering public trust in the democratic process. Securing the election process entails detecting and responding to false information, improving the security of the election process' digital aspects, and providing information and advice to relevant actors, such as political parties. Bolstering trust – an issue highlighted by Finnish respondents in particular – relies on communicating the trustworthiness and security of the election process in order to avoid misunderstandings. In this regard, the denial-of-service attack on Sweden's election authority website during the country's 2018 elections was mentioned as an example of the dangers of inadequately communicating an election process' security (Olsson and Wollner 2019).

As to policies and tools aimed at combating disinformation beyond elections, these fall into two broad types of resilience measures: firstly, fostering critical thinking, and secondly – a point mentioned by respondents in all three countries – improving awareness and the capacity to detect and respond to incidents. A key factor highlighted by respondents was improving cooperation and collaboration within government, namely: raising awareness about the problem of disinformation, setting guidelines for effectively communicating facts and counter-narratives, and establishing networks of stakeholders working on relevant issues. These networks, while largely similar, also have a regional tinge – respondents in Finland and Norway more frequently mentioned collaboration with traditional media outlets than did respondents in the UK. In all three cases, the vital importance of exercises, real-life experiences and continued cooperation was emphasised.

Fostering critical thinking is a third major focus in all three countries, through national campaigns aimed at raising awareness and building trust, and through educational systems. The need for members of the public to develop their ability to identify false claims and make informed choices is a concern that spans multiple fields and applies far more broadly than simply the issue of disinformation (Aronson et al. 2019). Most respondents agreed that fostering critical thinking was a long-term project – though some immediate gains can be made, it cannot be expected to serve as a standalone solution in the short term. Such approaches are also seen as involving third parties, such as fact-checkers used to counter false claims and disinformation, but this represents only a minor part of the picture.

Beyond these resilience measures, respondents in all three countries mentioned challenges in dealing with new digital technologies, and the limitations faced by individual states in governing them. While all respondents agreed that digital platforms should play a role in minimising disinformation, the ability of individual states to regulate or incentivise this was contested. In the case of the UK, respondents and several reports have argued for platform regulation, as noted above. Our Finnish respondents explained that most of their country's efforts were being conducted within the EU framework, which is perceived as increasing the chances of successful regulation. With our Norwegian respondents, on the other hand, independent experts – though not government representatives – linked disinformation to the growth of digital platforms. Regardless, while the reasons given differed, all three countries have few policies specifically aimed at addressing the structural issues, potentially enabling the spread of disinformation.

The fact that Norway was not prioritised for Microsoft's AccountGuard – a new security service offered to customers in the political space[5] – may indicate that the Norwegian local elections were not interpreted as being particularly vulnerable to digital threats and disinformation campaigns. This is in contrast to the EU parliamentary election, which apparently was prioritised. Microsoft's AccountGuard is designed to help highly-targeted customers protect themselves from cybersecurity threats,[6] and is part of the company's defending democracy programme aimed at election integrity, campaign security, advertising transparency and disinformation. It is active in 44 countries, including the UK and Finland, but not yet in Norway. This broadly mirrors other trends when it comes to the relationships between governments (in particular smaller ones) and large tech firms: while the initiatives taken by these tech firms should largely be seen in a positive light, they are very much designed and rolled out according to the preferences of the firms themselves. Most of the respondents that did address the issue of self-regulation and corporate initiatives saw the tech platforms' approach as insufficient and remarked on their unwillingness to address criticisms by, for instance, fact-checkers in a constructive manner. It was noted that the blame for this situation should not be placed solely on the tech companies, as they were asked to self-regulate on challenging political issues, but all respondents agreed they were failing in doing so. While some government respondents were willing to acknowledge these issues, none offered any indications that substantive regulation or shifts in strategy were forthcoming, but they may nevertheless be under development.

