

Chapter from: *The World Information War: Western Resilience, Campaigning and Cognitive Effects*.

Edited by Timothy Clack, Robert Johnson. Routledge May 2021.

(Final draft subject to copy edits).

## **Algorithmic Pluralism: media regulation and system resilience in the age of information warfare**

*Damian Tambini*

Attention is online. After a century in which newspapers and broadcasting were the dominant media, the second decade of the 21<sup>st</sup> century saw a decisive migration of viewing and listening onto Internet-enabled devices such as smartphones, tablets and smart TVs.<sup>1</sup> As these new media gradually displaced the press and broadcasting, democratic communication became more open and decentralised, creating new possibilities for external interference with domestic public opinion. Hence the debates about fake news and disinformation.<sup>2</sup> Within military circles, doctrines of information warfare and reflexive control gained renewed significance.<sup>3</sup>

Mounting evidence<sup>4</sup> that new vulnerabilities to external manipulation are being exploited by hostile actors have led policymakers to call for new forms of control: many argue that defence from foreign disinformation and hate speech requires a more censorious regime for social media, for example through new laws to hold internet intermediaries responsible for misleading or hateful content.<sup>5</sup>

In this chapter I will examine the role of media regulation and governance in information warfare. I will look at the ways existing press, broadcasting and Internet regulation shape resilience to external info-war threats, and examine some proposals for reform of regulation. My focus is the new proposals for regulation in the UK and I argue that current proposals for tighter regulation risk falling into the trap of surrendering the core values and liberties that define democracy. The final section will outline a case for decentralised, competitive, plural media governance systems featuring ‘algorithmic pluralism’ – strength in diversity of independent media and citizen-led resilience rather than censorship, as the most effective defence against information war.

### **The New Paradigm: Info-War and Democracy**

Propaganda is not new. What is new is that data driven, social media tools have dramatically reduced its cost, and increased the speed and effectiveness with which information operations can reduce a democracy’s capacity to act. At the centre of the new information warfare are new capabilities to understand the needs, desires and aspirations of individual citizens, through analysis of online data traces, and use knowledge thus gained to undermine the autonomy of individual human decision-makers through targeting messages and control over the information environment. Official Russian doctrines of information warfare refer to ‘information viruses’ that can be planted in individual citizens minds through propaganda, and emotive and doctored video and images being used in targeted disinformation campaigns (Thomas 2015). Big data and artificial intelligence (AI) offer the potential to scale these propaganda effects to historical proportions, at a time when legacy “mainstream” media’s ability to counter the narratives of hate, division and mistrust is undermined by audience decline and lack of funding.

As an information-based exercise, info-war may seem victimless, but in terms of military realities of control and the national interest, its consequences can be immense: not only can domestic political actors potentially be persuaded to support policy that is the interests of foreign political actors, but the uncertainty, mistrust and confusion created by significant foreign intervention in communications processes can lead to an inability to form workable political consensus around any long-term strategy or action. Whereas in traditional warfare interference is assumed to follow “defeat”, foreign actors could become puppeteers of hollowed out democratic states without any such defeat. Successful political manipulation by information warfare could in theory create “zombie” states subject to external manipulation.

Information warfare<sup>6</sup> is often conflated with cyberwarfare, but the two are distinct. Cyberwarfare has the objective of disabling or control of infrastructure: transport systems, communication facilities, power grids. Information warfare seeks to alter the preferences and behaviour of human beings by altering the information environment in which they operate, with the ultimate objective of undermining a democracy’s capacity to make and legitimise collective decisions.

### **The World Information War is a War on Democracy**

Information warfare is not a weapon that can be deployed by any country, against any other country with similar results. It is a form of warfare that favours closed authoritarian states against open, liberal democracies. The info-war is an attack on liberal democracy itself. Leaders of authoritarian states such as Putin are vocal critics of Liberal civil society and deliberative democracy<sup>7</sup> and the current doctrine of Russian information war can be seen as a reassertion of information sovereignty as a response to ‘Western pro-democracy propaganda’ in Russia in the 1990s (Giles *et al.* 2018). Information warfare thus has a dual role: not only does it undermine the operational capacity of the adversary in conventional terms, but it also undermines domestic opposition and debate, by undermining civil society. Should authoritarian information warfare have the effect of triggering a clampdown by democracies towards more authoritarian, less liberal positions, this would have the additional benefit – from the autocrat’s point of view - of normalising authoritarian government and the suppression of free speech.

Russians will claim relativism, arguing that the US and its allies have long engaged in information warfare against a range of states. Whether or not this is true, the strategic asymmetry remains. Leaders of authoritarian states are threatened by their own citizens, by democratic ideals, and by alternative political elites. Regimes such as Putin’s seek to remove the democratic reproach and the threatening demonstration effect that liberal democracies provide to such opposition movements, through attacking the vulnerabilities that liberal democracies share and by extending control over domestic public opinion (see Rogov and Ananyev 2018). Leaders of authoritarian states seek to confuse and disorient their opponents through feeding and exploiting political turbulence (Giles *et al.* 2018). The confusion they are able to create through disinformation provides a salutary tale that can be utilised as they seek to communicate the penalties of liberty and cosmopolitanism as a means to sustaining the legitimacy of their own authoritarian rule. Information warfare is, par excellence, a challenge by *authoritarian* states to the vulnerabilities of *democratic* states. It is an attack on open society and liberalism per se.

The asymmetrical nature of information warfare has implications for information strategy. Organisations such as 77<sup>th</sup> Brigade (Miller 2018)<sup>8</sup> could develop an offensive capability to pursue the objective of creating confusion and mistrust and a ‘post truth’ environment in the Russian

electorate, but in a 'managed' democracy (Wolin 2008) such as Russia, the results of such efforts may be disappointing. Because citizens have weaker expression rights and less power in Russia, it is easier to contain and block such disinformation. Even if it is disseminated, it is unlikely to undermine the Russian state's capacity to effectively operate. The more democratic a country is, the more vulnerable it is to attack by opinion manipulation; and the more authoritarian a country is, the less vulnerable it is. By definition, authoritarian countries are better equipped to control the impact of hostile information manoeuvres, because the state controls the media, and free expression is not protected.

The simplest way to defend against information warfare is to block communication from abroad. This was the approach during World War II when foreign broadcasts were jammed. Domestic censorship operated alongside counter propaganda. This is also the approach of countries such as Russia and China post-1945, which have pursued a policy of excluding or controlling foreign media and managing foreign journalists, and in recent years have worked to exclude foreign Internet platforms through firewalls and supporting platforms such as Baidu, RusNet, Weibo and VKontakte. Indeed, the theory of Russian information warfare regarded these processes as a defensive response to what was viewed as Western aggression in the 1990s. The Russian claim was that the West sought to implement media freedom and undermine nationalist narratives in favour of a global doctrine that favoured Western objectives (see Thomas 2015, p. 17).

