Unsocial media in the EU and Russia

Maxine David

In its 2018 report on the state of EU-Russia political relations, the European Parliament condemned Russia for its use of disinformation campaigns, referring specifically to Russia's use of social media to interfere in the affairs of EU member states (European Parliament 2018). As a space, therefore, in which existing tensions in the EU-Russia relationship are played out, attention to social media is warranted. However, as 'Internet-based applications' (Kaplan in van Dijck and Poell 2013), social media are caught up in arguments about the future of internet governance generally, such that, when it comes to social media, EU-Russia relations exist within a wider context. Each actor is just two among an array of actors facing similar challenges as technology develops in such a way and at such a pace as to outstrip the capacity of any governmental actor to anticipate or control fully developments in the information space. The EU and Russia have responded in ways that are not necessarily bound up in their mutual relations. Their separate responses nevertheless illuminate the relationship, particularly with respect to their political and normative differences and how they act on behalf of their societies in terms of reinforcing democracy or undermining it.

'[D]esigned to facilitate social interaction and for using, developing and diffusing information through society' (Kavanaugh et al. 2012: 482), social media are spaces in which a range of actors, including governmental, can insert themselves in both transparent and opaque ways. This explains the resurgence of political, scholarly and journalistic work on propaganda, misand disinformation (Bennet and Livingstone 2018; Helmus et al. 2018; McGeehan 2018; Nimmo 2016). This agenda is driven by the actions of Russia, the dogwhistle tactics of certain EU leaders and politicians (witness the conspiratorial discourse of Italy's Matteo Salvini on the 'genocide of the Italian people' or Hungary's Orban on 'Islamic expansion') and by the Trump administration and associated claims of 'fake news'.

This chapter proceeds as follows. It first considers the literature regarding what social media are, talking through the platforms and their 'ecological' environment, the context in which they and their users operate. This first section also examines the evolution of social media research, from earlier preoccupations with identifying users¹ to more recent research concerned with patterns of and motivations for usage, as well as the response of governments to developments here. The chapter then moves to a discussion of Russian attempts to manipulate EU societies using social (and other) media before looking at the separate responses in Russia and in the EU

to the challenges brought by technological changes impacting on information, democracy, the public sphere and political participation. Here, the role of corporations is also considered, an important conversation for understanding the values debate in relation to the EU and Russia.

Social media – context and ecology

It is worth cementing understandings of what social media are, given a noticeable lack of time is spent on defining them (Lomborg 2017). First, their base on the internet means social media form part of an interconnected system, meaning policy relating to internet governance has implications for social media; indeed, such media often occasion the need for regulatory mechanisms. Second, social media are applications or, better, platforms that allow ordinary people to self-publish, facilitating 'the creation and exchange of user-generated content' (Kaplan in van Dijck and Poell 2013; see also Bennett and Segerberg 2012; Lomborg 2017; Shirky 2011). A third definitional aspect is that social media are platforms for building hierarchical or horizontal connections among people. Motivations may be purely social, with social media used for building and maintaining social relationships (Valenzuela 2013), what Van Dijck and Poell (2013) refer to as 'connectedness' and Boulianne (2019) as 'networking'. Social media platforms have been focused on, too, for their role as a place where people read and exchange news (Boulianne 2019; Lomborg 2017; Valenzuela 2013), as well as a forum for political participation or expression (Bennett and Segerberg 2012; Boulianne 2019: 40; Valenzuela 2013). Finally, social media are used for information sharing (Bennett and Segerberg 2012; Boulianne 2019; Shirky 2011; Valenzuela 2013).

Social media platforms are therefore fora for citizens to self-publish, exchange information, communicate and build communal connections, including politically directed networks. The latter two aspects particularly have centred societies in EU-Russian relations, as well as state–society relations – with many EU states concerned about Russian state-sponsored attempts to influence the information shared on social media (Willemo 2019: 16–17) with a view to 'erod[ing] the EU countries' internal consensus' (Liik 2018: 7); while the 2011 and 2012 anti-regime protests in Russia meant the 'state began to narrate the Internet as a Western subversive technology . . . and ultimately a threat to Russian society that needs to be controlled and curtailed' (Budnitsky and Jia 2018: 606).

