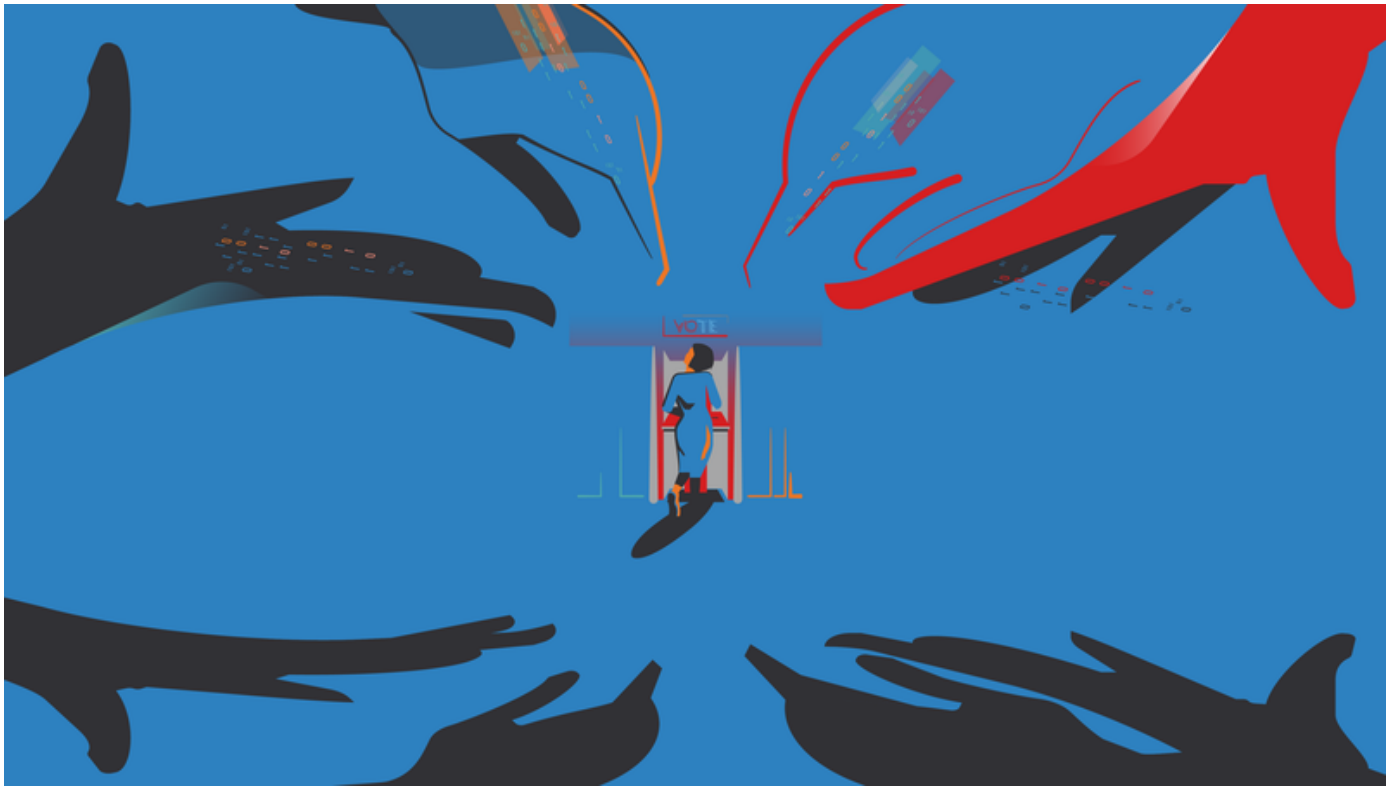
Curbing digital election interference in the Age of Disinformation:

Embellishing the robustness and independence of electoral systems in modern liberal democracies



Marcus Marritt for NPR (Ewing, 2019)

Master Thesis

Supervisor: Jens Olav Dahlgaard, Copenhagen Business School (DK)

No. of pages: 120 / Characters (incl. spaces): 236,551

15th May 2020

André Oliver Daab – 124553

Petros Katakis Anastasakos - 125153

Copenhagen Business School | MSc International Business and Politics

[Page intentionally left blank]

Acknowledgements

Firstly, we would like to thank our families from whom we have always received profound support and encouragement throughout our academic and professional careers. Without their genuine care and loving appreciation, the passion and dedication that fostered this research would have not been possible. Secondly, our friends, colleagues, and professors for nurturing a drive that allows our work to be inspired, devoted, and impactful.

This thesis would not have been possible without the thorough commitment of our supervisor Jens Olav Dahlgaard, who took the time beyond all distances to assist us through this final academic journey of our masters under the most extraordinary of circumstances. We are grateful for the deep sense of integrity and work ethics he installed within us.

Let this project also be a manifest of a shared passion for the politics of this world, the intrinsic networks governing our societies, but first and foremost the mutual respect and awe we foster for each other as academic partners and as friends. The genuine bond reflected in our cooperation is deeply valued and shall continue to be a building block of reciprocate support and companionship for our future post CBS.

On an individual note, Andy would also like to thank his boyfriend Vincent McLeese for the strong believe he has exercised in him and his abilities, always making him understand that he can achieve and be the best version of himself.

Pledge of Academic Honesty

I hereby declare that this piece of written work is the result of my own independent scholarly work, and that in all cases material from the work of others (in books, articles, essays, dissertations, and on the internet) is acknowledged, and quotations and paraphrases are clearly indicated. No material other than that listed has been used. This written work has not previously been used as examination material at this or any other university. This written work has not yet been published.

André O. Daab, Amsterdam 14th May 2020

Petros Katakis Anastasakos, Copenhagen 14th May 2020

Abstract

Recent incidents of alleged election interference and large-scale disinformation campaigns in the West (i.e. 2016 US presidential elections, Cambridge Analytica scandal) have caused heightened awareness and interest in the topic of electoral interference (EI) and social media manipulation (SMM). Due to the very current and ongoing nature of EI in the digital age, and more so the age of disinformation, research and reporting focuses predominantly on producing nouvelle and timely content often with the consequence of overlapping and redundant coverage. Very few of these investigations are academic, and many of the academic studies existing only aim at contributing new data. There is a severely limited effort of using the vast existing data to draw fundamental analyses, building the basis for a better understanding of election interference. This is the research gap addressed in this project.

This thesis asks: employing secondary data analysis, can a concrete set of policy recommendations be produced to set a benchmark for modern liberal democracies (MLDs) to counter election interference and prevent uncoordinated national efforts? The thesis builds a holistic and comprehensive literature review setting an interdisciplinary foundation synthesising vocabulary, analysis, and intellectual paradigms around election interference, social media manipulation, and disinformation. The literature introduces applicable concepts relating to theories of electoral ethics, privacy, and data management and protection to elucidate the challenges and process that substantiate policy design and research in an attempt to further the analysis of this report. Using a varied qualitative method approach this thesis combines multiple qualitative methods in a Nested Analysis (NA), synthesising the strengths of two methods with one broad and one narrow focus of data. Binding the existing literature, we operationalise secondary data analysis, a method founded on the belief that necessary data to answer new research questions can be found in already existing data.

The hypothesis that existing data in literature on election interference holds the necessary answers to build a set of applicable policy recommendation is tested throughout five chapters exploring 1) intent recognition behind election interference, 2) electoral infrastructures, 3) online advertising by foreign governments and nationals, 4) foreign media organisations, and 5) international norm setting. Following a quality-controlled structure supported by the NA, the chapters review timely reporting and popular academic work around the topics at hand to build recommendations that are validated against three expert publication, namely Stanford's Cyber Policy Center Report on securing American elections in 2020, and two NATO reports exploring government and industry responses respectively.

Promoting pluralist public dialogue and mitigating polarisation by fostering literacy brings a unique and dynamic approach to this study aiming to contribute a valuable element in election interference studies, by not only being easily replicable but expandable as a source of secondary data for related studies.

Keywords: Election Interference, Public Policy, Social Media Manipulation, Disinformation

Table of Content

Introduction

The Age of Disinformation

The Covid-19 pandemic beginning in 2019 and ongoing at the time of this paper, not only froze much of the global economy and involuntary closed the borders of a world that had seemed inseparably set on globalised traffic, it also held democratic processes in many parts of the world (Verhofstadt, 2020). With analogue elections effectively impossible, campaigning and ballot casting have to be conducted in often entirely unexplored physical and digital spaces that bring a range of challenges to an already fragile electoral ecosystem (Synovitz, 2020). Preceding the pandemic had been a gradual rise in new populism in the West, alerting democracies to the most severe vulnerabilities it faced since the end of WWII just 75 years ago (De Cleen, 2017).