Contemporary information operations are difficult to detect and combat because they exploit the system features of social media. It is often challenging to separate effects of deliberate actions of 'bad actors' including foreign states and hostile actors, from effects of the business model of data-driven social media targeting (Larnier 2018, Zuboff 2019). Whereas the press (through the ethics and professional practices of journalism) and broadcasting (due to ethics and also licensing) tended to have at least a veneer of professional commitment to virtues such as 'truth' and 'the public interest' and 'news values' based on social importance, the algorithms driving social media are based on opaque advertising-driven calculations that prioritise not socially important content, but content that has been prioritised by others or that generates the most intense emotional resonance and therefore engagement (see for a detailed explanation of these effects Larnier 2018, Zuboff 2019).

Information warfare today exploits the operating model of commercial social media and the asymmetries between on the one hand democracies, which are based on popular sovereignty, open deliberation and free expression, and on the other, closed authoritarian societies, where interference with deliberation or voting is less effective. Let us now turn to how these systems work in practice and highlight the governance arrangements that determine the vulnerabilities of democracies to external manipulation. The next section illustrates how regulation and law impact the ability to control the spread of disinformation and propaganda and how this varies by medium.

### **Media Narratives of the Salisbury Poisonings**

On 4 March 2018, two people in Salisbury, UK, were exposed to a nerve agent and became seriously ill. In the subsequent months two more people became ill due to a second incident of exposure and one later died. These events, and subsequent news events including the appearance of suspects on Russian media, were the subject of widespread allegations of news manipulation, information operations and strategic disinformation coordinated by state and non-state actors (Ramsay and Robertshaw 2019).

The attacks themselves could be seen as a ‘media event’ enabling the Russian state to project power internationally and also to engage in complex strategic information campaigns abroad and at home. Even the official Russian Embassy account of the poisonings – which itself could be read as an attempt to foster mistrust and confusion - focused on UK ‘Media Policy’ and alleged that the UK media were misleading the public in their handling of the story, and were guilty of breaching international human rights and media freedom (Embassy of the Russian Federation to the United Kingdom 2019). The result of the debate, and the serious diplomatic repercussions that followed, was widespread mistrust of the official UK narrative, and of “mainstream media” interpretations, and, according to many reports, widespread and growing mistrust and confusion among the general public.

Attempts to undermine the official narrative of the UK government during the Salisbury poisoning event involved broadcasting, newspapers, and also blogs and social media, bots and human interventions, professional journalism, social media posts and both state and non-state actors. (Ramsay and Robertshaw 2019). It included the flow of news and information between each of these. The case illustrates the extent to which existing law and regulation shapes the resilience of different media to such forms of external strategic disinformation and how this varies across different media platforms.

UK newspapers generally reported the UK government position as well as others including those of Russia. Some newspapers attempted a degree of objectivity, but in line with usual practice they tended to choose an editorial position in defence of perceived UK interests. The newspapers reported the poisoning incident with their usual mix of wild speculation based on quotes from named and un-named individuals, as is reflected in the list of headlines in the official response of the Russian Embassy (Embassy of the Russian Federation to the United Kingdom 2019, Section VIII). They were later criticised for taking a significant number of their stories from Russian state media such as *RT* and *Sputnik* (Walker 2019).

Russian Newspapers by and large followed a similar pattern to the UK in the sense that they followed normal journalistic approaches to sourcing but fit this within a nationalistic populist narrative. They are arguably less influential domestically (Open Society Foundations 2011) but they did contribute to the sharing of what was found to be more than 40 basic narratives (Ramsay and Robertshaw 2019) on the story that were seen as a concerted campaign of disinformation.

Broadcasters presented a more balanced view in line with their legal obligations to maintain news impartiality. One of the most controversial aspects of this case was the reporting of the poisonings by English language broadcaster *Russia Today* and other Russian outlets between March and May 2018.<sup>9</sup> *Russia Today* is widely viewed as the propaganda arm of the Kremlin, but as a UK-based broadcaster licensed by the independent communications regulator Ofcom, the broadcaster is licensed under the Communications Act 2003 and is therefore subject to the Ofcom Broadcasting Code, in particular obligations to treat matters of political and industrial controversy with due impartiality. In connection with the series of reports about the poisonings, *Russia Today* had a number of complaints upheld against it that eventually resulted in a fine.

As is illustrated in the report of the Ofcom adjudication from November 2018 (Ofcom 2018), the regulator sought to demonstrate that it is not and should not be an arm of the state, and it should not bow to government pressure, particularly where this may lead to censorship. There is no prior approval of broadcasts or journalists by the regulator, or any other authority, which is why there was no attempt to interrupt the RT broadcasts when the complaints arose. The decisions of Ofcom are subject to judicial review under the jurisdiction of the European Court of Human Rights, and

therefore to Council of Europe standards under Article 10 of the European Convention on Human Rights which guarantees freedom of expression. When challenging sanctions imposed by Ofcom after complaints, the *Russia Today* lawyers cited the standards extensively in their defence (Ofcom 2018, p. 10) and Ofcom acknowledged them in its adjudication (Ofcom 2018, p.7). Ofcom upheld some but not all of the complaints of a lack of impartiality in reporting, finding that there was a notable lack of a UK perspective in the reporting.

The point of 'due impartiality' regulation in UK broadcasting is to limit the capacity of influential broadcasters to persuade and control by offering an imbalanced view. Governance arrangements for broadcasters have been carefully designed to protect the autonomy of the broadcaster in a system of checks and balances, and thereby to sustain trust in the reporting of the broadcaster. If there are obvious alternative views, broadcasters are obliged to present them: either in the programme as a whole or in a series of programmes. Anybody can complain (Ofcom 2019a, section five). The regulatory process is subject to standards of free expression, and, importantly, rules on the independence of regulatory authorities (European Audiovisual Observatory 2019, EU Council Directive 2018). The governance arrangements are based on the idea that regulation should take place according not to arbitrary fiat or the interests of the incumbent authority, but to rules agreed by Parliament according to accepted procedures and transparently available, interpreted by an independent authority such as a judge or specialist regulator.

Broadcasters in Russia operate within a contrasting environment where the state is not so constrained, despite the fact that the Russian Federation is a signatory to the convention, because ECtHR judgements and Council of Europe standards are often not adhered to, and because in any case impartiality (unlike broadcaster independence) is a matter for national regulation rather than international fundamental rights obligations (Open Society Foundations 2011), and because under the doctrine of information warfare, executive control of narratives is an aspect of the prosecution of the permanent war of information. In contrast with the exhaustive due process and caution with which Ofcom dealt with the complaint against RT, the Russian Ministry for Communication warned that "not a single British media outlet will work in our country if they shut down Russia Today" (DTG 2018). In August 2019 the Russian regulatory body was reported as threatening to "respond in kind" after RT was fined (Martin 2019).