In terms of what social media might be researched, a distinction can be made between those social media that allow people to self-publish and connect versus social media messaging apps such as Whatsapp, Telegram or Signal that allow connections (although the end-to-end encryption of the latter two make them invaluable applications for organising political activity without fear of state surveillance) but which are not used for the creation and publication of user content. In the EU-Russian context, the major social media platforms, Facebook, Instagram and Twitter are used in the EU states and Russia and therefore offer scope for the building of cross-national social connections. Russian social media platforms, Vkontakte (equivalent to Facebook), Odnoklassniki and My World are used (the latter two much less so) in Russia but, while not restricted to Russia, are not in common use across the EU states by non-Russian EU citizens. Unsurprisingly, given their reach, Facebook and Twitter garner the lion's share of general analytical attention, 2016 statistics showing that approximately 80 per cent of Facebook users and 72 per cent of Twitter accounts are located outside the United States (Alexa.com in Boulianne 2019: 41).

While the platforms *can* be investigated individually, they exist in a broader set of communications, both online and offline. Scholars argue for an ecological mindset when working in this area. Tufekci and Wilson (2012), for instance, argue social media must be placed in relation to

wider changes in political communication: 'the connectivity infrastructure should be analyzed as a complex ecology rather than in terms of any specific platform or device' (2012: 365). Others have made a different but connected point about the limits of what is analytically possible if the intent is to establish the effect of a single social medium upon its users. Boulianne cautions that:

Given the seamless use of multiple platforms, it is difficult to distinguish the use of specific platforms. While platform effects seem to be a promising line of future research, the challenge will be untangling the effects of specific platforms given the interconnectedness of their uses.

(2019:49)

Others have focused on these interconnections. Lokot (2018) reveals how Russian opposition activists understand the importance of social media in generating a public profile but also, in the context of the 'networked authoritarian regime' (see also Maréchal 2017) operated in Russia, focus on their own security, hosting some material abroad and using whatever tools the internet provides to highlight their causes. This is consistent with other studies focused on how social media are used in protest situations, the method used for accessing the platforms, for example, computer, mobile or both, as well as other connectivity tools, text, television and so on (see Tufekci and Wilson 2012). Thus, social media are an important part of the online world but precisely that, a *part* of it, meaning analysis of social media necessarily strays beyond those media alone.

Underlining the ecology of technological communications, studies have found that social media function as channels of communication to traditional media, sometimes even setting 'mainstream' media agendas.² Traditional media can also have amplifying effects. However, in their useful overview of how social media have evolved, McCay-Peet and Quan-Haase (2017) make the powerful point that we are talking of a highly dynamic area, that context is all important. This is a point underlined by Lomborg (2017: 8) too, who also argues for more conceptually directed research that is critically and historically rooted. There is therefore a limit to how far conclusions drawn in any one context can be deemed applicable to another – relevant counsel for the study of EU-Russian social media relations.

Such caution is doubly warranted given the fast pace at which social media analysis has shifted. In the context of arguments that social media were democratising tools, earlier accounts were concerned with the demographics of internet access and social media usage: typically, questions revolved around whether usage differed along gender, age, education and other lines and what this meant for representation. In the context of EU-Russia relations, this was especially true in the Russian, rather than EU, case (David 2015). At the current time, given internet penetration rates are far higher,³ aided by developments in mobile technology, especially 4G, analysis takes internet access – and therefore social media access – across all the people in EU-Russia relations far more for granted. The bigger questions debated revolve around the role and influence of a wide variety of actors – whether governmental or non-governmental. Additional preoccupations are how people use social media, to what effect, the impact of corporatism on social media and therefore democracy and recently created citizen journalists.

It is worth adding here the voices of the social media platforms themselves. Vkontakte's 'mission is to connect people, services and companies by creating simple and convenient communication tools' (Vkontakte n/d). In 2017, Facebook changed its mission statement from one that spoke of 'making the world more open and connected' to one in which the stated aim is to 'give people the power to build community and bring the world closer together' (Zuckerberg 2017). But are social media platforms really empowering people?

Social media's dwindling democratising potential

Given the nature of the media under examination – that is, the social world – it is unsurprising that questions of power feature. Questions about whether technological advances like the internet and, later, social media, could facilitate the building of a more politically participative citizenry became particularly acute in the aftermath of the so-called Arab Spring of 2011, in which social media were widely reported as having contributed to this showing of democratic spirit. Work focused on the capacity of social media to put pressure on authoritarian regimes (Tufekci and Wilson 2012), offering a new space in which to organise opposition and express opinions. The tale was largely one of social media empowering people to tell their own story in their own way, using self-gathered evidence, relaying it in real time (Van Dijck and Poell 2013). Facebook was an important first source of information about the 2011 Egyptian protests, also playing host to documentary photographs and videos. Both Twitter and blogs were important media for keeping others informed about events as they occurred (Tufekci and Wilson 2012: 374).