It was the 2015-2016 presidential campaign of Donald Trump that popularised the term 'Disinformation Age' (Coppins, 2020). Disinformation strategies are not new and authoritarian regimes have practised them for many decades preceding the rise of new populism (Waller et al., 2009). However, the practice in Western MLDs and more so their susceptibility to those strategies was virtually unheard of prior to the 2016 Brexit referendum and 2016 U.S. presidential elections (Babington, 2019). The victories of large-scale sophisticated disinformation and social media manipulation campaigns in the context of these two electoral examples, gave momentum to a global wing of far-right populists that, particularly in the West, were quick to replicate disinformation strategies (Baldini, 2017). The 2018 Cambridge Analytica scandal demonstrated how in the face of the harvesting and exploitation of more that 87 million Facebook user profiles, neither public policy makers nor private business leaders had the adequate literacy, mandate, or capacity to respond effectively to these threats within the vacuums of their authority (Kang & Frenkel, 2018). Data assets have become the most valuable capital for companies to hold, and the vast majority of them are amassed by

but a few corporations such as Facebook, Twitter, and YouTube (Crilley & Gillespie, 2018). In the clear absence of a coordinated response across nations, as well as among national private and public sectors, this research sets out to see whether *employing secondary data analysis, can produce a concrete set of policy recommendations to set a benchmark for modern liberal democracies to counter election interference and prevent uncoordinated national efforts?*

The traditional assumption that domestic election fraud is largely committed by manipulating analogue election infrastructure (Alvarez et al. 2009) has been significantly disturbed by the Cambridge Analytica scandal which proved that there is notably more exposure and disruption capacity in the digital space, more so, these domestic disruption can often have sources abroad (Badwy et al., 2019). In fact, the vast majority of digital election interference is instigated by foreign actors seeking to disrupt or interfere in electoral processes (Bessie, 2017). Russia, which will take a prominent role in the analysis of this research, has been identified to be executing one of the most sophisticated and comprehensive disinformation and election interference campaigns world-wide with a particular target in the US and the UK (McFaul & Kass, 2019). But it is not just Russia that has gained a prominent position in the publications on modern election interference, China too exerts considerable interest in exploiting the current power vacuum of a withdrawing and increasingly inward-looking USA (Zeng & Spark, 2019). In fact, this study identifies that much of the current fraction around election interference is caused by geopolitical tension.

Because of the ongoing developments and findings, as well as the rapid velocity of information traffic with regards to the electoral ecosystems of the twenty-first century, academic ambition has been largely with creating new data and being at the forefront of election interference studies. The sheer volume of literature and data produced are seldom connected and often repeated. This study sets itself apart by

observing the existing data to build a benchmark of policy recommendations that can be replicated and expanded upon. Deciphering the vast network of election interference studies is crucial in synthesising the necessary bases to build literacy and gain the ability to respond to this modern challenge. The delineated problem articulated in the research question is the absence of a coordinated (inter)national response on part of policy makers who in particularly struggle to comprehensively address the issue of election interference due to 1) lacking digital literacy, 2) a consequent expertise gap, causing 3) shortcomings in recruitment of the expertise required, as well as 4) a stagnating ability to grasp the dispersed and rapidly developing information stream around election interference (Skierka, 2014). This thesis consequently adapts and applies relevant theories of established academic fields and research around election interference, electoral studies, and SSM, which it compliments by choosing relevant methods of a varied qualitive approach that is justified by the qualitative data utilised in this research. The analysis section of this paper will combine secondary data analysis (SDA) and validation by means of expert publications to demonstrate a critical understanding of methodological and theoretical choices presented in the foundational sections of this study. It is paramount that throughout the comprehensive and extensive study, logical coherence between the research question, analysis, and conclusion is ensured by weaving sections into each other and having them substantiate the progress of this paper. The conclusion will demonstrate a considerable addition to the current research gap and present a holistic set of recommendations, that will be debated also in context of potential further research in the discussion. Overall, this research is an elemental building block to the discussion around election interference and policy setting that has been seemingly been missing until now.

Research Question

The research question was designed to integrate the most principal elements of this project, and is consequently crafted as follows:

Employing Secondary Data Analysis, can a concrete set of policy recommendations be produced to set a benchmark for modern liberal democracies to counter election interference and prevent uncoordinated national efforts?

This research question consists of three fundamental components: 1) the urgency for this study, and 2) the aim of this study to produce applicable policy recommendations, and 3) a brief mention of the methodology by touching upon the existing data as the foundation of this study. The introduction briefly lay the foundation for the research gap, but it will be further elucidated throughout each section of this paper, in particular during the analysis which dedicates great attention to the current context of the content. The following theory section will build a comprehensive vocabulary and establish an academic grammar to equip both the reader and future the researchers with the intellectual language required for in-depth analysis of election interference and social media manipulation. The methodology section is built around the data observed and will in great detail guide the reader of this study through the process of answering the research question. Finally, this paper will return to the research question as it presents its findings and offers a discussion for further research.

Hypothesis

Our hypothesis is that *by employing secondary data analysis we can produce a replicable method to build regulatory policy recommendations that can be validated against*

expert publications. We will expand the academic field buy using the largely dispersed, rapidly developing research and reporting on election interference in MLDs to prove that when bound together they build a commonly applicable base of policy design and research. By doing so we achieve a new sense of cross-national response capacity previously absent from individual national and academic efforts to combat social media manipulation and election interference by preventing exclusive and uncoordinated efforts not in line with global efforts.

Literature

This literature review identifies, outlines, and evaluates how scholars, researchers, and journalists have investigated and theorised about the relationship between election interference and robust democratic processes. The aim is to sketch the current state of knowledge on the subject, identify gaps in the literature, and justify the chosen scope of this research project.

State of Knowledge

In an era defined by Big Data, post-truth, and post-trust an increasing amount of people follow digital pathways to news (Mitchell et al., 2016). Cross-country studies on news sources, show that in Western MLDs such as the US, the UK, France, Sweden, and Germany, the modern news consumer (aged 18 to 49) has settled for online sources as their primary information wellspring (ibid). The Pew Research Centre (2015) shows that 61% of millennials use Facebook as their primary source for news on political issues. Whether it be news websites or social media platforms, these web spaces are more susceptible to the spread of false information than traditional printing press (Kovic et al., 2018). At its core stands an identity gap wherein social media platforms operate as cooperate entities and do not perceive themselves as members of

the online press leading to apathy when requested to comply with journalistic ethics (El Bermawy, 2016).

This reality has shaped the socio-political phenomenon branded as 'post-truth'. According to the Oxford dictionary, the post-truth era is characterised by "circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal beliefs" (Oxford Dictionaries, 2016). A consequential trend is the receding occurrence of evidence-based political decision-making at the individual level and the dominance of personal, psychological and demonstrative factors in shaping voting choices, behaviour, and policy preferences (Davies, 2019). The associated relevance of 'filter bubbles' and 'eco-chambers' further reinforces the inoculation of the individual from reason-based political decision-making and favours a polarisation of the public sphere. According to fundamental political philosophy, Habermas (1995) and Rawls (1996) argue that when involvement in political reasoning and policy debate deviates from factual argumentation and moves towards emotions or convictions, consensus building becomes far less attainable. Coupled with the rise of populist politics and rhetoric, these developments create challenges for the preservation of a healthy democratic fibre in Western MLDs (Jones, 2019).

The most obvious link between the post-truth era and election interference is the access to information - where and how people get their information directly influences the object of their political choices. This 'susceptibility' of certain demographic groups to be swayed towards a particular political decision by emotional 'engineering' or 'steering' has created new opportunities for foreign, domestic, state and non-state actors to promote their particular economic and political interest in ways, which raise legal and moral challenges for the manner in which modern democratic processes are carried out (Flynn, 2017; Tarran, 2018). Incumbent governments, electoral candidates,

campaign managers, advisors, and consultants are very much aware of this alteration in the channels of news circulation and deliverance. Using state-of-the-art technological tools, made available by novel information infrastructure systems, these actors directly or indirectly, shape the flow of information to further their interests with, sometimes, ambiguous legitimacy (Shorey & Howard, 2016; Cadwalladr & Harrison, 2018; ICO, 2018: Bradshaw et al., 2018). In this sense, the landscape of electoral races and legislative debate has also been affected by the shift in news sourcing, which blurs the line between campaigning and influencing vs. propaganda and manipulation.