Broadcasters are more directly susceptible to control and influence by government in Russia than in the UK, because the UK has deeper and more effective legally-enforced doctrines of freedom of expression (Open Society Foundations 2011). One channel that has had difficulties negotiating relationships with the Russian state is BBC Russia, and this serves as a useful contrast. The Russian language service of the UK public broadcaster was frequently jammed in Soviet countries during the Cold War. Following a resurgence of its audience in the 1990s the station was subject to sustained criticism over its partnerships with Russian state broadcasters at a time when BBC programmes had a growing influence in post-Soviet Russia. As the result of difficulties in establishing distribution the decision was made by BBC Russia to distribute only on the Internet from 2011. *Russia Today* benefits from the liberty of expression under the European Convention on Human Rights but the BBC has not the same protection in Russia.

There was evidence of widespread and coordinated internet-based Russian disinformation around the Salisbury attacks, according to reports of UK government sources as well as independent research (see for example Volpicelli and Bedningfield 2019). There was a widely reported spike in coordinated disinformation activity designed to create confusion and conflict, including for example faking a Twitter statement by the UK Defence Secretary that the attacks had been facilitated by the IRA. According to experts, such an approach followed a well-established Russian pattern and there

were numerous linguistic and other indicators that linked the posts to Russian state actors.<sup>10</sup> Social media bloggers, in particular, tended to draw ‘true but misleading’ material into a single one-sided pro-Kremlin narrative (Giles *et al.* 2018, p. 40). It is notoriously difficult to quantify the impact of these Russian internet campaigns of disinformation, and to develop an appropriate defensive response that does not compromise free expression. In the UK at least, the response has not been the removal of material on the basis of executive orders. Where traditional media are involved, the existing governance arrangements for newspapers and broadcasting have had an effect, but pure internet offerings exist largely outside of accountability mechanisms based on self-regulation or the law.<sup>11</sup>

Following the Salisbury events, experts debated how law and regulation should respond. Were the governance arrangements for broadcasters and the internet the weak points in info-war defences? There were calls for censorship and regulation of both the traditional media and social media, including demands for a new set of standards to apply to broadcasting content and fines for social media companies that fail to control disinformation.<sup>12</sup> The alternative view was that these were unnecessary and would constitute an unwelcome slide towards censorship: specifically, the restriction of ‘permissible’ views on broadcasting to a narrower ‘state sanctioned’ range of views. At the core of the debate was a concern with whether European human rights standards, and norms of broadcasting and Internet freedom were compatible with national security. The standards set out the basic ground rules for defending against malicious speech on the basis of a concern with national security.

### **Freedom of Expression, National Security: Fundamental Rights as a Framework for Media in Liberal Democracy**

Does the World Information War require suspension of freedom of expression? Under existing standards, it is already justified to restrict speech if national security requires it.

According to the founding document of the UN, the Universal Declaration of Human Rights: “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and *regardless of frontiers*.” Rights to freedom of expression are not absolute, and national security provides some justification for restrictions of freedom of expression, but the ‘regardless of frontiers’ standard creates difficulties when questions arise about foreign interference in democratic processes. Information operations can take the form of perfectly legal speech, even the selective amplification or suppression of true speech (Krasodonski-Jones *et al.* 2019), and as political speech, mis- or even dis-information<sup>13</sup> would be considered worthy of a high level of protection from state interference.

The European Convention on Human Rights provides a general framework for the balancing of the right to freedom of expression with justified restrictions of that freedom by reference to article 10.2 of the convention. In order to suspend freedom of expression as a defence from information warfare the justification would need to be found within this framework, or the framework would need to be suspended. In ECHR Art 10, it states:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

National security is thus one of the specifically mentioned legitimate justifications of restrictions on freedom of expression, and there is now developed case law in which the justification of various restrictions has been established, while a number of international standards and codes have been established which attempt to encapsulate what constitutes a justified restriction. For example, the Johannesburg principles (The Johannesburg Principles 1996) and the Tschwane Principles (The Tshwane Principles 2013) attempt to limit the scope for state restriction on the freedoms of information and expression which are based on mere diplomatic embarrassment, rather than genuine danger to life or limb which would result from publication of information.

The Johannesburg principles maintained that:

A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government. (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

National security justifications for restriction of speech within this regime are overwhelmingly therefore concerned with kinetic warfare: "information warfare" would not justify restrictions unless it met a demanding test of incitement to violence, which is rarely applied.<sup>14</sup>

Defending against speech that can be said to undermine national security or interfere in democratic processes is a subtle matter within this general regime of speech control: it is rather difficult to identify speech that constitutes a genuine national security threat by this standard. In terms of the law freedom of speech national security in other words, information war does not count as war.

Interference in democracy – even election meddling - would not constitute a national security threat by this standard and there is a high risk of 'collateral damage' –exerting a widespread chilling effect on speech that has genuine social value. For example, when the UK government proposed in 2019 a completely new framework to establish a higher degree of liability for social media platforms to reduce online harms, some responded by saying that they may not be able to continue to provide social network services due to the increased costs of moderation, thereby reducing the provision on free online spaces for debate and others argued that this constituted a disproportionate effect on expression.<sup>15</sup> Clearly there is something to be gained by improving trust in new media sources of information, but a censorious state led defensive stance risks compounding a lack of trust in "establishment" voices if it creates the impression that media are no longer separate from the state.

Whilst it is entirely possible that restrictions on free speech as a response to infowar may be justified as “necessary in a democratic society”, it would be difficult to construct a justification of censorship based on national security. Defensive censorship would sacrifice freedom of expression and thus surrender one of the basic tenets of democracy. Infowar does not involve a declaration of war, nor is there a clear distinction between a state of war and a state of peace. In conventional warfare, freedom of expression rights tend to be restricted ‘at a time of war’.<sup>16</sup> With no transition to a state of declared ‘information warfare’, suspending rights in order to defend against information operations risks becoming permanent.

#### **Fourth Estate as Front Line: Truth, Responsibility and Autonomy in Press and Broadcasting Regulation**

As the example of the Salisbury poisonings shows, perceptions of news events depend on diffusion of information over multiple platforms, broadcasting, newspaper, and also online. The development of the story, and the ability to challenge certain framings and viewpoints varies considerably according to the institutional and governance arrangements for each of those platforms. Due to their contrasting arrangements however, the press conduct robust experimentation for truth, whereas broadcasting regulation demands more sober verification. There have historically been comparatively high levels of trust in the overall system, though these have declined in recent years (see Edelman 2019, slide 46).