All ideas of the democratising potential of social media have been tempered by evidence that governments are alive to this potential (Bruns 2019; Shirky 2011; Tufekci and Wilson 2012; van Dijck and Poell 2013). The Arab Spring engendered feelings of vulnerability in some, including among 'Russian leaders, who are seeking to impose strict regulation on the internet infrastructure and social networks' (Nocetti 2015: 112), impelled by their own experience of protests at home, especially in 2011–12, which '[p]opular and media discourse framed . . . as a revolt of the networked online public' (Budnitsky and Jia 2018). But governments of all persuasions have understood social media potentially expose government and society to risk, provoking repressive responses.

Positive accounts exist, of course, of how social media, as sources of information, can facilitate exchange of knowledge, perception or need, of concerns and experience. Kavanaugh et al. (2012) point out that governments can access huge amounts of information about their citizens, extending their reach with a view to providing better services (see also Van Dijck and Poell 2013: 10). Such accounts are outweighed, though, by those who consider the ways in which governments use social media *against* rather than *for* their citizens. Fuchs (2012) reminds us of responses to the 2011 riots in England in which government and mainstream media talked of social media as the causes of the riots, distracting from the economic and political root causes. Thus, social media became a scapegoat for poor policy rather than a platform to build more responsive policies (see also van Dijck and Poell 2013; and Zollmann in Klaehn et al. 2018: 184–5). Other governmental responses are deeper and more extensive, China a common reference point for showing what governments are capable of in this regard (see Xu and Albert 2017). But it is clear that a far wider range of citizens are vulnerable to injurious government responses:

Social media manipulation is big business. Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media. In a few countries this includes efforts to counter extremism, but in most countries this involves the spread [sic] junk news and misinformation during elections, military crises, and complex humanitarian disasters.

(Bradshaw and Howard 2018: 3)

In their report, Bradshaw and Howard identified evidence of political parties employing consulting firms to 'use social media to manipulate public opinion' (2018: 9) in 14 countries, including

Austria, Poland and the United Kingdom, while Russia employed 'tech savvy youth... to support social media manipulation efforts' (ibid.). In just short of a decade, analysis of social media has made a journey from optimism that ordinary people can both exercise and enhance their democratic rights to concerns about how they are the subject of manipulation by both governmental (including Russia and some EU states) and corporate actors on those very platforms supposed to 'emancipate' them.

Analysts have also noted the fragmenting effects of social media: 'social networks . . . have actually increased the tendency of people to polarize along group and even tribal lines' (Barabanov et al. 2018: 17). As far as the Russian landscape is concerned, this is a development out of step with a Kremlin that 'continues to create a unipolar political space within Russia' (Morozov 2008: 173). But for a Kremlin intent on eroding democracy and sowing confusion *elsewhere*, such media are important instruments. For an EU concerned about the susceptibility of their citizenry to conspiracy theories, mis- and disinformation and fake news, malign intentions on the part of the Kremlin combined with a public largely lacking good information literacy make for a perfect storm.

Social media as a battleground

In the ECFR 2018 Power Audit, 18 of the then-28 member states were reported as fearing Russian interference in their domestic politics through propaganda. Boyd-Barrett (in Klaehn et al. 2018: 174) spoke of how in the 2017–2018 period or so he was focused on 'some of the most significant propaganda wars of our times', most of which Russia had been part of and which successfully sowed doubt regarding what constitutes a reliable source. Others also echo the language of war, Giles (n.d.) referring to Russia's 'information warfare'. Direct lines to the Kremlin are not always easy to establish, but, whether directly or through tacit permission, consensus abounds: the Kremlin enacts (or allows) disinformation and propaganda policies, mixing truth and fiction in a near-perfect concoction designed to instil doubt in the mind of the public (Helmus et al. 2018; Hug 2017; Soldatov and Borogan 2015).

While the St Petersburg troll factory is known to most, it is just one of a 'network of troll farms' (Giles n/d: 10). Trolls and bots are used to disseminate and augment mis- and disinformation on social media sites (Willemo 2019), the Kremlin and its proxies understanding all too well the relationship between traditional and social media and its amplifying effects, especially given the increasingly cluttered but fragmented information environment. There are numerous cases that illustrate Russian activity seeking to divide society in EU member states, many exploiting existing vulnerabilities. The so-called migration crisis was a particular case in point, exemplified by the 2016 fake 'Lisa' story in Germany, where Muslim migrants were accused of raping a Russian-German girl, a story amplified over RT Deutsch as well as social media and attracting attention beyond Russian state media in Germany and elsewhere. Further, Russia is deemed to have used social media to manipulate publics in elections in France, Germany, the United Kingdom's EU referendum and the Catalan vote on secession from Spain (McGeehan 2018: 52; Chernenko in this volume). Other tactics look mischievous rather than malicious, such as the taking over of a Swedish television station's Twitter account in 2015 to relay Russian information (Giles n/d: 10). But not all those who fall victim to Russia's 'information war' do so unwillingly. Orban's Hungary is regarded as consenting to Russian state capture, among other things, by inviting Russian disinformation through the establishment and part funding of a Russkiy Mir Centre in 2017 (see Krekó and Győri 2017).