Political campaigns in MLDs currently run on data-focused systems for voter outreach and categorisation (ICO, 2018; Bradshaw et al., 2018). According to Freedom House, digital platforms are the new battleground for democracy (Shahbaz & Funk, 2019). The emergence of 'Big Data' has enabled the use of accumulated, detailed personal profiles, for micro-targeting based on a user's internet traffic (collated personal data) and sophisticated psychological profiling (Shorey & Howard, 2016; Jones, 2019). This has given rise to a number of digital propaganda techniques for political persuasion on matters of political importance, from deploying a digital army of political disinformation bots to digital astroturfing and political (digital) redlining (ibid; Kovic et al., 2018).

However, to this day, no scientific evidence exists to establish a direct causal correlation between digital propaganda, disinformation, and individual political choices and voting behaviour (Bayer et al., 2019). Ensuing policy recommendations, regulatory initiatives, and governmental responses have arisen as a result of posteriori attempts to assess the impact of such campaigns on real-world elections and referendums (ibid). In one of the biggest studies on the issue today, Freedom House assessed 30 countries that held elections or referendums during 2016-2019 and

reported an alarming number of 1.6 billion internet users being exposed to election interference, by domestic actors alone (Shahbaz & Funk, 2019). Following the US 2016 presidential election, the UK Brexit referendum and the scandal of Cambridge Analytica, "the manipulation of public opinion through social media, during critical moments of political life, has emerged as a pressing policy concern" (Bradshaw et al.,2018: 4). Before breaking down the different components of this phenomenon and its implications for healthy and resilient democratic processes, the next section will attempt to clarify the definitional dimension of election interference and set a clear typology of the concept.

Defining Election Interference (EI)

In understanding EI and defining a clear set of actions, techniques and tactics framing its conceptual definition, it is paramount to distinguish it from: 1) ordinary electoral campaigning and 2) electoral fraud. With regards to campaigning, there is a clear differentiation between campaigning aims and those of EI. EI aims at disrupting the democratic transfer of power by denigrating individual candidates or political parties, sowing polarisation and division and thus ultimately undermining faith and trust in democracy (Shahbaz & Funk, 2019). Campaigning simply promotes a specific individual or legislative path as the most suitable political outcome, reinforcing the democratic ideal of representation and civic participation (Barton et al., 2014). This distinction alludes to the motives behind these two different concepts and by extension to the difference between misinformation and disinformation. When a fact is twisted to serve a specific political end, i.e. when misinformation is spread, no direct harm is meant towards the public interest (Bayer et al., 2019). While disinformation concerns the intentional reporting of falsehoods as facts in order to directly undermine the institutional foundations of democratic processes (ibid). Hence, a definitional

characteristic of EI stems from the use of disinformation to persuade the public of a specific political outcome while simultaneously corroding democratic capital. Campaigning on the other hand relies mainly on misinformation to gain political capital.

Furthermore, available literature suggests that EI is distinct from election fraud as the latter relies predominantly on analogue methods to either discredit or artificially recast the outcome of an election or referendum (Alvarez et al., 2009). In contrast, the kind of EI investigated in this paper focuses on digital and online strategies to influence an electoral result, namely: 1) digital propaganda and 2) political hacking (Berghel, 2017). The former will be taken to refer to the spread of disinformation and deep fakes and the use of political bots. These two techniques are put together under the umbrella term 'Social Media Manipulation' (SMM), which will be defined in the next section. Political hacking refers to cyberattacks and information warfare through data and e-mail leaks with the purpose of inducing the paralysis of democratic systems by putting pressure and creating paranoia both among the public but also among decision-makers (Mansfield-Devine, 2018). Even though scholars such as Alvarez et al. (2009), Berghel (2017), and Taylor (2019) have argued that, in contrast to election fraud, EI is primarily international, we maintain that the source of digital electoral intervention can and has been found to be domestic as well. In light of recent experiences around the world, the origin of EI cannot be limited to that of foreign actors (Shahbaz & Funk, 2019). Conclusively, for this project's purposes, digital EI is defined as the online disinformation and propaganda campaigns (i.e. via social media) aimed at deceiving the public, illegitimately interfering and undermining democratic processes, involving violations of fundamental human and civil rights in the manipulation of public opinion, leading towards sub-optimal political outcomes and potentially causing public harm (Bayer et al.,2019; European Commission, 2019).

Before investigating the literature and vocabulary of EI further, it is important to stress the importance of the source of disinformation in defining EI. Sources of digital propaganda campaigns specifically can be both state and non-state actors as well as have domestic or foreign origins. In Table 1 the types of disinformation and propaganda campaigns found in the literature are summarised and their impact on democratic processes and values accordingly assessed.

Table 2: Types of disinformation and propaganda with their assessed impact on democratic values, rule of law and fundamental rights

Disinformation and propaganda	Targeted at domestic population	Targeted at foreign population
A. Source is a non-state actor, e.g. political party, or unidentified person	A1. Unethical political campaign, misleads society; if the political party is successful in the elections B1 may follow	A2. Citizens' actions, as well as disguised or unattributed attacks: similar to election hacking by 'patriotic citizens'; states may be responsible under international law for the aggressive actions of non-state actors acting on their territory against another state
B. Source is a state (governmental) actor	B1. Governmental political propaganda; clear transgression of democratic values, rule of law and human rights; captured state tries to strangle democracy; within the EU, a cause for the Article 7 mechanism	B2. Information warfare, interference with sovereignty; global threat against democracy – threatens geopolitical stability

Note: Yellow (A1) = harmful; orange (A2 and B1) = very harmful; red (B2) = critical threat.

Source: Authors.

Table 1. Types of disinformation matrix, taken from (Bayer et al., 2019)

This classification helps to set the scope for further exploration by providing the following suppositions: 1) EI is most harmful for democracies when it is carried out by state actors, 2) domestically-driven EI carried out by state actors can be equally as harming for democratic processes as that of non-state actors targeted at a foreign population but when non-state actors are behind EI, it is much harder to identify them and attribute responsibility, and 3) digital propaganda targeted at domestic population by non-state actors like political parties is overtly misleading and considered unethical political campaigning but only moderately threatening to democratic robustness. This last point helps formulate one further distinction between

EI and political campaigning, that is, for the former to be the case, the source of the propaganda must be a state actor. This means that whether the disinformation is forwarded by an incumbent party, i.e. a governmental actor or a running candidate, is determinate in defining an act as illegitimate interference in electoral processes.

At this point it should be noted that EI is not a twenty-first century phenomenon, especially in its foreign-driven variant. In fact, Levin (2016) finds that between 1946 and 2010, the US and the former USSR intervened in 117 elections around the globe. Following his findings, Tomz and Weeks (2019) present three different versions of foreign EI: "1) Endorsements occur when foreign countries express their opinions about candidates; 2) Threats combine an endorsement with a promise of future reward or threat of future punishment, such as threatening to downgrade future relations if the preferred candidate loses; 3) Operations when foreign powers undertake efforts such as spreading embarrassing information about a candidate, hacking into voting systems, or donating money to an election campaign" (ibid: 9-10). They claim that operations have proven to be the most corrosive type of foreign EI for democracies (ibid). Following this assumption, in our definition of EI, the scope is narrowed to 'operations', as SMM includes both defamation and political hacking. This scope is justified by the analytical focus of our project, that is, the assumed adverse impact of EI on public accord, faith in democracy, and trust in democratic institutions.

To recap, this section served to explore literature on the meaning of election interference and delimits the definitional scope of the use of the term in this research project. Firstly, the section separated EI from political campaigning in terms of its sources (state vs. non-state actor), aims (electoral win vs. corrosion of democratic capital), and means (misinformation vs disinformation). Secondly, the section distinguished EI from electoral fraud based on the offline and the illegal nature of the latter. Thirdly, the differences between domestic and foreign EI were explored and it

was concluded that despite the latter posing greater threats to Western MLDs, the potential challenges posed by the former should not be downplayed. In the following section, the specifics of SMM are laid out and academic findings on its function and effect on liberal democratic functions and values assessed. This serves to identify the information technologies and infrastructure as well automation tools that can be used to undermine free and fair democratic processes.

Social Media Manipulation (SMM)

Terminology

In the context of social media, manipulation is defined as "serving of an ad or message to a viewer of paid and organic manipulative content" (Aral & Eckles, 2019). Examples of manipulative content include the amplification or repression of political content, hate speech, fake or junk news, and disinformation (Ma, 2020). The next section will explain the manner in which SMM takes place without engaging into too excessive technical jargon.