The ability of fact-checkers, traditional media and public bodies to respond to disinformation is backed by a growing research literature. Here, there has been some success, and this has also been the case in terms of fostering critical thinking (Kalsnes 2019). Still, important questions remain as to whether this approach is sufficient. Leaving aside the question of whether training in critical thinking is feasible at scale, it clearly places the burden of dealing with new forms of communication and knowledge-sharing on members of the public, while expanding whole-of-society approaches to include national security. Relying solely on such policies fails to deal with larger structural issues, such as who controls what information, how such information is made available, and to whom. This, according to our respondents, was due more to a lack of will and/or ability on the part of national governments, than ignorance. If a country is unwilling, or unable, to deal with the ever-growing power and influence of digital platforms, then the tools at its disposal are likely to remain limited. That all three states studied here focused on individual citizens, public bodies and elections should be understood as being largely the result of these limitations. Thus, similarities in policy may be evidence of the three countries facing similar issues in governing large global platforms, rather than indicating best practice.

Conclusions

Disinformation is a difficult and challenging issue. While propaganda and various forms of influence have always been present in politics, recent technological developments risk undermining established equilibriums for dealing with false or misleading information. In addition, the lack of transparency characteristic of today's large digital platforms has made measuring the societal impact of disinformation accurately almost impossible.

Comparing the approaches taken by Finland, the UK and Norway, we find broad similarities in terms of policies and initiatives centred mainly on resilience and collaboration. Furthermore, most efforts are domestic in nature, targeting either public authorities or individual citizens. Though these are indeed important steps, such approaches put the onus on members of the public to navigate the broad structural changes taking place in patterns of communication, leaving the disproportionate influence of large digital platforms largely unaddressed. The erosion of autonomy that such a dynamic entails, with large parts of the regulation of public discourse left to private global corporations, appears both unsustainable, and possibly dangerous, in the long term.

Notes

1. While EU regulations are relevant for Finland, they were not included in the scope of this research project and so are not specifically examined here.
2. See: https://gcs.civilservice.gov.uk/podcasts/fact-countering-misinformation-in-the-media/
3. See: https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online
4. See: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/
5. See: www.microsoftaccountguard.com/en-us/. During the COVID-19 crisis, AccountGuard to protect healthcare from cyberattacks was launched, see: https://blogs.microsoft.com/on-the-issues/2020/04/14/accountguard-cyberattacks-healthcare-covid-19/
6. See: https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/

Acknowledgements

Thanks to the editors and the anonymous reviewers for their helpful comments, as well as to the interviewees in the three countries. Financial support was provided by the Norwegian Research Council's IKTPLUSS Program under grant number 288744, 'Digital Vulnerability and National Autonomy' and by the Norwegian Ministry of Defence, 'Protecting Democracies from Digital Threats (PRODEM)'.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Financial support was provided by the Norwegian Research Council's IKTPLUSS Program under grant number 288744, 'Digital Vulnerability and National Autonomy' and by the Norwegian Ministry of Defence, 'Protecting Democracies from Digital Threats (PRODEM)'.

Notes on contributors

Niels Nagelhus Schia is a senior research fellow and manager for NUPI's Center for Cyber Security Studies. He is a former fellow of the NSSR (New School for Social Research) and holds a PhD degree in social anthropology from the University of Oslo.With a focus on the role of cybersecurity and cybersecurity governance in international relations Schia tracks new developments in policy and research, and provide academic studies, expert analysis and strategic policy recommendations. His research focus combines anthropology and international relations theory with theories of cyber

security. His current projects are concerned with norms and state behaviour in cyber space, development assistance and capacity building, societal vulnerabilities, sovereignty and cyberspace, global governance and cyberspace.

Lars Gjesvik is a PhD Candidate in the Research group for Security and Defence, working mainly on cybersecurity. He holds a master's degree in political science from the University of Oslo, and has studied international studies and history. His research interests are cybersecurity and cyber warfare.