The EU, albeit slowly, has responded to Russian interference. In March 2015, the European Council (2015) instructed the high representative to develop an action plan in response

to Russian disinformation. From this emerged a communication team (East StratCom), which identified a relative vulnerability in the eastern neighbourhood and a need to bolster the general media environment (EastStratCom 2015). Strengthening the message of EU unity against the Kremlin's assault on the information space, the European Parliament delivered its own report outlining its own concerns, 5 of its 24 points speaking to questions of information, journalism, censorship and their impact on civil society (European Parliament 2015). In 2019, the budget for the EEAS's strategic communications was doubled, to 5 million EUR, part of it allocated to increasing staffing, to work in Brussels as well as the delegations. Despite this, it remained unclear whether the East StratCom Team was an effective way of managing the problem. In the longer term, we would want to see research focused on perceptions of the EU as a propaganda actor itself: what has been, in Bjola's words (2018) the impact on the EU's 'moral authority'?

Meanwhile, in March 2019, the establishment of the Rapid Alert System saw the EU joining forces with the G7 and NATO to 'identify and prevent spread of disinformation campaigns' online, including through social media (European Commission 2019). The year before, the Social Observatory for Disinformation and Social Media Analysis (SOMA) was launched after receiving the EU's H2020 funding. In process terms, it bears some resemblance to the East Stratcom team in that it also asks people to report on disinformation. However, its objectives are wider, addressing many of the criticisms levelled at the EU approach so far. It is well resourced, for example, in terms of applications to verify content, and embodies the widening actorness talked about so much in the social media literature, bringing universities, media organisations, tech and consulting companies and civil society organisations (SOMA 2019a) under an umbrella organisation that demarcates independent members from policymakers. To cement its structural base, in May 2019, it launched the EU Centre for Research in Social Media and Information (EU REMID) (SOMA 2019a). Perhaps most notably, by funding SOMA, we see the EU turning from a dominant focus on identifying and countering Russian disinformation on social and other media to looking inward, too, examining interactions on social media among Italian political parties and their Twitter followers, for instance (SOMA 2019b).

While unlikely to have any effect in terms of improving EU-Russia relations, the revised approach has two benefits. First, it suggests the EU realises Russia is not the only source of disinformation EU citizens encounter on social media. Second, it represents a more sensible approach to improving the social media landscape for EU citizens. This is much needed considering a 2018 Eurobarometer report revealed a very low level of trust (26 per cent averaged across the EU) in the news EU citizens read on their online social networks and messaging apps, albeit with considerable differences among the member states (Flash Eurobarometer 464 2018: 4; 9). SOMA is a relatively new actor in the EU environment, so its efficacy is undetermined, but the EU's reinvigorated approach to the information space and to the regulation of social media companies gives some cause for optimism.

Regulating the online world

As already intimated, state actors are not the only sources of threat to the EU or Russia. Both have fought battles to ensure they can assert some control over the internet and social media companies. Both share misgivings about the hegemony of the United States, whether the US state with respect to internet governance or its corporations with respect to social media platforms. The damage to democracy that corporations can do was highlighted in the Cambridge Analytica scandal, a prime example of how certain logics, in this case capitalist economics, function to depress democratising potential. With access gained to huge data sets of social media users, the consulting firm Cambridge Analytica used algorithms to mine the data harvested from social media, much

of it from Facebook,⁴ categorising groups of people in order to micro-target social media users in the United Kingdom's referendum on EU membership and in the 2016 US elections. Such use of proprietary knowledge makes it impossible to know precisely how users are being steered or by whom. The scandal is important for revealing the microtargeting but also outlines a pattern of dubious behaviour on Facebook's part, its tendency to attempt to 'divert attention from its own business practices' and to employ strategies that 'by accident or design also severely undermine critical, independent, public-interest research' (Bruns 2019: 5); analysis supported by Broudy, who speaks of the interesting nature of social media in relation to propaganda and commercial logics, commenting that 'there isn't much profit in truth-telling' (Klaehn et al. 2018: 181–2).