For the purpose of this paper and under the aforementioned definitional context, SMM will be employed to refer to the use of (social) political bots, sockpuppets, trolls, astroturfing and political redlining (Wooley & Howard, 2016). Political bots are defined as "the algorithms that operate over social media, written to learn from and mimic real people so as to manipulate public opinion across a diverse range of social media and device networks" over nodal political moments in a society's trajectory (ibid). A 'sockpuppet' is a jargon term for fake profiles or identities used to "interact with ordinary users on social networks" (ibid). When sockpuppets are politically motivated and used by government proxies, electoral candidates or interrelated actors to influence a citizen's voting choices and behaviour, they are called, 'trolls' (ibid). These automated scripts, or social bots, generate content on social

media platforms such as Twitter, Facebook, or YouTube and interact with consumers, through the use of algorithms and automation (ibid). In context of major public policy issues, elections, and political crises, these bots are termed political (ibid).

Political astroturfing refers to the deceptive practice of presenting a political target, such as an electoral victory or a preferred policy outcome, as being supported by the public. Astroturfing fabricates the illusion of grassroot origins and widespread public support. Political redlining concerns the inequities and divisions caused by the use of data and analytics categorising Internet users and identifying particularly vulnerable populations (i.e. with specific personality traits or tendencies) to which tailored messages and ads are especially attractive and more effective in nudging them towards a particular political decision or choice.

Traditional Media Propaganda vs. Social Media Manipulation

So, digital or computational propaganda refers to the use of automated and manipulated social media accounts to spread disinformation across the public sphere. Yet how does this differ from traditional forms of propaganda and attempts to manipulate public opinion? To answer this question first consider how in contrast with traditional media and the printed press, social media relies on 'user-generated content', meaning end-users or the general public publishes outside of editorial or ethical scrutiny (Bertot et al., 2012). This translates into added uncertainty and ambiguity with regards to the accuracy and validity of the information provided (ibid).

Still, the fact remains that 'fake news' (as coined by the Donald Trump campaign during the 2016 presidential elections; Wendling, 2018) is not something new in a world where, even in liberal democracies constitutionally supporting the impartiality of the press, bias and partisan media are more or less a reality. The issue start meriting

more scholar and legal attention, due to the level to which disinformation can be channelled and the extent to which it can be pulled. As academic literature suggests, SMM is far cheaper, less transparent and detectable, and has a greater scope and reach that is potentially much more effective due to its reliance on Big Data than traditional forms of propaganda (Kovic et al., 2018; Jones, 2019; Wooley & Howard, 2016). The obscurity that characterises the use of these political bots, which does not allow to immediately identify allegiance to specific political actors or ends (Bastos & Mercea, 2017), also raises new obstacles in maintaining political processes in line with the principles of transparency and accountability. So, the nature of cyberspace and digital techniques used in computational propaganda far exceed the accountability, transparency, accuracy, and credibility deficiencies of traditional forms of propaganda. From traceability issues to amplified outreach, its adverse impact on the quality of public dialogue and consequent voting behaviours, is arguably quite differentiated from that of older version of propagandistic techniques.

The Role of Social Media Platforms in Data-driven Political Campaigning

The next paragraphs show why a user's movement on the internet, from reading news on reputable sites to visiting disinformation blogs, is among the most valuable data points in their political and social profile. They also serve to show how unrestricted and vast access to citizens' personal information has drawn into question the adequacy of legislative measures around the issue (Martínez et al., 2007). All platform providers and online content producers follow a data asset driven profitability incentive in tracking users, building profiles and ultimately selling access to that data to interested parties (such as political campaign managers and political commutation experts) (Moore, 2018: 136-165).

Facebook is the first platform that came into the spotlight as a facilitator for large scale and sophisticated electoral campaign employment. In 2008, Barack Obama's campaign reached out to voters on social media through a Facebook app that collected supporters' contact details, spurred interaction between party members and voters, and helped the Democratic party raise money for the campaign (Tett, 2020). In 2012, this escalated when the same team discovered a loophole in Facebook's system which allowed access to the so-called 'social graph of users' (ibid). This meant that by acquiring one user's data, the team could access data on their contacts too.

This is how the first psychological profiling, or psychographic, targeting tools were developed. Say a voter completed a Facebook survey, they provide data about their demographic background, interests, political affiliations, and policy preferences, not only for themselves, but also for their social network (ibid). This data can then be used to send personalised political messages- to accurately reach sets of people on individual basis, infiltrating their social news and applying peer pressure (Moore, 2018: 128). The privacy implications raised by psychographic targeting without users being aware or giving consent for the use of the private data are quite straightforward.

By the 2016 election US presidential elections, psychological profiling had developed into new, much larger dimensions, which for some far exceeded the ethical boundaries of personalisation and persuasion tricks of political campaigning (Tarran, 2018). As mentioned in the introduction, the Trump campaign created psychological profiles on almost 90 million voters which were used to forward manipulative, targeted propaganda (Tett, 2020). As it later became known, during this campaign, the personal data of 50 million Americans had been harvested and inappropriately shared with Cambridge Analytica (Wong, 2018). The political consultancy used personal information taken from Facebook without authorisation to construct a profiling system for US voters which would allow targeted and personalised political

advertising (Cadwalladr & Harrison, 2018). The scandal that broke out stemmed from exactly the same loophole in Facebook's policies that enabled third-party app developers to extract personal data of users and their 'social graph' without them being aware or giving consent (Wong, 2018). According to the official election result reports approximately 140 million Americans voted in 2016 (U.S. Federal Election Commission, 2016), a number that places considerable importance on the impact of this type of SMM.

To this day, there is no law in the US that renders disinformation campaigns illegal as long as they are not funded by 'foreign money' (Uchil, 2019). Candidates, parties or political groups can launch such campaigns either in-house or through subcontracting as not even the use of fake 'political bots' and/or troll accounts is legally treated as a protected form of political speech (ibid). A major obstacle to overseeing this practice stems from the fact that it is very difficult to ensure that the multiple sources from which individual information is retrieved, are legitimate and in line with legal requirements (such as collected with a stated purpose; not disclosed without consent; available to the individual for reviewing and many more) (ICO, 2018). More on this

Disinformation & Deepfakes

How is Disinformation Defined?

Disinformation is defined as "verifiably false or misleading information that is created, presented and disseminated […] to deceive the public" and "does not include inadvertent errors, satire and parody, or clearly identified partisan news and commentary" (European Commission, 2019: 1). To be considered disinformation, the reporting of false facts has to be consistent and specifically targeted. In their extensive study across all EU Member states, Bayer et al. (2019) list four elements for defining

computational propaganda campaigns. These include information which: "i) is by design partly or completely false, manipulated or misleading, and entails unethical persuasion techniques [such as the SMM methods described earlier]; ii) concerns an issue of public interest; iii) intends to breed insecurity, hostility or polarization and/or attempts to cause disruption in democratic processes; iv) is disseminated and/or amplified through automated and aggressive techniques, such as social bots, AI, paid human trolls, and micro-targeting" (ibid: 9). Under this definition, agents of disinformation are not restricted to non-state or foreign actors. Aggressive, opaque and targeted digital political campaigning and influence or persuasion tactics can be regarded as propagandistic and manipulative, as long as the false content that is published belongs to an intended strategy with a political effect on a topic of high public interest (ibid). This definition of EI was developed based on Russia's interference in several elections of European member states and is purposed to fit the study's aim of assessing the impact of the rule of law in the EU and its members. However, its applicability can be taken to transcend the study's scope and aim, and thus also fit the case of domestically driven computational propaganda.

How is Disinformation spread?

Ever since social media became the most common sphere of collective interaction, their importance as means of spreading disinformation has risen exponentially (European Commission, 2019). The process by which disinformation is spread through these platforms starts with the identification of specific users, which this disinformation is meant to affect (i.e. sway towards a specific target) the most. These users are identified by third party apps and or Application Programming Interfaces (APIs) that gain unauthorised access to their private data through social media platforms (Facebook, Twitter, Google etc.) (Taylor, 2019). In order for

disinformation to be convincing and thus effective it must have at least a minimum factual basis or reflect a widely accepted belief, fit with prevailing narratives in the target population, accommodate common prejudices, and nurture innate suspicions (Moore, 2018: 80). Access to 'Big Data' allows for malicious actors to identify 'fake news' meeting these criteria and the end-users susceptible to consuming them and thus enables the delivery of disinformation content where it will be more fertile in cultivating the preferred electoral result or policy outcome. The most common techniques of disinformation diffusion which this study focuses on include deepfakes (video manipulation), falsification of official documents, information theft and leakage, troll attacks and the use of bots (European Commission, 2019).