The role played by all media is based not on absolute freedom of expression, but on liberty within the law: a qualified and instrumental right to autonomy on condition of responsibility (Barendt 2005, Lichtenberg 1990). While broadcasters are licensed, press licensing was abolished by the end of the seventeenth century. An institutional framework has evolved according to which newspapers have enjoyed significant autonomy but have been subject to various forms of accountability and to the law. This framework of self-regulation, ethics and law, whilst maintaining media freedom, has been an important factor in the generation of resilience and trust. It is a key factor in UK defences against information warfare. Nevertheless, this framework faces unprecedented challenges in the contemporary period, so reform should seek to update and repair it.

With the emergence of universal suffrage and mass literacy, newspapers emerged as key source of power because of their ability to shape as well as reflect public opinion. A growing awareness of abuse of press power – and its role in democratic breakdown, notably in Europe in the mid twentieth century, led to the development of constitutional standards limiting press power but preserving the autonomy of newspapers from the state. In brief, liberal democratic media were permitted a wide degree of freedom and autonomy, so long as they pursued high professional standards in accuracy: the very quality that enable them to filter out a good deal of hostile disinformation, and provide a valuable ‘reality check’ for disinformation and hate. This has not been perfect – there is some hostility to “mainstream media” among a minority but surveys still show that people return to broadcasters and newspapers for confirmation when conflicting information is provided or at times of emergency.<sup>17</sup>

The public have a strong perception that media act ethically and do so voluntarily, although this has been tested by the failure of the press to comply with Parliament and implement the recommendations of the independent Judge led Leveson Inquiry into press ethics. There have been restrictions in place regarding who can own a broadcaster or a newspaper<sup>18</sup> and what they can do with it,<sup>19</sup> but newspaper publishers have enjoyed relative autonomy from the state during



peacetime. In the United Kingdom the key source of mistrust in public information is the capture of press interests by powerful industrial interests and of individual politicians by powerful press barons such as Rupert Murdoch.

The strong protection of institutional autonomy is a reaction to the endemic problems of capture, groupthink, and conflict of interest that tend to characterise the relationship between media and state institutions in liberal democratic media systems.<sup>20</sup> Within Council of Europe member states, newspapers should be free, but not in absolute terms: the corollaries of media freedom are media responsibility, pluralism, ownership limits and transparency, to prevent abuse of the media's power to shape public opinion, and a commitment to self-regulation of journalistic ethics.<sup>21</sup> If journalists or owners of newspapers are subject to illegitimate restrictions on their speech they can sue in the ECHR and appeal to the standards of the Council of Europe. Readers and listeners similarly can claim their right to receive ideas.

The United Kingdom approach to freedom of expression eschews prior censorship of any form. National security provides one exception to this in the form of DA notice committee which provides an informal interface between foreign office, Ministry of Defence and the leading media in order to prevent loss of life resulting from publication of news about security. Newspapers therefore enjoy considerable autonomy in the context of a general understanding that this must be enjoyed responsibly, or legislation will come into play (Tomlinson 2014).

The regulatory framework for the press includes the following key elements:

- Foreign and other ownership requirements. Foreign ownership is limited and transparency of ownership is required. National security could provide a legitimate reason to block a merger if it qualifies for referral to the Secretary of State for approval.<sup>22</sup>
- Content codes. Ethical codes are 'voluntarily' adopted by the press, often with informal or formal oversight of government. Codes provide sanctions for 'unethical' journalism including inaccuracy.<sup>23</sup>
- Pluralism guarantees. These limit the power and reach of any one media owner, through structural limits on market share and also viewpoint diversity rules.<sup>24</sup>
- Specific rules apply at time of elections such as blackout periods and transparency of advertising.

The extent to which newspapers, despite 'ethical self-regulation' are ideological, captured and subject to foreign influences is the subject of continuing debate (see for example Leyva 2019). Law and regulation have attempted to develop a complex set of legislative incentives that reinforce journalistic behaviours that encourage a truth seeking, deliberative role for the press. A strong presumption against prior censorship has applied, though this is suspended in relation to active operations through the DA notice system which operates as a 'voluntary' scheme.

As a centralised system with strict control of market entry, broadcasting as a system has a contrasting set of controls against potential foreign interference that contrast with those of the press. Not only are licensees subject to strict ownership controls and a specific 'fit and proper person' test applied by Ofcom, restrictions on content that can be broadcast, including requirements for political impartiality, and other licensing requirements restrict the potential for foreign interference.

In election periods in particular, the UK has maintained much stricter rules against foreign funding and also a strict ban on political advertising on television, impartiality rules and rationing of slots on public broadcasters. This has been justified<sup>25</sup> in terms of the need to maintain fairness and

legitimacy of electoral processes. These bans on political advertising have been subject to repeated challenge on freedom of expression grounds. In reaching a judgement in the lower courts Auld LJ noted that the ban on political advertising was justified because “the United Kingdom Parliament has chosen to introduce a prohibition on political advertising confined to the broadcast media because of its perceived greater power than that of other media and, consequently, greater potential for distortion by wealthy interests of the democratic process.”<sup>26</sup>

To summarise, in the era prior to the internet, the UK media system as a whole has been based on principles of autonomy, trust and liberty within the law. Public trust in information has been underpinned by an understanding that media institutions are separate from the state. This principle has been supplemented by rules to ensure that media are not captured by hostile forces and that media autonomy and liberty are not exploited. It is a widely acknowledged that the removal of media autonomy would result eventually in a tipping point: it is impossible to predict at which point trust fails irrevocably, but as members of the public become aware of effective state control of media they would cease to trust media narratives and truth claims.

UK press and broadcasting are not subject to state control or elite capture as are media in Russia and China. But this does not mean that they escape accountability, or that free speech is absolute: they are accountable to professional self-regulation and to their users, and subject to many regulatory limits on the exercise of their considerable power. Propaganda of both domestic and foreign origin has been a constant concern shaping the development of these governance rules in all post-war European media systems. The use of mass media systems to dominate individual citizens, to the extent that they are deprived of autonomy in decision-making processes was seen as a key factor that led to the European dictatorships of the mid twentieth century, and frameworks were introduced to avoid the possibility of this recurring (see for discussion Craufurd Smith and Tambini 2012).