Despite, widely speaking, converging concerns about regulation of the information and social media space, the EU and Russian responses have diverged. Russia has been a consistently vocal voice on internet governance, failing in its 2012 attempts to secure revision of the International Telecommunication Regulations that govern the internet, in order to ensure the influence of multiple stakeholders, the EU voting against the revisions. Russia has participated in the global Internet Governance Forum (IGF) since its inception and the regional group of IGFs since 2010. It has also been concerned with ensuring social media platforms, including non-Russian, are subject to Russian regulatory forces and, even without this, has sought to compel social media companies such as Facebook and Twitter to remove content (see Vendil Pallin 2017: 11-12). More recently, it has taken steps at home to assert its sovereignty over the internet, as discussed in more detail later. The European Commission became seized of the matter in a different way; witness the 2018 General Data Protection Regulation (GDPR), important for social media since it affects how online companies, including social media platforms, collect user data. This is a point much understood by the EU, as its 2017 antitrust case against Google (European Commission 2017) and the launch of its probe into Facebook and Google in late 2019 (EUObserver 2019) attest. However, the effectiveness of the GDPR is much questioned as a result of little evidence the EU is enforcing it against Big Tech, suggesting 'the EU Parliament might have the greatest domain knowledge and political will to act', but it 'has little actual leverage over the platforms' (Bruns 2019: 15).

Clearly, social media do not form a landscape in which transparency abounds, to the detriment of democracy, given an 'open public discourse is one of the basic conditions of democracy, because this is how citizens can discuss their common matters, form political opinions and ultimately reach a political decision' (European Parliament 2019: 11). The EU has focused increasingly on protecting citizens, conscious that they make themselves more vulnerable to malign intentions by providing, largely unwittingly in terms of understanding how they might be used, data about their preferences, politics, family and friends.

Facebook's Mark Zuckerberg has acknowledged that online regulation is unavoidable but has also correctly identified the fact that questions abound regarding: 'which nation's values are going to determine what speech is going to be allowed for decades to come' (in Brandom 2019). The existing differences between the EU and Russia are, as in other areas explored in this Handbook, brought sharply into focus.

Russia's approach

Russia offers evidence to support theoretical arguments about how governments can subvert the democratising potential of social media, with recent developments sparking speculation about the internet environment and, by extension, social media. Russia has used its membership of the Shanghai Cooperation Organisation and BRICS to drive an 'Internet sovereignty narrative' (Budnitsky and Jia 2018: 600; David 2018) abroad, while enacting it at home through a

November 2019 bill, known as the internet sovereignty bill. Once fully implemented, it will mean all internet activity passes through state-controlled points, such that the state will be able to block content and identify the origin of traffic. Its critics rightly argue it threatens online freedom, while the Kremlin argues it is justified given the CIA origins of the internet and the freedoms it offers (Soldatov and Borogan 2015). These are merely the latest official developments in a longer pattern of increasing surveillance: from the System for Operative Investigative Activities (SORM), allowing the interception of information; to the 2012 creation of the Federal Supervision Agency for Information Technologies and Communications (Roskomnadzor), authorised to blacklist and block sites; to laws such as the so-called Yarovaya's Law, ostensibly a tool in the fight against terrorism but used to require certain surveillance actions of telecoms providers, including decryption, as well as retention of data in Russia (see David 2015, 2018); or the 2017 legislation forbidding access to proxies, such as VPNs, that allow citizens anonymous access to banned information or sites.

These efforts have had mixed effects. Soldatov and Borogan (2015: 314) point out that Russian internet companies have responded to Kremlin threats by capitulating, that threats can achieve self-censorship. Nevertheless, the Kremlin has not always successfully established control: few VPN providers complied with Roskomnadzor's demands and, famously, neither did Telegram's Chief, Durov. Having failed to force Telegram to deliver on decryption requirements, the Kremlin was then forced to halt its far from granular attempts to block the app after unintentionally blocking a host of other services, with an attendant effect on regular business and economic activities (Kolomychenko 2018). Equally, Russian citizens proved creative, themselves installing VPNs to prevent geo-blocking and ensure encryption.

The latest legislation is a response, however, to such resistance. It empowers the state to cut Russia off from the outside world through the creation of a local domain name server system. This 'splinter-net' will likely reduce the reach of Russian citizen journalism in the types of crisis moments in which such an instrument might be used (Gershkovich 2019), as was the case in the 2011–12 protests. Whether the deep packet inspection tools required to achieve the granularity missing from the 2018 action against Telegram can be made effective still remains to be seen. Nevertheless, the intention – both to censor and silence Russian users of social media – is significant and sets Russia on a quite different path to that advocated in Brussels, although the same cannot be said for all the member states.

EU member states

EU member states may not have gone so far as Russia but they also give cause for concern as the European Parliament (2019) has remarked.