This points to another fundamental difference between media and social media relevant to the exacerbation of 'tribalism' and the political correctness and pluralism of the news. Traditional media are found in literature to have a de facto more conservative approach to reporting than the news content found in social media platforms. Some scholars attribute this to their commercial marketing orientation, which compels them to at least appear moderate, and cautious, while more or less obeying conventional norms and not openly offending any particular important group. Although they do at the same time, highlight and exaggerate events involving deviant behaviour since that attracts the audience's attention (Neumann, 2016: 209-242). This kind of bipolarity is absent in social media, which has a different relationship with the formation of public opinion. Relying on user-generated content, implies that platform providers have little legal responsibility for the actual news content that they host, and much less reason to consider individual sensibilities. Nonetheless, this enable s minorities which would otherwise be suffocated by dominant discourse to speak out and express themselves. However, besides providing extremist elements and divisive discourse such as hate speech more

platforms, it creates a persistent demand for a new kind of news, one of a more sensationalist, ephemeral and shallow nature (Moore, 2018).

The discussion over the last five years around the real and perceived threats of disinformation for democratic institutions and processes have risen to global prominence and are subject to heated scholarly debate. In the following section, we attempt to investigate the features of the academic landscape vis-a-vis the relationship between democracy and disinformation.

Democracy in the Era of Disinformation

This section investigates theoretical literature around the impact of disinformation on democratic capital. It is important to clarify the meaning of the term 'Modern Liberal Democracy' (MLD) and the kind of political regime addressed in this project. We stress the word 'liberal' because it effectuates a core distinction from just a simply 'electoral democracy' (Schedler, 2002). In the latter, the 'electoral minimum' suffices as a condition for modern democracy (ibid). In contrast, in a liberal democracy, certain fundamental dimensions of democratic constitutionalism need to be institutionalised, such as "the rule of law, political accountability, bureaucratic integrity and public deliberation (ibid). Our central hypothesis is that EI, to a lesser or greater extent, challenges these fundamental pillars. Hence, in order to devise measures to safeguard them and in turn, modern liberal democratic values and processes, we first have to formulate an outline of the tensions caused by advancements and the ensuing threats of contemporary information technologies and infrastructure as well as automation.

The Democratic Ideal, Human Rights and SMM

Basic democratic theory found in the works of liberal thinkers such as Roald Dahl underlines the importance of the 'democratic ideal'. This requires that the whole of the citizenry faces 'unimpaired opportunities' in 'formulating' political preferences, in 'signifying' them to one another and in being ensured that they are 'weighted equally' in public decision making (Dahl, 1971: 2). Along similar lines, Andreas Schedler (2002) shows how modern liberal democracies rest upon the normative premises of democratic choice depicted in Table 2 (Appendix). On the right side of the table, the most common strategies of violating these norms can be found. With regard to EI, it seems like dimension 2-4 are most relevant, but given the specific focus of our project, number 3 is most applicable. To explain, if the ideal of democratic choice requires that "citizens must be able to learn about alternatives through access to alternative sources of information", then SMM and disinformation campaigns directly undermines this capacity (Schedler, 2002: 39).

The normative premise of democratic choice found in the requirement that is demanded freely presupposes that voter preferences are formulated without interference, or at least, under the same amount of it. Consider the following statement: "citizens who vote on the basis of induced preferences are no less constrained than those who must choose from a manipulated set of alternatives" (ibid: 40). This means that for modern democracies to function properly all citizens, notwithstanding educational or social status differences, are assumed to possess equal faculties of autonomous decision making (ibid). It can then be argued that micro-targeting, psychological profiling, and other means of altering the availability of information on presented choices that create discrepancies between the level of autonomy each citizen enjoys in forming voting preferences and making a political decision, directly violate the democratic ideal of free demand (ibid).

In short, a citizen susceptible to SMM, consuming fake news and voting according to them is more constrained in making a political decision than one that does not. This implies a corrosion of democratic capital both because of: 1) the low level of awareness amongst the public with regard to the manner data analytics works and their private data collected, shared used; and 2) the information asymmetry between different groups of voters when it comes to verifying and reacting to manipulative content (ICO, 2018: 47).

A similar way of framing this issue can be found in obtaining a human rights-based approach. Under this, EI impacts privacy, human dignity and autonomy as well as violates the right of freedom of expression and the right to seek and receive information (Bayer et al., 2019). With regard to privacy and data protection, the violation refers to the previously discussed non-consensual use and/or misappropriation of private data afforded by platform providers, mined, analysed and brokered by political consulting firms or other types of strategic communication enterprises, for political campaigning purposes during electoral races (ICO, 2018). Protecting and promoting the right to freedom of opinion and expression, requires that when it concerns common matters, the formation of political preferences, and ultimately voting choice, interferences of a manipulative nature (such as strategic controlling and targeted altering of the content of information) are absent. This is just an alternative way to frame the 'free demand of democratic choice' concept, which however allows connection to legal protected rights, and not normative imperatives.

Last but not least, when individuals are not provided with full and clear information about the use of their personal information by political parties, and their rights regarding data privacy, both the rule of law and the principle of political accountability are undermined (ICO, 2018). "The lack of fair processing information and due diligence in relation to personal information obtained from data brokers"

(ibid: 30) raises compliance issues with data protection law, decreases transparency of political campaigning and voter targeting practices and thus undermines trust and confidence in democratic processes.

SMM and Voting Choice

As previously mentioned, the majority of academic research has focused on foreign EI (European Commission, 2019; Wooley & Howard, 2016). However, recent experiences around the globe, have given rise to a novel strand of literature which explores the overall use and impact of algorithms, automation and big data on democratic states regardless of the origin of the disinformation campaign (Shorey & Howard, 2016). These studies attempted to answer research questions such as 'To what extent democratic elections vulnerable to social media manipulation?', 'What is the relationship between social media manipulation and democracy?', "How does foreign EI affect domestic perceptions of and trust in democratic institutions"? (Anderson et al., 2005; Bessi & Ferrara, 2016; Badawy et al., 2018; Conover et al., 2011; Ferrara, 2017).

Neither has the lack of empirical evidence on the relationship between SMM and election outcomes thwarted the conduct of numerous qualitative studies assessing the impact of disinformation campaigns on democratic processes. Several political organisations, such as the UK and the European Parliaments, have commissioned investigations into the potential threats that the illegal, unlawful and/or deceitful exploitation of personal data (available via social media platforms) for political gain poses for the undisrupted function of democratic states (Harriss & Raymer, 2017; Bayer et al,2019; European Commission, 2019; OSCE, 2015).

Findings present an ambiguous situation. Social media are argued to play an instrumental role in promoting reason-based deliberation, argumentative diversity, generally reinforcing public participation in policy debates and strengthening the democratisation of public discourse on key political issues (Badawy et al., 2018). On the other hand, the negative effects of abusing of social media platforms on democratic functions have also been empirically identified. Manipulating public opinion through uncontrolled, opaque and abusive digital propaganda and disinformation tools, has been connected to increased polarisation of political conversation, loss of trust and confidence in fundamental democratic institutions such as the electoral process, suppression of voter turnout/civic participation and ultimately delegitimization of the political system causing the erosion of democratic capital and social instability (Norris, 2014; Tucker, 2007; Wellman, Hyde & Hall, 2018; Bradshaw et al., 2018; ICO, 2018). In other words, empirical evidence on social media manipulation's isolated impact on elections is scarce and fractured (Paquet-Clouston, Bilodeau & Décary-Hétu, 2017). The sensitive nature of the issue, involving conflict of interests between public and corporate policy, practical trade-offs between security and privacy as well as normative questions like where to draw the line between campaigning and manipulation or influence and propaganda, raises additional hurdles for furthering coordinated efforts towards studying this phenomenon.

Building upon this premise, Aral and Eckels (2019) provide a methodology framework for measuring SMM of elections and establishing a precise causal inference between the latter and political opinions/behaviour. This methodology entails 4 procedural steps; first, cataloguing data on exposures to manipulative content; second combining the latter with data on voting behaviour; third, assessing the actual effect of manipulative message on opinions and behaviour; and finally, calculating the

cumulative impact of voting behaviour changes on election outcomes (ibid: 859). The limitations of this methodological approach are rather obvious and hard to overcome.