Regulation of media content and ownership, within a broader framework of freedom of expression and media plurality have formed the bedrock of a system of media that is inherently resilient to propagandist uses. For example, the occupying powers in Germany in the period 1945 to 1950 established a decentralised, federalised broadcasting system in order to ensure that it was this some susceptible to monopolisation and information control. This in turn was checked by a developing commercial sector and the model of the ‘mixed broadcasting system’ was born (Humphreys 1994). In the US, commercialisation was seen as a means to guard against propaganda, and the Hutchins Commission proposed a new framework for press responsibility and accountability (Pickard 2015). Common to both North American and European approaches is the development of the principle of media diversity or pluralism: this is the notion that media systems must maintain diversity of media types or owners, viewpoints, cultures and other dimensions.<sup>27</sup> In 2018, a Recommendation of the Council of Europe described media pluralism as the corollary of freedom of expression.<sup>28</sup> Since World War II, governments of all stripes in the UK have considered media plurality to be crucial to democracy. In 2011, the UK Secretary of State said “I think the media industry is different because of the special influence that it has on our national culture, on our identity and on the way that we view ourselves. So, I think it is incredibly important that we have a structure that makes sure that in a vibrant, open democracy - such as we are proud to have - no one person or organisation has undue control of our media” (Hunt 2011).

During the 20<sup>th</sup> century, newspapers and broadcasting have been regulated by laws and codes that reflect the dangers of propaganda, but also permit autonomy within a relatively wide legal scope. Ownership controls and ethics for the press and stricter liability for the more influential broadcasters. These frameworks have not been applied to social media.

## Social Media Regulation and the New Information Warfare: Surrender?

In the wake of widespread evidence of information operations against the United Kingdom, particularly after the Salisbury poisonings, there is a growing awareness that social media lack the institutionalised protections for truth seeking and democratic deliberation that have evolved for the press and broadcasting. This has led to calls for new ways of enforcing the “responsabilization” of social media.<sup>29</sup> In 2019, the UK government published a proposal for legislation on ‘Online Harms’ which set out a new regulatory framework for, among other things, regulation of disinformation (Gov UK 2019, p. 31). Other countries such as France and Germany have made proposals for comparable legislation. From an information warfare perspective, one key question is whether such frameworks would contribute to an enhanced defensive capability in information warfare. As will be evident by now, I argue that an approach based on decentralised, bottom-up, trust-based resilience as the basis for defensive capabilities in information warfare is superior to authoritarian restrictions.

Policy proposals have focused on effectiveness of removals of speech that is illegal or breaches the community guidelines of social media services, reducing and constraining anonymity of use, and introducing a range of sanctions for hateful and misleading content in particular<sup>30</sup>. Policy responses have taken the form of the following main approaches:

- Specific new laws to incentivise social media companies to moderate and potentially to remove ‘harmful’ social media posts, by making them liable for fines and other sanctions if they fail to do so.
- Introduction of specific new offences such as electoral manipulation (e.g. in France).
- Encouraging the development of new Ethical Codes and Community Guidelines alter the acceptable standard of speech on social media services. Self-regulatory codes of conduct in particular to deal with problems such as disinformation
- Information provision: websites such as EU vs Disinfo<sup>31</sup> which ‘call out’ disinformation and hostile information campaigns
- Flagging, labelling and warnings, including collaboration with fact checkers to enable social media to flag suspect content.
- Transparency of political advertising and funding, including revision of electoral laws to promote transparency and more enforceable spending and advertising restrictions.

Calls for tighter restriction of freedom of expression on the basis of defensive interests against foreign actors have been relatively muted, and contained, but they are growing. After widespread allegations of foreign interference, for example by the so-called “Russian Troll Farm” (the Internet Research Agency of Saint Petersburg, known as IRA), a growing number of European states have published proposals for laws introducing new regulatory frameworks for social media (Wardle and Derakhshan 2017, DCMS 2019).

One problem for policy is that information operations do not necessarily involve breaching self-regulatory or legal standards of hate speech, or knowingly disseminating information that is inaccurate or misleading (Krasodonski-Jones *et al.* 2019). Therefore improvements to enforcement or raising standards in relation to hate, terrorism, or secrecy would be unlikely to have a beneficial impact.

Democratic countries have not been able to impose the restrictive means imposed by authoritarian states, in part because they are subject to, and actively support, the standards of free expression. The UN special rapporteur for freedom of expression has actively warned against establishing new

laws that infringe free expression and could be the first step to censorship (Kaye 2019). But a great many policy proposals are under discussion (Wardle and Derakhshan 2017, see also European Commission 2018). The question is whether they undermine the established model of democratic media autonomy that has provided robust defence against disinformation.

Social media has yet to achieve a mature governance settlement. In the light of recent allegations of various forms of foreign interference and information warfare, France, for example, passed a new law on electoral manipulation in December 2018, and outlined a framework for social media regulation in June 2019. Germany passed a new law setting out enhanced obligations on social media platforms to remove illegal hate speech content in 2018. The UK government published a framework for social media regulation in 2019 and proposes to legislate in 2020 (UK Gov, Online Harms 2019).

These legislative proposals have been criticised for predictable reasons, namely the fear of unnecessary restrictions. There is always a danger that creating a single, more regulated social network will, on the one hand, legitimise a similar approach in other countries, and, secondly, that it will reduce overall system resilience in the face of sustained information attacks.

### **Conclusions: Pluralism and Media System Resilience**

Under sustained attack by “the three wars”<sup>32</sup>, reflexive control (Giles *et al.* 2018), and a range of other information warfare techniques<sup>33</sup>, the superficially rational response is to respond in kind by developing similar information warfare capabilities: to assert control over domestic information and media to defend against foreign intrusion, and engage in offensive operations of retaliation through similar forms of disinformation.

Both strategies are problematic. Whilst introduction of censorship controls as a form of information defence may on the surface be an attractive proposition, such an approach is likely to be ineffective as well as unacceptable. A degree of wartime censorship may be acceptable in a democracy, but it is not a valid strategy during an information war. Information war is not ‘declared’ but is a permanent condition (see Robert Johnson and Timothy Clack (2020), Introduction), therefore simply suspending free expression indefinitely would equate to surrender. Without media independence, and freedom of expression, liberal democracy would cease to exist and the Infowar would thereby be lost.

Being drawn into a full-scale information war by upscaling offensive infowar operations from the Western powers would be short-sighted and naïve about the deeper roots of legitimacy and trust, because information wars are asymmetric. If they are drawn onto this battlefield, democracies will always be at a disadvantage. In the short-term censorship may present an illusion of improved protection. In the long term it would undermine trust and resilience because in mature democracies, enduring trust is generated by media institutions that operate autonomously from the state, thus providing genuinely independent forms of verification.