Bibliography

Ahonen, Anneli. 2018. "'Finland Puts Russian Kids in Prison' – Disinformation that Shaped the Minds of Millions'. *EU vs Disinformation*. Accessed 24 August 2020. https://web.archive.org/web/20191216091254/https://euvsdisinfo.eu/finland-puts-russian-kids-in-prison-disinformation-that-shaped-the-minds-of-millions/.

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31 (2): 211–236. doi:10.1257/jep.31.2.211.

Allcott, Hunt, Matthew Gentzkow, and Chuan Yu. 2019. "Trends in the Diffusion of Misinformation on Social Media." *Research & Politics* 6 (2): 1–8. doi:10.1177/2053168019848554.

Amoore, Louise, and Volha Piotukh. 2015. "Life Beyond Big Data: Governing with Little Analytics." *Economy and Society* 44 (3): 341–366. doi:10.1080/03085147.2015.1043793.

Aronson, Jeffrey K., Eric Barends, Robert Boruch, Marnie Brennan, Iain Chalmers, Joe Chislett, Peter Cunliffe-Jones, et al. 2019. "Key Concepts For Making Informed Choices." *Nature*, August 12. Accessed 24 August 2020. www.nature.com/articles/d41586-019-02407-9.

Badawy, Adam, Emilio Ferrara, and Kristina Lerman. 2018. "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign." In *ASONMAN 2018. Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, edited by Ulrik Brandes, Chandan Reddy, and Andrea Tagarelli, 258–265. Barcelona: IEEE.

Bartles, Charles. 2016. "Getting Gerasimov Right." *Military Review* 96 (1): 30–38.

Bastos, Marco T., and Dan Mercea. 2019. "The Brexit Botnet and User-Generated Hyperpartisan News." *Social Science Computer Review* 37 (1): 38–54. doi:10.1177/0894439317734157.

Bendiek, Annegret, and Matthias Schulze. 2019. "*Disinformation and Elections to the European Parliamen*. SWP Comment." *Stiftung Wissenschaft und Politik*. doi:10.18449/2019C16.

Benkler, Yochai, Rob Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press.

Bradshaw, Samantha, and Philip N. Howard. 2018a. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71 (1.5): 23–32. www.jstor.org/stable/26508115.

Bradshaw, Samantha, and Philip N. Howard. 2018b. "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life." *Knight Foundation*, January 29. https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf?fbclid=IwAR33kKGH8EVEol-YNTmLTheN38Blfy1px04zKU7QlLgH0tHZPlhJFMtkduY.

Bradshaw, Samantha, Philip N. Howard, Bence Kollanyi, and Lisa-Maria Neudert. 2019. "Sourcing and Automation of Political News and Information Over Social Media in the United States, 2016–2018." *Political Communication* 15 (5): 1–21. doi:10.1080/10584609.2019.1663322.

Bulckaert, Ninon. 2018. "How France Successfully Countered Russian Interference During the Presidential Election." *Euractiv.fr*. June 17. Accessed 9 January 2020. www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/.

Cairncross, Frances. 2019. "Cairncross Review: A Sustainable Future for Journalism." *Department for Digital, Culture, Media and Sport*, February 12. Accessed 16 December 2019. https://web.archive.org/web/20191216095344if_/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf.

Cockburn, Harry. 2019. "Schools to Teach Children About Fake News and "Confirmation Bias", Government Announces." *The Independent*, July 15. Accessed 24 August 2020. www.independent.co.uk/news/education/education-news/fake-news-schools-education-online-risks-confirmation-bias-damian-hinds-government-a9004516.html.

Connell, Michael, and Sarah Vogler. 2017. "Russia's Approach to Cyber Warfare." *CNA Analysis & Solutions*.Accessed 24 August 2020. www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Crain, Matthew, and Anthony Nadler. 2019. "Political Manipulation and Internet Advertising Infrastructure." *Journal of Information Policy* 9: 370–410. doi:10.5325/jinfopoli.9.2019.0370.