The latest policies and legal measures developed at the Member State and the EU level to tackle disinformation and propaganda have been collected and analysed . . . including the German Network Enforcement Act, the French Act against Informational Manipulation and the Italian law against fake news, along with the co-regulatory initiative between the French government and Facebook. . . . The analysis finds that the **legal restriction of content may pose a greater harm to democracy than disinformation itself**.

In the German case, legislation policing social media companies came into force in 2018, requiring them to remove hate speech and propaganda in 24 hours. In France, President Macron introduced legislation in 2018, conferring power upon the judiciary to remove 'fake news' in an election period, occasioned by concerns of Russian interference in the United Kingdom's EU

referendum and also by the dumping of email data from Macron's party just before the presidential elections, with many suspecting a Russian hand there, too. Further, in late 2018, Facebook announced a time-limited experiment in co-regulation, giving French authorities access and insight into the platform's content policies and how it polices hate speech. In 2018, Facebook also announced an initiative directed at allaying Italian fears, this time through fact-checking on the Italian side, Facebook hosting a corrective piece where necessary. Such moves diverge from the Russian approach but remain vulnerable to much criticism, including for ceding too much ground to the social media companies. However, it is on the grounds of subjectivity of interpretation and consequent censorship that citizens should be concerned, as illustrated in the UK case.

In June 2019, experts of different nationalities came together with a view to '[examining] the similarities and differences between the approach being taken by Russia, the UK and a number of EU member states in managing the online lives of their citizens'. Organised in the context of the British Government's White Paper on Online Harms, the seminar focused on what the United Kingdom could learn from Russian experiences in using child protection laws to regulate (inhibit) freedom of expression online (Foreign Policy Centre 2019). The White Paper proposed that a new regulator be established, with the power to create codes of practice, to sanction (including forcing withdrawal of services and blocking ISP access) offending online platforms and to initiate legal proceedings against the relevant executives (GOV.UK 2019). Those familiar with the 2012 creation and subsequent actions of Roskomnadzor will recognise clear similarities in this securitisation of the online environment. That the United Kingdom is a vastly freer society and largely seen as operating a governmental structure prohibiting the wrongful exercise of power⁵ is beside the point. The seminar functioned as an important moment in which observers were reminded about the dangers of complacency⁶ and of the fact that lessons learned in the Russian environment are not applicable to that space alone.

Concluding remarks

A stark absence considering the social world focused on in the previous discussion has been in relation to people-to-people contacts. The vast majority of attention is focused in the EU-Russia case not on how social media can connect peoples but rather on how Russia has utilised a range of instruments with no particular goal except to erode the trust of EU citizens in their own state, in democracy and information. Equally, scholarly and political attention has been seized by responses to such actions in the EU and recognition that EU member states are no less susceptible to securitising logics than Russia, although it should be emphasised in order to avoid any impression of equivalence that EU states are largely more politically constrained in terms of levels of scrutiny and challenge to governmental attempts to restrict online freedoms. Nevertheless, considering some of the democratic backsliding already seen in some EU states, Brussels has no room to be complacent that its vision of the social media environment - and information space more widely - will be realised and democratic values visibly realised for EU citizens in their social media interactions. There is at least a sign in the last two years or so of Brussels realising this. Future research should continue to focus on the EU institutions and developments in relation to regulatory mechanisms, content verification processes and counterpropaganda projects.

Meanwhile, after years of attempts to build support at the international level to temper the dominance of the United States over internet governance, Russia's domestic policies in relation to social media share more differences than similarities with the EU approach, even while falling short of the relatively repressive Chinese model of internet governance. Still, a continued focus

on the Russian information space, especially asking questions relating to social media platforms, their place in the information and communications ecology and their democratising potential, is very much required.

This therefore remains a ripe space for analysis, both on account of understanding processes in the EU and Russia separately and the impact on external perceptions of both actors. Equally, the 'information war', fought on social as well as other media, warrants continued attention. This is a space in which EU-Russia relations could easily deteriorate further or improve enormously – the direction of travel resting in Russian (Kremlin) hands. As with so many aspects of EU-Russia relations, therefore, this is a story still very much in the writing.

Notes

- 1 Those interested in internet penetration issues can usefully access sources such as the ITU, comScore or statista.com. Other sources, such as Alexa, sit behind paywalls.
- 2 For arguments regarding how Facebook and Twitter fed Al-Jazeera and other media, such that: 'This emerging communication system [...] profoundly transformed the Arab public sphere', see Tufekci and Wilson (2012: 367).
- 3 According to the International Telecommunications Union (2018) 80.86 per cent of Russians were internet users in 2018, up from 70.52 in 2014. EU countries in 2018 varied: France 82.04 per cent, Germany 89.74, Portugal 74.66 and United Kingdom 94.9.
- 4 Cadwalladr has written extensively on this for *The Guardian* over a number of years. See also the documentary *The Great Hack*.
- 5 See Freedom House for country reports: https://freedomhouse.org/report/freedom-world/freedom-world-2018
- 6 See also the work of Index for Censorship.