Offensive information operations will have a limited ability to undermine the agency of authoritarian states. Not only because such societies are characterised by more effective control over domestic opinion and the internet, but because the key decisions – such as foreign policy changes, trade and industrial policy, are made by an unaccountable clique with little or no regard for processes of deliberation or civil society input, and without regard to the unpredictable tides of online opinion and memes. Democracies need a new and smarter approach, and they need to trust and extend their established institutions for trust building and deliberation.

Rather than following the Russian model of domestic information control, democracies should deploy smart policy responses, supporting an ethics of information based on truth, trust and the public interest. Trust in narratives and reporting of institutions such as the BBC and the World Service are based on a form of trusted independent journalism that has developed over a century, and a concern with reporting the truth, independently of government and other actors.

Democratic governments should not only protect the ability of the legacy institutions of such twentieth century media. They should support gatekeepers in new media and treat them as media (see Council of Europe 2011). Mainstream media, to a degree, are being displaced as audiences move online. New gatekeepers such as social media are developing new forms of independent verification independently from the state. These processes should be encouraged by a long-term media policy that works with multiple stakeholders to develop institutions of news ethics genuinely independent from the state, and consumer awareness and digital literacy that fosters new forms of 'due trust' in the media.

Democratic governments can also act to supporting a competitive media ecology based not on reflexive control, behavioural biases and information cascades (Sunstein 2017) but on digital literacy, algorithmic pluralism and enhanced consumer information. Ultimately it is the scepticism of citizens that is the best defence against disinformation. Algorithmic pluralism: - maintaining a variety of social platforms and limiting the market power of each one -is another source of resilience. Informed consumers capable of switching between them on the basis of a wider range of information on service quality will be another source of resilience and is one that can be fostered by active regulatory agencies such as Ofcom.

These institutions will develop quickly in a situation of genuine competition and choice for consumers and enhanced consumer information. Doctrines of national security should be re-examined but existing freedom of expression standards should be respected rather than compromised. It may be necessary to introduce some new regulatory approaches, to update transparency and ethical regulation, and introduce new offences such as electoral manipulation. But these offences should be very narrow and specific and regulatory discretion must be conducted transparently, and independently, preferably by judges. In any new regulatory settlement, it is imperative that no attempt is made to create any form of 'truth commission'. Democracies should establish the long-term goal of developing new online institutions to manage external threats and structure the deliberative search for truth and consensus, independently from the state, just as they did with the press and broadcasting. This will provide resistance to foreign attacks within the framework of freedom of expression that has been established over centuries. Trust and resilience to disinformation is best fostered in a media system based on an ethics of truth and the public interest, in a framework that is genuinely independent of the state and is in no way viewed as a system of censorship. Policy coordination should have an autonomous, self-regulating media system as its ultimate objective. On the surface this may appear to be chaotic. But it will in fact be more resilient to foreign interference.

Ultimately an approach that updates existing traditions of free and independent media, and seeks deliberately to apply them to new media, and one that is characterised by algorithmic pluralism, rather than enhanced central control, will guard against the virality of malign messages.

## Bibliography

- Article 19, 2019. *Online harms: Duty of care would restrict free speech in the UK* [online]. Available from: <https://www.article19.org/resources/online-harms-duty-of-care-would-restrict-free-speech-in-the-uk/> [Accessed 23 February 2020]
- Baldwin, R. and Black, J., 2008. Really Responsive Regulation. *The modern law review*, 71 (1), 59–94.
- Barendt, 2005. *Freedom of Speech*. Oxford, Oxford University Press.
- Bradshaw, S., Neudert, L.-M. and Howard, P.N., 2018. *Government Responses to Malicious Use of Social Media* [online]. Riga: NATO Stratcom COE. Available from: <https://www.stratcomcoe.org/government-responses-malicious-use-social-media> [Accessed 23 February 2020]
- Chafee, Z. Jr., 1919. Freedom of Speech in War Time. *Harvard Law Review*, 32 (8), 932–973.
- Craufurd Smith, R. and Tambini, D., 2012. Measuring Media Plurality in the United Kingdom: Policy Choices and Regulatory Challenges. *Journal of Media Law*, 4 (1), 35–63.
- Craufurd Smith, R., Tambini, D. and Morisi, D., 2012. Regulating Media Plurality and Media Power in the 21st Century [online]. In: S.B. Micova and D. Tambini, eds. *Media Policy Brief 7*, June 2012 London. London: LSE Media Policy Project, 1–24. Available from: <http://www.lse.ac.uk/media@lse/documents/MPP/Policy-Brief-7-Media-Pluralism.pdf> [Accessed 23 February 2020]
- DCMS [Digital, Culture, Media and Sport Committee], 2019. Eighth Report of The House of Commons on Disinformation and ‘fake news’: Final Report HC 1791 17/19 (2017–19).
- DTG, 2018. *Ofcom to review Russia Today (RT) Channel* [online]. Available from: <https://dtg.org.uk/ofcom-to-review-russia-today-rt-channel/> [Accessed 23 February 2020]
- European Commission, 2018. *A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation* [online]. Luxembourg: Publications Office of the European Union. Available from: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> [Accessed 23 February 2020]
- European Council Directive 2018/1808 of 14 November 2018, amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [online]. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN> [Accessed 23 February 2020]
- European Audiovisual Observatory, 2019. *The independence of media regulatory authorities in Europe* [online]. Strasbourg: European Audiovisual Observatory. Available from: <https://rm.coe.int/the-independence-of-media-regulatory-authorities-in-europe/168097e504> [Accessed 23 February 2020]
- Edelman, 2019. *2019 Edelman Trust Barometer Global Report* [online]. Available from: <https://www.edelman.co.uk/research/2019-trust-barometer> [Accessed 23 February 2020]