Darczewska, Jolanta. 2014. *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*. Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia / Centre for Eastern Studies (42).

Digital, Culture, Media and Sport Committee. 2019. "Disinformation and 'Fake News'." *UK Parliament*. Accessed 24 August 2020. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Digital Forensic Research Lab. 2018. "Fake News: Defining and Defeating. Atlantic Council." *Medium*, January 19. Accessed 24 August 2020. https://medium.com/dfrlab/fake-news-defining-and-defeating-43830a2ab0af.

Eady, Gregory, Jonathan Nagler, Andy Guess, Jan Zilinsky, and Joshua A. Tucker. 2019. "How Many People Live in Political Bubbles on Social Media? Evidence From Linked Survey and Twitter Data." *SAGE Open* 9 (1): 1–21. doi:10.1177/2158244019832705.

EU vs Disinfo. 2019. "UK Destroying Evidence on the Skripal Case." *EU vs Disinformation*. Accessed 8 January 2020. https://euvsdisinfo.eu/report/uk-destroying-evidence-on-the-skripal-case/.

Facebook. 2019. "Removing Coordinated Inauthentic Behavior From China." *Facebook*, August 19. Accessed 8 January 2020. https://about.fb.com/news/2019/08/removing-cib-china/.

Facebook. 2020. "About the Ad Library.". Accessed 24 August 2020. www.facebook.com/business/help/2405092116183307?id=288762101909005.

Farrell, Henry, and Bruce Schneier. 2018. *Common-Knowledge Attacks on Democracy*. Berkman Klein Center Research Publication 7. doi: 10.2139/ssrn.3273111.

Feikert-Ahalt, Clare. 2019. "Initiatives to Counter Fake News." Library of Congress. Accessed 9 January 2020. www.loc.gov/law/help/fake-news/counter-fake-news.pdf.

Franke, Ulrik. 2015. *War by Non-Military Means: Understanding Russian Information Warfare*. Stockholm: Totalförsvarets Forskningsinstitut. https://dataspace.princeton.edu/jspui/handle/88435/dsp019c67wq22q.

Gillespie, Tarleton. 2015. "Platforms Intervene." *Social Media+Society* 1 (1): 1–2. doi:10.1177/2056305115580479.

Goodman, Emma. 2019. "The Online Harms White Paper: Its Approach to Disinformation, and the Challenges of Regulation." Blog-paper. *London School of Economics*, April 10. Accessed 24 August 2020. https://web.archive.org/web/20191216095351/https://blogs.lse.ac.uk/medialse/2019/04/10/the-online-harms-white-paper-its-approach-to-disinformation-and-the-challenges-of-regulation/.

Gorwa, Robert. 2019a. "The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content." *Internet Policy Review* 8 (2): 1–22. doi:10.14763/2019.2.1407.

Gorwa, Robert. 2019b. "What is Platform Governance?" *Information, Communication & Society* 22 (6): 854–871. doi:10.1080/1369118X.2019.1573914.

Gorwa, Robert, and Douglas Guilbeault. 2018. "Unpacking the Social Media Bot: A Typology to Guide Research and Policy." *Policy & Internet* 40 (3): 420. doi:10.1002/poi3.184.

Government Communications Department. 2019. "Finland Has Yhe Best Elections in the World. And Why is That?" Accessed 16 December 2019. https://valtioneuvosto.fi/en/article/-/asset_publisher/10616/suomessa-on-maailman-parhaat-vaalit-mieti-miksi-.

Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122. doi:10.1080/00396338.2017.1399730.