References

Barabanov, O. et al. (2018) 'Living in a crumbling world', Valdai Discussion Club Report, October.

Bennett, W.L. and Livingston, S. (2018) 'The disinformation order: Disruptive communication and the decline of democratic institutions', *European Journal of Communication* 33(2): 122–39.

Bennett, W.L. and Segerberg, A. (2012) 'The logic of connective action. digital media and the personalization of contentious politics', *Information, Communication & Society* 15(5): 739–68, doi:10.1080/1369 118X.2012.670661

Bjola, C. (2018) The ethics of countering digital propaganda', Ethics & International Affairs 32(3): 305–15.
Boulianne, S. (2019) 'Revolution in the making? Social media effects across the globe', Information, Communication & Society 22(1): 39–54, doi:10.1080/1369118X.2017.1353641

Bradshaw, S. and Howard, P.N. (2018) Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, available at, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf (accessed 3 January 2020).

Brandom, R. (2019) 'Mark Zuckerberg took on China in a speech defending free expression', *The Verge*, available at www.theverge.com/2019/10/17/20919464/mark-zuckerberg-facebook-china-free-speech-georgetown-tiktok-bytedance (accessed 3 January 2020).

Bruns, A. (2019) 'After the 'APIcalypse': social media platforms and their fight against critical scholarly research', *Information, Communication & Society*, doi:10.1080/1369118X.2019.1637447

Budnitsky, S. and Jia, L. (2018) 'Branding internet sovereignty: digital media and the Chinese-Russian cyberalliance', European Journal of Cultural Studies 21(5): 594–613, doi:10.1177%2F1367549417751151

David, M. (2015) 'New social media: modernisation and democratisation in Russia', Perspectives on European Politics and Society 16(1): 95–110, doi:10.1080/15705854.2014.965892

David, M. (2018) 'Russia's Challenge to US hegemony and the implications for Europe', in Salvador Santino F. Regilme Jr. and James Parisot (eds.), Global Cooperation or Conflict? Emerging Powers and the Future of American Hegemony, London: Routledge.

EastStratCom (2015) Action Plan on Strategic Communication, Ref. Ares (2015)2608242-22/06/2015, available at http://eap-csf.eu/assets/files/Action%20PLan.pdf (accessed 1 August 2019).