- Embassy of the Russian Federation to the United Kingdom, 2019. *Salisbury: Unanswered Questions* [online]. Embassy of the Russian Federation to the United Kingdom. Available from: <https://rusemb.org.uk/fnapr/6762> [Accessed 23 February 2020]
- Giles, K., Seaboyer, A. and Sherr, J., 2018. Russian Reflexive Control [online]. Kingston: Defence Research and Development Canada, DRDC-RDDC-2018-C182. Available from: <http://www.conflictstudies.org.uk/publications.php> [Accessed 23 February 2020]
- Gov France, 2019. Créer un cadre français de responsabilisation des réseaux sociaux: agir en France avec une ambition européenne [online], *Rapport de la mission* [mission report] May 2019. Available from: <https://www.numerique.gouv.fr/uploads/rapport-mission-regulation-reseaux-sociaux.pdf> [Accessed 23 February 2020]
- Gov UK, 2019. Online Harms White Paper [online], *White Paper* April 2019. Available from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/793360/Online\\_Harms\\_White\\_Paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf) [Accessed 23 February 2020]
- Hallin, D. and Mancini, R., 2004. *Comparing Media Systems: Three Models of Media and Politics*. Cambridge: Cambridge University Press.
- Humphreys, P.J., 1994. *Media and Media Policy in Germany since 1945*. Oxford: Berg.
- Hunt, J., 2011. Speech to the Royal Television Society [online]. 14 September, Royal Television Society, London. Available from: <https://www.gov.uk/government/speeches/royal-television-society> [Accessed 23 February 2020]
- Impress. Standards Code. <https://www.impress.press/standards/> [Accessed 23 February 2020]
- IPSO. Editors Code. <https://www.ipso.co.uk/editors-code-of-practice/> [Accessed 23 February 2020]
- Krasodonski-Jones, A., Smith, J. and Jones, E., 2019. *Warring Songs: Information Operations in the Digital Age* [online]. London: Demos. Available from: <https://demos.co.uk/wp-content/uploads/2019/05/Warring-Songs-final-1.pdf> [Accessed 23 February 2020]
- Lanier, J., 2019. *Ten Arguments For Deleting Your Social Media Accounts Right Now*. London: Vintage.
- Leyva, R., 2019. 'Real news' may be doing more harm than 'fake news' [online]. Inform's Blog. Available from: <https://inform.org/2019/07/24/real-news-may-be-doing-more-harm-than-fake-news-rodolfo-leyva/#more-42809> [Accessed 23 February 2020]
- Leveson Inquiry, 2012. Report of the Leveson Inquiry. London, HMSO.
- Lichtenberg, 1990. *Democracy and the Mass Media*. Cambridge Studies in Philosophy and Public Policy Cambridge University Press, Cambridge, UK.
- Martin, A.J., 2019. *Russia to retaliate against UK media after RT fined for biased coverage of Skripal attack* [online]. Sky News, 1 August. Available from: <https://news.sky.com/story/russia-to-retaliate-against-uk-media-after-rt-fined-for-biased-coverage-of-skripal-attack-11774935> [Accessed 23 February 2020]

- Miller, C., 2018. *Inside the British Army's secret information warfare machine* [online]. *The Wired*, 14 November. Available from: <https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military> [Accessed 23 February 2020]
- Moore, M. (2018). *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*. London: Oneworld.
- Moore, M. and Tambini, D., eds., 2018. *Digital Dominance. The Power of Google, Amazon, Facebook and Apple*. New York, NY: Oxford University Press.
- Newman, N., Fletcher, R., Kalogeropoulos, A. and Nielsen, R.K., 2019. *Reuters Institute Digital News Report 2019* [online]. Oxford: Reuters Institute. Available from: <https://reutersinstitute.politics.ox.ac.uk/our-research/digital-news-report-2019> [Accessed 23 February 2020]
- NetzDG, n.d. Network Enforcement Act (Netzdurchsetzungsgesetz, NetzDG) [online]. Available from: <https://germanlawarchive.iuscomp.org/?p=1245> [Accessed 23 February 2020]
- NUJ code Code of Conduct of the National Union of Journalists. Available From <https://www.nuj.org.uk/about/nuj-code/> [Accessed 26 February 2020]
- Ofcom, 2004. *Consultation on Ofcom guidance for the public interest test for media mergers* [online]. London: Ofcom. Available from: [https://www.ofcom.org.uk/data/assets/pdf\\_file/0025/37186/pitest.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0025/37186/pitest.pdf) [Accessed 23 February 2020]
- Ofcom, 2018. *Ofcom Broadcast and On Demand Bulletin, Issue 369* [online]. London: Ofcom. Available from: [https://www.ofcom.org.uk/data/assets/pdf\\_file/0020/131159/Issue-369-Broadcast-and-On-Demand-Bulletin.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0020/131159/Issue-369-Broadcast-and-On-Demand-Bulletin.pdf) [Accessed 23 February 2020]
- Ofcom, 2019a. *The Ofcom Broadcasting Code (with the Cross-promotion Code and the On Demand Programme Service Rules)* [online]. London: Ofcom. Available from: <https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code>
- Ofcom, 2019b. *Communications Market Report 2019* [online]. London: Ofcom. Available from: <https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr-2019> [Accessed 23 February 2020]
- Open Society Foundations, 2011. *Mapping Digital Media: Russia* [online]. London: Open Society Foundations. Available from: <https://www.opensocietyfoundations.org/publications/mapping-digital-media-russia> [Accessed 23 February 2020]
- Ramsay, G. and Robertshaw, S., 2019. *Weaponising news RT, Sputnik and targeted disinformation* [online]. London: Policy Institute, King's College London. Available from: <https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf> [Accessed 23 February 2020]
- Robertson, Geoffrey and Nicol, Andrew. (2008). 5<sup>th</sup> Ed. *Media Law*. London: Penguin.
- Rogov, K. and Ananyev, M., 2018. Public Opinion and Russian Politics. In: D. Treisman, ed. *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Washington, DC: Brookings Institution, 191–216.



- Sunstein, C., 2017. *#Republic: Divided Democracy in the Age of Social Media*. Princeton, NJ: Princeton University Press.
- The Johannesburg Principles, 1996. *The Johannesburg Principles on National Security, Freedom of Expression and Access to information* [online]. London: Article 19. Available from: <https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf> [Accessed 23 February 2020]
- The Tshwane Principles, 2013. *The Global Principles on National Security and the Right to Information (The Tshwane Principles)* [online]. New York, NY: Open Society Justice Initiative. Available from: <https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles> [Accessed 23 February 2020]
- Thomas, T., 2015. Psycho Viruses and Reflexive Control: Russian Theories of Information-Psychological War [online]. In: *Information at War: From China's Three Warfares to NATO's Narratives*, September 2015 London. London: Legatum Institute, 16–21. Available from: <http://www.lse.ac.uk/iga/assets/documents/arena/archives/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf> [Accessed 23 February 2020]
- Tomlinson, H., 2014. The New UK Model of Press Regulation [online]. In: S.B. Micova and D. Tambini, eds. *Media Policy Brief 12*, March 2014 London. London: LSE Media Policy Project, 1–24. Available from: <http://www.lse.ac.uk/media@lse/documents/MPP/LSE-MPP-Policy-Brief-12-The-New-UK-Model-of-Press-Regulation.pdf> [Accessed 23 February 2020]
- Volpicelli, G. and Bedningfield, W., 2019. *A huge new Russian propaganda effort is attacking much more than Facebook* [online]. *The Wired*, 23 June. Available from: <https://www.wired.co.uk/article/russia-facebook-atlantic-council-disinformation> [Accessed 23 February 2020]
- Walker, J., 2019. Academics condemn UK tabloids for sourcing articles from Kremlin-backed RT and Sputnik [online]. *Press Gazette*. 5 March. Available from: <https://www.pressgazette.co.uk/academics-condemn-uk-tabloids-for-sourcing-articles-from-kremlin-backed-rt-and-sputnik/> [Accessed 23 February 2020]
- Wardle, C. and Derakhshan, H., 2017. *Information Disorder: Toward an interdisciplinary framework for research and policy making* [online], Council of Europe report DGI(2017)09, Strasbourg, 31 October. Available from: <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c> [Accessed 23 February 2020]
- Wolin, S.S., 2008. *Democracy Incorporated: Managed Democracy and the Spectre of Inverted Totalitarianism*. Princeton, NJ: Princeton University Press.
- Zuboff, S., 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

---

<sup>1</sup> These developments are non-controversial, but see Ofcom (2019b), Newman *et al.* (2019).