Grøtan, Tor Olav, Jannicke Fiskvik, Peter Halland Haro, Per Gunnar Auran, Per Gunnar Mathisen, Geir Hågen Karlsen, Melanie Magin, et al. 2019. På leting etter utenlandsk informasjonspåvirkning. En analyse av det norske kommunestyre- og fylkestingsvalget 2019. (Searching for foreign

disinformation campaigns) SINTEF Report. Accessed 24 August 2020. www.regjeringen.no/contentassets/4d850821991746ecbcd9477a475baf73/sintef-rapport_2019-01292_gradering_apen.pdf.

Guess, Andrew, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, and Jason Reifler. 2019. "Fake News, Facebook Ads, and Misperceptions." Accessed 24 August 2020. www.dartmouth.edu/~nyhan/fake-news-2018.pdf.

Gusterson, Hugh. 1997. "Studying Up Revisited." *Political and Legal Anthropology Review (PoLAR)* 20 (1): 114–119.

Heawood, Jonathan. 2018. "Pseudo-public Political Speech: Democratic Implications of the Cambridge Analytica Scandal." *Information Polity* 23 (4): 429–434. doi:10.3233/IP-180009.

Helberger, Natali, Jo Pierson, and Thomas Poell. 2018. "Governing Online Platforms: From Contested to Cooperative Responsibility." *The Information Society* 34 (1): 1–14. doi:10.1080/01972243.2017.1391913.

Herpig, Sven, Julia Schuetze, and Jonathan Jones. 2018. "Securing Democracy in Cyberspace." *Stiftung Neue Verantwortung*. October 2018. Accessed 24 August 2020. https://cyber-peace.org/wp-content/uploads/2018/10/TCF-Securing_Democracy_in_Cyberspace.pdf.

HM Government. 2019a. "Online Harms White Paper." Accessed 16 December 2019. https://web.archive.org/web/20191216095340if_/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

HM Government. 2019b. "SHARE Checklist. Don't Feed the Beast." *HM Government*. Accessed 16 December 2019. https://web.archive.org/web/20191216094044/https://sharechecklist.gov.uk/.

Howard, Philip N., and Samantha Bradshaw. 2019. "The Global Disinformation Disorder." *Oxford Computational Propaganda Project*. Accessed 24 August 2020. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

IFCN. 2020. "IFCN Signatories." Verified Signatories of the IFCN code of principles. Accessed 24 August 2020. https://ifcncodeofprinciples.poynter.org/signatories.

Jamieson, Kathleen Hall. 2018. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*. New York: Oxford University Press.

Johansen, Per Anders, and Fredrik Hager-Thoresen. 2019. "Slik har partiene prøvd å vinne valget på Facebook." *Aftenposten*, 9 September. Accessed 1 September 2020. www.aftenposten.no/norge/i/XgpVPb/slik-har-partiene-proevd-aa-vinne-valget-paa-facebook.

Just, Natascha, and Michael Latzer. 2017. "Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet." *Media, Culture & Society* 39 (2): 238–258. doi:10.1177/0163443716643157.

Justitieministeriet. 2019. "Valpåverkan – Val." Finnish Government, Ministry of Justice, department for democracy and public law. Accessed 24 August 2020. https://web.archive.org/web/20191216092556/https://vaalit.fi/sv/valpaverkan.

Kalsnes, Bente. 2019. *Falske Nyheter. Løgn, desinformasjon og propaganda i den digitale offentligheten*. (Fake News. Lies, disinformation and propaganda in the digital public sphere). Monography. Oslo: Cappelen Damm Akademisk.

Karlsen, Geir Hågen. 2019. "Divide and Rule: Ten Lessons About Russian Political Influence Activities in Europe." *Palgrave Communications* 5 (1): 138. doi:10.1057/s41599-019-0227-8.

Kenney, Martin, Dafna Bearson, and John Zysman. 2019. "The Platform Economy Matures: Pervasive Power, Private Regulation, and Dependent Entrepreneurs." (June 25, 2020). 59 pages. Available at *SSRN Journal*. doi:10.2139/ssrn.3497974.