- EUObserver (2019) 'EU probe targets Google and Facebook data collection', 3 December, available at https://euobserver.com/tickers/146795 (accessed 3 January 2020).
- European Commission (2017) Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. Press Release 27 June 2017, Brussels.
- European Commission (2019) Action plan against disinformation. Report on progress, June 2019, available at https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final. pdf (accessed 3 January 2020).
- European Council (2015) 'European Council meeting, 19 and 20 March 2015 conclusions EUCO 11/15', available at http://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf (accessed 1 August 2019).
- European Parliament (2015) 'European Parliament resolution of 10 June 2015 on the state of EU-Russia relations (2015/2001(INI))', available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015IP0225 (accessed 1 August 2015).
- European Parliament (2018) 'Report on the state of EU-Russia political relations, 2018/2158(INI), A8-0073/2019', Committee on Foreign Affairs, European Parliament 2014–2019.
- European Parliament (2019) 'Disinformation and propaganda impact on the functioning of the rule of law in the EU and its Member States', PE 608.864, February.
- Flash Eurobarometer 464 (2018) 'Fake news and disinformation online', European Commission, available at https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82797 (accessed 3 January 2020).
- Foreign Policy Centre (2019) 'Taking back control? How Russia, the UK and EU member states are seeking to regulate the internet', 18 June, available at https://fpc.org.uk/events/taking-back-control-how-russia-the-uk-and-eu-member-states-are-seeking-to-regulate-the-internet/ (accessed 30 June 2019).
- Fuchs, C. (2012) 'Behind the news. social media, riots, and revolutions', Capital and Class 36(3): 383-91.
- Gershkovich, E. (2019) 'Point of No Return, Russia's libertarians lead protest against sovereign internet', *The Moscow Times*, March 10, available at www.themoscowtimes.com/2019/03/10/point-of-noreturn-russias-libertarians-lead-protest-against-sovereign-internet-a64758 (accessed 1 August 2019).
- GOV.UK (2019) 'Online harms white paper', available at www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#enforcement (accessed 1 August 2019).
- Helmus, T.C. et al (2018) Russian Social Media Influence, Understanding Russian Propaganda in Eastern Europe Santa Monica, CA: RAND.
- Hug, A. (ed.) (2017) The Information Battle: How Governments in the Former Soviet Union Promote Their Agendas and Attack Their Opponents Abroad, London: The Foreign Policy Centre.
- International Telecommunications Union (2018) 'Country ICT data percentage of individuals using the internet', available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (accessed 20 August 2019).
- Kavanaugh, A.L. et al (2012) 'Social media use by government: from the routine to the critical', Government Information Quarterly 29: 480–91.
- Klaehn, J. et al (2018) 'Media theory, public relevance and the propaganda model today', *Media Theory* 2(2): 64–191.
- Kolomychenko, M. (2018) 'Russia tries more precise technology to block Telegram messenger', *Reuters*, 30 August, available at www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ (accessed 20 December 2019).
- Krekó, P. and Győri, L. (2017) 'Hungary: a state captured by Russia', Heinrich Böll Stiftung, available at www.boell.de/en/2017/10/11/hungary-state-captured-russia (accessed 20 December 2019).
- Liik, K. (2018) 'Winning the normative war with Russia: an EU-Russia power audit', European Council on Foreign Relations, May, available at ecfr.eu (accessed 10 August 2019).
- Lokot, T. (2018) 'Be safe or be seen? how Russian activists negotiate visibility and security in online resistance practices', Surveillance and Society 16(3): 332–6.
- Lomborg, S. (2017) 'A state of flux: Histories of social media research', European Journal of Communication 32(1): 6–15.
- Maréchal, N. (2017) 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy', *Media and Communication* 5(1), 29–41, https://doi.org/10.17645/mac.v5i1.808
- McCay-Peet, L. and Quan-Haase, A. (2017) 'What is Social Media and What Questions Can Social Media Research Help Us Answer', in L. Sloan and A. Quan-Haase (eds.), *The Sage Handbook of Social Media Research Methods*, London: Sage, pp. 13–26.

- McGeehan, T.P. (2018) 'Countering Russian disinformation', *Parameters* 48(1): 49–57. Online at https://search.proquest.com/docview/2062950905?pq-origsite=gscholar (accessed 10 January 2020).
- Morozov, V. (2008) 'Sovereignty and democracy in contemporary Russia: a modern subject faces the post-modern world', *Journal of International Relations and Development* 11: 152–80).
- Nimmo, B. (2016) Countering Disinformation: an ABC, Policy Brief, Issue 2016/01 February 2016, Institute for European Studies, Vrije Universiteit Brussel.
- Nocetti, J. (2015) 'Contest and conquest: Russia and global internet governance', *International Affairs* 91(1): 111–30.
- Shirky, C. (2011) 'The Political Power of Social Media', Foreign Affairs January/February, available at www. foreignaffairs.com/articles/2010-12-20/political-power-social-media (accessed 1 August 2019).
- Soldatov, A. and Borogan, I. (2015) The Red Web, New York: Public Affairs.
- SOMA (2019a) 'The observatory', available at www.disinfobservatory.org/the-observatory/ (accessed 3 January 2020).
- SOMA (2019b) 'SOMA project newsletter issue #3', available at https://mailchi.mp/651153c38aae/soma-newsletter-no3?e=%5BUNIQID%5D (accessed 3 January 2020).
- Tufekci, Z. and Wilson, C. (2012) 'Social media and the decision to participate in political protest: observations from Tahrir Square', *Journal of Communication* 62: 363–79.
- Valenzuela, S. (2013) 'Unpacking the use of social media for protest behavior: the roles of information, opinion expression, and activism', *American Behavioral Scientist* 57(7): 920–42.
- Van Dijck, J. and Poell, T. (2013) 'Understanding social media logic', *Media and Communication* 1(1): 2–14. Vendil Pallin, C. (2017) 'Internet control through ownership: the case of Russia', *Post-Soviet Affairs* 33(1): 16–33.
- Vkontakte (n/d) 'Company info', available at https://vk.com/about (accessed 1 August 2019).
- Willemo, J. (2019) Trends and Developments in the Malicious Use of Social Media, Riga: NATO Stratcom COE.
- Xu, B. and Albert, E. (2017) 'Media censorship in China', *Council on Foreign Relations*, available at www. cfr.org/china/media-censorship-china/p11515 (accessed 1 August 2019).
- Zuckerberg, M. (2017) 'Bringing the world closer together', *Facebook*, 22 June, available at www.facebook. com/zuck/posts/10154944663901634 (accessed 1 August 2019).