<sup>2</sup> The UK Parliament Select Committee Report on fake news was published in 2019. The European Union issued a high-level group report and subsequently a Communication on disinformation in 2018 (European Commission 2018). The Council of Europe published a report by Claire Wardle and Hossein Derakhshan on Information Disorder in 2017.

<sup>3</sup> Information Warfare is not new. In 1995, the Rand Corporation outlined what it saw as the key features of Information Warfare, which are highly relevant today. What has changed is the vulnerability of democratic

---

systems to destabilisation and interference. See:

[https://www.rand.org/pubs/monograph\\_reports/MR661/index2.html](https://www.rand.org/pubs/monograph_reports/MR661/index2.html)

<sup>4</sup> See for example the research of the Computational Propaganda Unit:

<https://comprop.oii.ox.ac.uk/publications/>

<sup>5</sup> In 2018, a new hate speech law came into force (the NetzDG) which aimed to ensure that illegal hate speech was taken down more quickly by social media. The UK government set out its legislative proposals for an even more radical and far reaching regulatory framework in the White Paper on Online Harms in 2019.

<sup>6</sup> The new doctrines of information warfare have been seen to have arisen in both China and Russia since the 1990s, and have also been referred to as China's 'Three Warfares' and Russia's 'reflexive control'. See for a discussion Thomas (2015).

<sup>7</sup> See Thomas (2015) for a description of the development of Russian approaches to social media propaganda. See also Giles *et al.* (2018).

<sup>8</sup> Under the banner 'influence and outreach', the British Army website lists the public the activities of 77<sup>th</sup> Brigade: audience, actor and adversary analysis; information activity and outreach; counter-adversarial information activity; disseminating media; monitoring and evaluating the information environment; and training on human security etc. The Army 'Integrated Action' model is also referenced.

<sup>9</sup> A large scale content analysis of the reporting by RT/ Sputnik has been carried out by Ramsey and Robertshaw (2019).

<sup>10</sup> For a review of the evidence of Russian disinformation campaigns more generally and in the US, see:

<https://medium.com/dfrlab/russian-interference-the-evidence-fe6e52e50dcd>

<sup>11</sup> There has been a deep and longstanding debate about these rules, for example in the context of the EC High Level Group on Disinformation, the Code of Practice on Disinformation and elsewhere, the AVMS code on self-regulation and the E-Commerce Directive.

<sup>12</sup> In 2019 the UK Government published the Online Harms White Paper which set out a new proposed framework for regulation of social media, including a new framework to encourage social media to take down misinformation and fine them if they fail to do so.

<sup>13</sup> Misinformation is unwitting or careless inaccuracy, disinformation is deliberate (Wardle and Derakhshan 2017).

<sup>14</sup> Subsequent to the Rwandan genocides a radio station (Radio Mille Collines) was found guilty of incitement to genocide. This was the first case of its type since the Nuremberg trials. See *The Prosecutor v. Nahimana et al.* International Criminal Tribunal for Rwanda . <https://www.justiceinitiative.org/litigation/prosecutor-v-nahimana-et-al>

<sup>15</sup> Article 19 Strongly Opposes a Duty of Care (Article 19 2019).

<sup>16</sup> Even in the US, which generally enjoys higher levels of speech protection, this is suspended at a time of war. See *Schenk vs US*: <https://constitutioncenter.org/blog/schenck-v-united-states-defining-the-limits-of-free-speech/>. See also Chafee (1919).

<sup>17</sup> The Edelman Trust Barometer conducts an annual survey into trust in the media. It is striking that the rather high levels of trust in traditional media (such as the BBC) and low levels of trust with social media were more or less stable between 2012 and 2019.

<sup>18</sup> One area where national security considerations are written into the institutional framework is in terms of a framework of controls on foreign media ownership. Whilst it is the case that these have been to an extent relaxed in recent years, enabling for example American citizens to own UK media assets, many other countries have retained these rules, a development which for example required Rupert Murdoch to take US citizenship in order to purchase newspapers and broadcasting interests there.

<sup>19</sup> Such as those provided by official secrets act and the self-regulatory standards of the DA Notice Committee (see Robertson *et al.* 2008).

<sup>20</sup> See for example Hallin and Mancini (2004). These issues were discussed at length in the report of the Leveson Inquiry (2012).

<sup>21</sup> Under the Enterprise Act 2002 (Section 58) there is an additional special procedure for ministerial approval of media mergers, which may be refused if they are deemed to operate against the public interest in a free, accurate and plural media.

<sup>22</sup> See Communications Act Schedule 14. Enterprise Act 2002 Section 58.

<sup>23</sup> See Impress; IPSO; NUJ codes.

<sup>24</sup> Enterprise Act 2002; Ofcom (2004).

<sup>25</sup> See the judgement in *Animal Defenders International vs UK* (ECtHR 2006) for a lengthy discussion of the links between electoral regulation and broadcasting.

---

<sup>26</sup> See for example *Animal Defenders International vs the United Kingdom* (ECtHR 2006).

<sup>27</sup> See for a discussion of the notion of media pluralism Craufurd Smith *et al.* (2012).

<sup>28</sup> Recommendation CM/Rec/2018(1) of the Committee of Ministers to member States on media pluralism and transparency of media ownership.

<sup>29</sup> The title of a recent French Government report on the problem was “Créer un cadre français de responsabilisation des réseaux sociaux” (Gov France 2019).

<sup>30</sup> Numerous attempts have been made to gather policy responses around the world. See Bradshaw *et al.* (2018).

<sup>31</sup> The EU vs Disinfo project is an EU funded project to monitor and call out disinformation.

<https://euvsdisinfo.eu/about/>

<sup>32</sup> The Chinese Notion of The Three Wars refers to information, media and legal attempts to undermine sovereignty and agency of the adversary. See:

<https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/>

<sup>33</sup> See Moore (2018).