Kim, Young. 2018a. "Anonymous Groups Targeted Key Battlegrounds on Facebook." Project Brief. *University of Wisconsin-Madison*. Accessed 24 August 2020. https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Anonymous-Groups-Targeted-Key-Battlegrounds-on-Facebook.YMK_.Project-Brief.v.6.1.final_.pdf.

Kim, Young. 2018b. "Nonwhite Recruitment and Suppression." *University of Wisconsin-Madison*. Accessed 20 August 2020. https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/08/nonwhite-recruitment-and-suppression.Russia.Kim_.v.3.080818.pdf.

Kim, Young Mie, Jordan Hsu, David Neiman, Colin Kou, Levi Bankston, Soo Yun Kim, Richard Heinrich, et al. 2018. "The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook." *Political Communication* 35 (4): 515–541. doi:10.1080/10584609.2018.1476425.

Kommunal og moderniseringsdepartementet. 2019. "Ti tiltak for hindre uønsket påvirkning i valggjennomføringen. regjeringen.no." Accessed 16 December 2019. https://web.archive.org/web/20191012130649/https://www.regjeringen.no/no/aktuelt/ti-tiltak-for-hindre-uonsket-pavirkning-i-valggjennomforingen/id2661220/.

Kragh, Martin, and Sebastian Åsberg. 2017. "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case." *Journal of Strategic Studies* 40 (6): 773–816. doi:10.1080/01402390.2016.1273830.

Kumar, Srijan, Robert West, and Jure Leskovec. 2016. "Disinformation on the Web." In *Proceedings of the 25th International Conference on World Wide Web*, edited by Jacqueline Bourdeau, 591–602. Accessed 3 October 2019. http://infolab.stanford.edu/~west1/pubs/Kumar-West-Leskovec_WWW-16.pdf.

Leiserowitz, Anthony A., Edward W. Maibach, Connie Roser-Renouf, Nicholas Smith, and Erica Dawson. 2013. "Climategate, Public Opinion, and the Loss of Trust." *American Behavioral Scientist* 57 (6): 818–837. doi:10.1177/0002764212458272.

Lin, Carolyn A. 2019. "The Challenge of Information and Communication Divides in the Age of Disruptive Technology." *Journal of Broadcasting & Electronic Media* 63 (4): 587–594. doi:10.1080/08838151.2019.1699677.

Mackintosh, Eliza. 2019. "Finland is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy." *CNN*. May 2019. Accessed 24 August 2020. https://web.archive.org/web/20191216090843/https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

Marwick, Alice, and Rebecca Lewis. 2017. "Media Manipulation and Disinformation Online." *Data & Society*. Accessed 3 October 2019. https://datasociety.net/wp-content/uploads/2017/05/DataAndSociety_MediaManipulationAndDisinformationOnline-1.pdf.

Moore, Martin. 2018. *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*. London: Oneworld Publications.

Morgan, Susan. 2018. "Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy." *Journal of Cyber Policy* 3 (1): 39–43. doi:10.1080/23738871.2018.1462395.

Mozur, Paul, and Mark Scott. 2016. "Fake News in U.S. Election? Elsewhere, That's Nothing New." *New York Times*, 18 November. Accessed 18 September 2019. www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-new.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=EndOfArticle&pgtype=article.

National Cyber Security Centre. 2019. "Election Guidance for Local Authorities." Accessed 16 December 2019. www.ncsc.gov.uk/guidance/election-guidance-for-local-authorities.

Nyhan, Brendan. 2019. "Why Fears of Fake News Are Overhyped." *Medium*, February 4. Accessed 3 October 2019. https://gen.medium.com/why-fears-of-fake-news-are-overhyped-2ed9ca0a52c9.

Olejnik, Lukasz. 2016. "Technological Soft Influence on Elections." Blog-post. Accessed 24 August 2020. https://blog.lukaszolejnik.com/soft-influence-on-societies/.