First of all, data access both for voting behaviour from government bureaus and personal data from the social media platforms faces major public policy and political constraints. Then there is the difficulty of isolating the impact of SMM from other factors affecting changes in voting behaviour or choices. At the same time, in order to assess the overall impact of SMM, data from all social media platforms in which it takes place should be combined. This seems a highly difficult task both because of data restrictions but also due to the different forms that SMM assumes across different digital platforms. For instance, aggregating the impact of social bots deployed Facebook with those operating on Tweeter entails several technical obstacles that require extreme statistical and computational expertise to be overcome (Lever, 2019).

Relating to this, consider Badawy et al (2018) that attempted to measure the impact of Russian trolls on the 2016 US Presidential election, by collecting tweets posted during September and November 2016 using a manually compiled list of keywords and hashtags. Their state-of-the-art bot detection method allowed them to estimate the percentage of bot-generated tweets yet did not provide any evidence either on their political bias nor on consequences for the electoral result. To explain, the manner in which social media source news, the frequency that news can as well as the user access frequency, has multiple implications for the functioning of the public sphere and the quality of political debate. Consider, for instance, the case of Twitter, where anyone, professional reporter or not, can make a post about any kind of incident happening anywhere in the world (ibid). No fact-checking mechanisms are in place and posts are ranked and displayed in a user's feed according to popularity. The challenges of credibility, dependability and news' factuality become apparent. Posts that attract attention, i.e. sensationalist news, are what dominate the average

user's Twitter feed. Consequently, the news or stories that circulate are less convincing, people trust the system less, and the public sphere suffers (ibid).

In summary, social media and in specific, social bots can and do enable a host of positive and negative actors. This is visualised in Table 2 (Appendix). In other words, their dual use, has been observed and found to both strengthen and facilitate certain democratic functions while at the same time, undermining some other core processes (Gorwa and Guilbeault, 2018). Previous studies have found that meddling by domestic actors raises doubts about the integrity of elections, triggering a chain reaction that delegitimizes the political system, depresses voter turnout, and encourages mass protest (Norris, 2014; Tucker, 2007; Wellman, Hyde & Hall, 2018).

W. R. Neumann (2016) coins the term 'valended communication' (ibid: 44-46) to refer to the human tendency to seek reinforcement of our identities and ideals in the news and the interpretation of political events. This is an argument that becomes highly relevant when it comes to eco chambers and filter bubbles and raises serious concerns about the quality of public deliberation based on online news sourcing. If we are only exposed to news that reconfirm our already comprehensive and established perspectives, then our political decision making lacks the pluralism and diversity that need to characterise our political communication in order to arrive at optimal political outcomes in our globalised and highly heterogeneous socio-political collectives. At the same time, we become even more absolute and polarised, leading to political deadlock and deliberative atrophy. In other words, there results a shortfall in adhering to the liberal democratic ideal which proposes that in a modern, diverse industrialized nation-state immersed in a global network of communication and interaction, effective public dialogue cannot be sustained without the promotion of open and vibrant pluralism.

Moreover, in the same context of self-validation seeking political behaviour, Achen and Bartels (2017) explore motivations behind voting preferences and argue in favour of a 'realist theory of democracy'. In this, people don't vote rationally (i.e. according to the choice best serving their interests) but based on group biases and social identities that lead voters to support candidates that are 'like them' (ibid: 267-296). Under such an understanding of voting behaviour, SMM becomes a necessary evil for any ambitious candidate as access to private digital data assumes an insanely high value. The latter includes much more than basic demographic information on a voter's age, race, sex, constituency, income, educational level and so on. It expands to family history, ideological allegiances, consumer choices and other types of sensitive information.

This section served to explore, analyse and evaluate theoretical literature and empirical evidence on the relationship between SMM and voting behaviour. For some, the identified depletion of democratic capital and disruption of core democratic processes, are naturally ensuing inefficiencies generated by technological advancement and the socio-political changes the information revolution has caused (Omotosho, 2019). To some extent, we share this scepticism towards alarmist voices foreseeing the 'end of democracy' (Shenkman, 2019). This is why the focus of our exploration is not placed on the impersonal and unintended impact on democratic capital caused by the paradigm shift of news sourcing that social media caused.

Rather, we investigate potentially disruptive and depleting effects on democratic processes, that social media create due to political actors exploiting his paradigm shift to favour their individual or party interest at the expense of the public's. In this light, our argument is not a teleological or consequentialist one, claiming a significant impact of SMM and data abuse (in political campaigning) on electoral results. We assume a deontological viewpoint, which regardless of the actual

consequences on voter choice, identifies a violation of individual privacy, a polarization of political dialogue, and an ensuing corrosion of democratic processes (ICO, 2018). In the next section we attempt to sketch the current regulatory environment surrounding EI and SMM. But for the sake of a thorough understanding of the issue, we first seek to shed light on the debate about where regulatory responsibility lies in the first place.

Governance Issues in the Digital Sphere of Automation and SMM

Where Does Regulatory Responsibility Lie?

One of the first question scholars attempt to answer is where does responsibility lie when it comes to the regulatory prevention and legal treatment of EI: to the state or private companies? Maréchal (2016) supports a state-based monitoring regime promoting standardisation and normalisation across all content providers at the algorithmic level. In contrast, Mittelstadt (2016) argues against a state-centric regulatory approach and places responsibility for eliminating political bias on the social media platforms themselves. He argues in favour of self-regulation premised on strict and thorough auditing procedures (ibid). Along similar lines, Sandvig et al. (2016) attempt to show that algorithms themselves can be checked for manipulative content and call for social scientists to focus their research activities on this increasingly pressing issue.

In our advisory framework, parts of all three approaches are adopted based on the two following observations: First, governments are found to adopt the use of specific social media tools (e.g. political bots) as they come from the social media providers. In this sense, they appear to tacitly endorse the privacy, security and other policies employed by these private companies, as adequate (Bertott et al., 2012). Second, Google, Twitter and Facebook have been observed to assume different or

even conflicting stances on their responsibility for content (Taylor et al., 2018: 14). This leads us to emphasize the importance of harmonisation of rules and standards across all disinformation and EI issue areas (from user terms and policy, third party access and privacy protection, to content ranking algorithms and fact-checking mechanisms). This is paramount both for governments to be able to provide an institutional framework for fostering the economic, moral and legal incentivising of corporate self-regulation and for monitoring and ensuring its enforcement. So, while the mandate for designing and implementing comprehensive policy responses belongs to the public sector, it is the private sector that possesses both the expertise and resources to tackle the complexity of SMM-related issues.

However, Susskind (2018) argues that relying on private tech firms to self-regulate is problematic due to generic characteristics of for-profit, commercial organisations along with technical facts about the software development and algorithmic design. First, there is an obvious lack of accountability both in a moral and legal sense. Private companies have no democratic constitution and are not answerable to citizens. Second, their incentives are not aligned with the 'common good', 'public benefit' or 'general interest' and is confined to commercial benefit and growth. To explain, the improvement of algorithmic transparency and platform accountability by enhanced public scrutiny, oversight mechanism and regulation requires a constructive dialogue between these companies and public authorities (Taylor et al., 2018). This presupposes companies to relax the protection of their innovations and share open access data with researchers and regulators (ibid). Since this is directly against their commercial interests, it becomes obvious, that a serious tension is created between the need for cooperation and the willingness of social media platforms to cooperate. Third, regulatory regimes and legal systems change systematically over time, whereas code is developed on an ad hoc basis and in an

inconsistent way. This means that regulation aimed at controlling SMM at a specific point of time, might end-up obsolete rather fast and unexpectedly.

The Current Legal Environment of EI

The legislative landscape around EI in Western MLDs is divided between a) a small number of legally binding national and regional regulation mainly around data privacy and security protection (e.g. the GDPR or the UK's DPA) and b) soft-law instruments such as self-regulatory initiatives and bilateral agreements between public bodies and social media technology providers with regard to archiving and information accuracy (e.g. the EU's Code of Practice on Disinformation). With few exceptions such as the GDPR most of the policy related to the use of the social media predates the creation of social media technologies, and when it does not, it focuses mainly on the governmental use of social media for e-governance purposes and other similar functions (Bertott et al., 2012).