Olejnik, Lukasz, and Claude Castelluccia. 2016. "To Bid or Not to Bid? Measuring the Value of Privacy in RTB." Accessed 1 September 2020. https://lukaszolejnik.com/rtb2.pdf.

Olsson, Jonas, and Ann Wollner. 2019. "Kritik mot Valmyndigheten efter SVT:s uppgifter om cyberattack på valdagen." *SVT Nyheter*, 23 February. Accessed 3 January 2020. www.svt.se/nyheter/inrikes/kritik-mot-valmyndigheten-efter-svt-s-uppgifter-om-cyberattack-pa-valdagen.

Patel, Andy. 2019. "Analysis of Brexit Centric Twitter." F Secure-Blog. Accessed 24 August 2020. https://web.archive.org/save/https://blog.f-secure.com/analysis-of-brexit-centric-twitter-activity/.

Pope, Amy E. 2018. "Cyber-securing Our Elections." *Journal of Cyber Policy* 3 (1): 24–38. doi:10.1080/23738871.2018.1473887.

Prier, Jarred. 2017. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* 11 (4): 50–85. www.nature.com/articles/s41599-019-0227-8.pdf.

Riiheläinen, Janne. 2018. "The Threat That Russia Poses." *Disciple Scientist*, July 23. Accessed 24 August 2020. https://web.archive.org/web/20190927023548/https://disciplescientist.wordpress.com/2018/07/23/the-threat-that-russia-poses/.

Robinson, Olga. 2018. *Malicious Use of Social Media: Case Studies from BBC Monitoring*. With assistance of BBC Monitoring. NATO STRATCOM COE.

Sablina, Liliia. 2019. "'We Should Stop the Islamisation of Europe!': Islamophobia and Right-Wing Radicalism of the Russian-Speaking Internet Users in Germany." *Nationalities Papers* 24: 1–14. doi:10.1017/nps.2019.76.

Splidsboel Hansen, Flemming, and Troels Jensen. 2016. "Russisk Hybridkrig. fremtidens krig er i fuld gang." Danish National Research Database. Accessed 24 August 2020. www.forskningsdatabasen.dk/en/catalog/2439570768.

Steensen, Steen. 2019. "Journalism's Epistemic Crisis and Its Solution: Disinformation, Datafication and Source Criticism." *Journalism* 20 (1): 185–189. doi:10.1177/1464884918809271.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. 2017. "Detecting Bots on Russian Political Twitter." *Big Data* 5 (4): 310–324. doi:10.1089/big.2017.0038.

Tufekci, Zeynep. 2018. "Facebook's Surveillance Machine." *New York Times*, March 19. Accessed 18 October 2019. www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

Twitter. 2018. "Database on Information Operations." Accessed 13 December 2019. https://transparency.twitter.com/en/information-operations.html.

Utdanningsdirektoratet. 2019. "Nye læreplaner – grunnskolen og gjennomgående fag vgo." The Norwegian Directorate for Education and Training. Accessed 24 August 2020. https://web.archive.org/save/https://www.udir.no/laring-og-trivsel/lareplanverket/Nye-lareplaner-i-grunnskolen-og-gjennomgaende-fag-vgo/.

Walker, Shawn, Dan Mercea, and Marco Bastos. 2019. "The Disinformation Landscape and the Lockdown of Social Platforms." *Information, Communication & Society* 22 (11): 1531–1543. doi:10.1080/1369118X.2019.1648536.

Woolley, Samuel C. 2016. "Automating Power: Social Bot Interference in Global Politics." *First Monday* 21 (4), doi:10.5210/fm.v21i4.6161.

Ziegler, Charles E. 2018. "International Dimensions of Electoral Processes: Russia, the USA, and the 2016 Elections." *International Politics* 55 (5): 557–574. doi:10.1057/s41311-017-0113-1.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89. doi:10.1057/jit.2015.5.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st ed. New York: Public Affairs.