This means that EI, disinformation campaigns and SMM fall within the technological capacities, operations and functions of social media which the current legislative environment is not adequately addressing (ibid). And when it does, it only does so in a broad, non-specific manner which fails to address social media related information management issues at the operational level (the immensely broad scope of GDPR is a primary example of such policy instruments) (ibid). Even though, at a European level, monitoring of platform providers and their use of private data is stricter than in the USA, a comprehensive, legally-binding and democracy-enforcing regulatory framework for controlling EI has is still lacking. In fact, in simple words, current legislation aims at ensuring third-party compliance of social media platform providers to governmental privacy, and security and accuracy standards and requirements (ibid). Given that the latter has not been designed to and thus fails to

address the information management issues relevant to EI, it follows that a large policy gap can be identified.

Interestingly enough, we observe a growing pattern that shows isolated, one-off initiatives, strategies and actions plans to tackle EI in a context-specific manner, which however, lacks generalisability and hence is hard to see them developing to stable, consistent and effect hard-law instruments. Examples include, the EC's 2018 Action Plan against Disinformation or Sweden's 2018 strategy for promoting, entrenching and defending a strong democracy (European Commission, 2019).

This section showed that despite the proliferation of attention paid to the issue from academics, experts and policy-makers current countermeasures taken at a national, regional and international level do not suffice to meet the challenges arising from SMM and Digital Propaganda. Only a few countries have actually implemented revised data protection measures to combat SMM, while existing legislation seems to be inadequate for dealing with the "new dynamics and content forms in our continuously evolving information ecosystem" (Bradshaw et al., 2018: 8).

Literature Synopsis

The first 'lesson learned' by reviewing literature on EI, was that social media companies seem reluctant to identify themselves as members of the online press community which decreases their moral and legal obligation to comply with journalistic standards and ethics (such as accountability, transparency, accuracy and credibility). This leads them to become more accommodative of 'affective' and non-factual reporting and thus reinforce the 'post-truth' character of public opinion formation. With regard to electoral races, this was observed to fuel a trend of personal, psychological and demonstrative factors shaping voting behaviour and political preferences. Referring to the liberal political philosophy found in the works of

scholars such as J. Habermas and J. Rawls this trend was found corrosive for productive public dialogue since it undermines the value of evidence-based political decision-making.

Yet despite this impact on depleting the informational basis of voter, our review showed that there exists no empirical evidence on a direct and strong positive correlation between EI and individual voting behaviour/choice. This shifted our attention back to the academic foundations of our research question and compelled us to establish a clear theoretical connection between EI and democracy. This was achieved by showing how the function of social media platforms in modern data-driven political campaigning as well as their utilisation as means to spread disinformation undermine Dahl's democratic ideal, transcend basic human rights. Examples of these tensions were found to vary from micro-targeting and the associated corrosion of voting autonomy and/or disinformation campaigns and the ensuing impairment of equal opportunities in political preferences formulation to political hacking and the resulting loss of trust in the democratic value of representation. Identifying the specific democratic principles that are challenged by EI was meant to facilitate a more well-targeted recommendation framework.

Towards meeting this end, the two last sections of our literature review enabled us to identify specific policy gaps in the regulatory environment surrounding EI across MLDs. We found that current legislation lacks cohesiveness and consistency and is in urgent need of revision in order to adequately respond to the new challenges posed by the modern information ecosystem. In addition, after reviewing academic arguments on whether regulatory responsibility lies with states or companies themselves, we were led to conclude that any effective measure to counter/prevent EI must involve public-private collaboration.

Methodology

The methodology section of this paper will operationalise the knowledge gained in the literature review by providing concrete tools to endeavour with great depth into the analysis. Firstly, a scope captures the capacities and ambitions of this study, supplementing the literature review with practical context and reinforcing the research question. A philosophy of science provides guidance and an ontological basis for the concrete elements of the methodology that describe the analysis of this research. The analysis methodology is introduced by a varied qualitative approach section explaining the reasoning and advantages of the method chosen. Further the analysis section is split into three different sections: 1) Nested Analysis, 2) Secondary Data Analysis (SDA), and 3) validation against expert publications, each explaining the individual steps of the methodology while affording in depth understanding for the reader and future studies trying to replicate the methodology of this paper. Conclusively, limitations of the methodology will be addressed.

Timeliness

Preceding the philosophical and methodological sections of this methodology is the scope and extent of this study. Establishing sharp boarders for the study's capacities and ambitions serves as a clear catalyser for a successful conduct and conclusion thereof. Firstly, this study is being conducted within a four months' time frame from February to May 2020 affording sufficient coverage of political developments influencing the research effort surrounding EI. Among the most prominent political process in 2020 are the US presidential elections (Flegenheimer, 2020), and the Taiwan general elections (Babones, 2020). Secondly, this study is also conducted during the corona crisis which began with an outbreak in China in 2019

and has caused multiple national lockdowns in the West in 2020 (Falush, 2020). The corona crisis is setting unprecedented examples of policy capacity and the gravitas of the digital sphere for the continuation of both governance and business. It is therefore a unique competent influencing the analysis possible within this paper. Particularly with a strong focus on SMM with regards to digital and online strategies that corrupt and influence electoral results, digital propaganda and political hacking, the two tools in special focus (Berghel, 2017), have become a more paramount threat than ever. The crisis has also potentially worsened the already thin line between misinformation and disinformation (Bitiukova et al., 2019), bringing extra layers to the study. Thirdly, the methodology chosen is customised to capture a rapidly changing field of revelations by means of setting selective literary scopes to inspect with higher precision and depth the topics set in each chapter. The ambition of this study is to build replicable regulatory policy recommendations by means of a Nested Analysis that employs Secondary Data Analysis and expert publications.

Philosophy of Science

Navigating the literature by means of the research question equally translates into the data collection and methodological approach. While the data determines the methodology chosen and is in large part anchored in the research question, it is important to contextualise the guidance and approach with a philosophical foundation. As the methodology will be centred around a mixed methods approach and employ Nested Analysis, utilising both large-N and small-N analysis, it is only appropriate to capture the same intersectionality and multifaceted approach in the philosophical part of the methodology. Such a driver helps widen the spectrum while simultaneously adding robustness to the hypothesis test. Qualitative data will build

the exclusive basis for this study's analyses, yet the procedural empirical methods employed draws from social sciences and sciences alike.

Drawing both from science and social sciences Roy Bhaskar (1975) sought to create an approach to elucidate the world existing regardless of human comprehension or actions intended to change it. He called this the intransitive dimension, a sphere that is formed beyond intent and that shapes the observable world around us. The access key to an informed interpretation of the intransitive dimension is the transitive dimension. The transitive dimension is the world that is governed by linearity and causality caused by human action and intent (Benton & Craib, 2011). In the transitive dimension observation are possible that help to explore the intransitive dimension, and consequently contribute to a more holistic understanding of reality (ibid). Initially employed as a philosophy for the sciences, Bhaskar entitled it 'transcendental realism' (Bhaskar, 1975). As it came to be adopted into the tradition of social sciences that etymology changed to 'critical naturalism', eventually evolving into the now commonly popularised term 'critical realism', as also used in this study (Cantor & Bhaskar, 1982).

Critical realism brings an ontological basis that helps define the various spaces across which this thesis operates. The research question asks how can (self-)regulation of Social Media Manipulation (SMM) assist in safeguarding free and fair election in modern democracies? Isolating the two variable elements, that is those which affect the fixed elements, EI and democratic elections, the applicability of critical realism becomes immediately apparent. SMM is equal parts observable in the transitive dimension by means of human actions and their causality, as it is rooted in the intransitive that is the digital sphere within which it operates. (Self-)Regulation, likewise, is the result of linear and traceable human action and intent while its consequences unravel in the intransitive dimension. Legitimate government theory

teaches a lot about how the intention of a policy can vary vastly from its perception, and how the gap between de juris and de facto implementation can thus be quite severe (Seagrave, 2015; McDermott, 1999). With both SMM and (self-)regulation nested between the transitive and intransitive, a clear link must be laid to capture a comprehensive understanding of their interplay in affecting democratic elections and EI. This link will be the mixed methods approach to capture a wide spectrum of data, which is the guiding principle in deciding the methodological approach. Nonetheless, critical realism facilitates the comprehension of the elusive reality in the intransitive dimension by means of empirically dissecting the transitive dimension. Carrying the philosophy of science in mind as the methodology is set up, an appreciation can be fostered that science in itself is a desire to find more robust truth by revealing the unobservable by means of the observable (Benton & Craib, 2011). And in that vein, this study follows to endorse that endeavour by setting a philosophical course that is so evidently driven by those principles.

Varied Qualitative Approach

Setting up the methodology a procedural element helps navigate the choices of methods available in social science research. Deriving from the research question a scope of data-needs can be identified (Béland & Cox, 2012). More specifically, the evidence required to either proof or disprove the hypothesis is an estimation at first and the methodology the development which enables the explorations of appropriate data to reach the desired result (Chernick, 2011). As the philosophy of science established the aim is to set up a methodology that in the first place serves proper accommodation of the data collected, and secondly facilitates access to a wider spectrum wherein the observable transitive dimension provides the insights necessary to infer knowledge about the more elusive intransitive dimension.

EI is steadily anchored in the social sciences and as such there exists a palette of methodological options that combine more qualitative heavy humanities approaches with more quantitatively driven approaches from the natural sciences (Béland & Cox, 2012). This study aims to bring to light inherent truths about the intransitive dimension which is rapidly shaping and reforming by means of the transitive dimension. Therefore, a qualitative dataset has been chosen as the basis for this study, as quantitative data might restrict the dynamics necessary to fittingly explore the reality shaping around EI. Combining methodological intent and philosophical guidance a varied qualitative approach has been chosen. A symposium of different strengths from interdisciplinary traditions has come to be considered particularly robust, especially with regards to subject matter that reach beyond one clear field of study (Greene, 2007) as is the case with EI. A varied qualitative approach entails combing multiple building blocks from different disciplines and translating them to fit the qualitative data employed, because the data should always dictate the methodology (Maher & Dertadian, 2017).

For this study a Nested Analysis approach has been chosen. Nested Analysis combines large-N and small-N analysis to build a more robust methodological approach in order to more deeply penetrate a given research focus (Lieberman, 2005). Approaching the Nested Analysis with a clear intention to exclusively employ qualitative data, the elements of the large-N and small-N analysis have been adopted to be reflective of such dataset, meaning rather using actual population samples (N) the large and small-N are denoting the volume of literature or secondary data consulted for the respective set of the analysis. Secondary Data Analysis will be the foundation for the large-N analysis, in this case meaning that a wider range of literature and research will be consulted, as it helps in identifying a wider scope of literature to build independent recommendations. Expert evaluations will then serve

as the small-N analysis, small-N denoted three chosen papers by recognised experts, to determine whether the independently reached results comply with the more targeted and defined trends in current expertise fields.

While there have been limitations discussed with regards to varied qualitative approach, those are more concerned with applying too broad or too interdisciplinary a framework where a simpler single method approach could have yielded sharper or more defined results (Lieber & Weisner, 2010). This is however not the case in this study, due to the nature of the subject and the wide scope of the field explored, consequently negating such concerns.

Nested Analysis

Nested Analysis is a mixed method approach usually employed in comparative studies aimed at observing correlation or regression across cases (Rohlfing, 2007). Wherein this might indicate an exclusively quantitative data approach, Nested Analysis has been identified to be addressing a deficiency in application of mixed qualitative and quantitative methods (Munck & Snyder, 2007). Through initial utilisation in the field of economics, Nested Analysis further evolved a strong qualitative suitability that was eventually adopted in the political science (Patton, 2015). A more meta approach in the political science even allows for a purely qualitative engagement of the method (ibid).

Nested Analysis was first introduced by Lieberman (2001) in a study analysing income tax rates in the comparative examples of Brazil and South Africa. According to Lieberman (2005) Nested Analysis has multiple advances. Firstly, Nested Analysis is a grave assistance in guiding in-depth research. Setting out a procedural and linear methodology, Nested Analysis allows a researcher to dive from a macro into micro level without losing focus or the sharpness of the argument. Secondly, in that vein,

Nested Analysis provides direction which is of particular value when multiple cases are being compared. Thirdly, Nested Analysis aims to provide extra strength to testing the hypothesis by means of additional tests provided in Large-N analysis (LNA) and Small-N analysis (SNA). In fact, integrating LNA and SNA is the core advantage of using Nested Analysis. For the purpose of this section SNA and LNA will continue to be denoted as though they were addressing a quantitative population sample. However, as stated earlier, the N merely denotes the volume of literature and research consulted in each step.

LNA and SNA are ultimately also the two steps of the Nested Analysis. LNA is the first and preceding step to executing a Nested Analysis. The preliminary LNA is meant to provide information that eventually compliments the SNA (Lieberman, 2005). Fig. 4 in the Appendix taken from Liebman (2005) visualises the branches used to guide the Nested Analysis. The figure uses the quantitive terms LNA and SNA.

Secondary Data Analysis (SDA)

The elusive nature and sophisticated diversification of EI across a multitude of spheres make it notoriously difficult to track as it unfolds. As established in the literature, the fine line between legitimate intention, such as in the case of misinformation, and malicious manipulation, or the mirrored concept of disinformation, are often times shrouded in interpretational vacuums (Bitiukova et al., 2019). Particularly recent examples of EI in the 2010s display unprecedented levels of sophistication eroding the precision of the public and private sector response (McFaul, 2020). Much of the current understanding around EI campaigns and SMM in the Age of Disinformation is the direct result of the processes set up to investigate their nature and scope (Mueller, 2019). Consequently, EI seems to be by definition best observed and interpreted retrospectively to guarantee linear cohesion and overall

comprehension. Primary data can be produced to capture informed interpretation post-EI. Such research may generate a dataset more abreast to the current state of knowledge but might also neglect proper attention to the more lingering elements of EI, which are crucial to understand when crafting preventative measures. Secondary data offers to bridge that gap by including information from prior research that expands beyond the scope of current understandings. As this study will concern itself primarily with secondary data drawn from literature, and is in that respect exclusively assembling qualitative data, SDA presents a notably suitable and appropriate method for the data concerned.

The relevance of SDA becomes particularly evident when considering the digital aspect of the research question that is guiding the data collection. The speed and information velocity afforded by digital tools and increased digital literacy among individuals (Akçayır et al., 2016) has cemented a modern urgency to capture and archive information at historically unparalleled capacities. The tools necessary to build mature strategies of cyber manipulation have become increasingly available online (Wooley & Howard: 2016). The theory section of this paper already alluded to concrete forms of SMM defined by the employment of (social) political bots, sock puppets, trolls, astroturfing and political redlining (ibid). All of these provoke various research across different disciplines. Data evidence and understandings in the field of digital EI are being pursued on a large, rapidly evolving scale indicating a strong possibility that the answers sought in the context of this research might already exist (Andrews, Higgins, Andrews, Lalor, 2012).

SDA is in its core akin to the collection of primary data (Johnston, 2014). Guided by the academic principles of empirical research, SDA applies the same procedural steps of data collection and evaluation as a primary data focused study would (Doolan & Froelicher, 2009). The only observable shift that underlines the most apparent

difference is the gravitas put with the literature (Johnston, 2014). Theory and conceptual application become a stronger focus where secondary data provides the basis for analysis, which makes the forming of the research question all the more poignant as it is the quintessential determinant of the way SDA is exercised (ibid). In fact, the fit between the research question and dataset is paramount in SDA (Kiecolt & Nathan, 1985), especially with the researcher in charge to select appropriate secondary data to support the hypothesis or aim of a research question (Magee et al, 2006).

The first step of SDA is to identify the dataset. Much as with the approach to a cohesive literature review, rather than merely setting up an experiment to collect primary data to a question, the research questions guides the initial undertaking of what knowledge is already out there and where are the gaps that analysis will try to close by analysis the exciting knowledge (Creswell, 2009). Where SDA exceeds the effort of the literature review is in considering and including data from related and supporting literature that has been identified in conjunction with the study at hand (Dale, Arbor, & Procter, 1988). One of the leading principles motivating an SDA is the premise that data to answer a nouvelle research question might already exist in adjacent fields of study and previously executed research efforts (Doolan & Froelicher, 2009). This premise is supported but earlier studies which showed that in primary data collection a significant part of data is not utilised or employed in the research it is intended for because it does not support the research question and hypothesis at hand (Heaton, 2008; Smith, 2008). Conclusively, an SDA is started by expanding on the literature review and explore potential dataset applicable to the aim of the research question. Ideally such data has not been previously utilised to answer a similar research question. The first step of identifying the dataset(s) is followed by evaluating the appropriateness of the chose dataset(s) for the research question to guarantee the

necessary fit is substantiated (Dale et al., 1988). Stewart and Kamins (1993) offer set of parameters consisting of six elements to guide the evaluation of dataset appropriateness in SDA. 1) The purpose of the study. What was the initial research question that motivated the primary data collection and to what end was it followed. It also looks at wording, context, and agency granted to topics, individuals, and groups within the study. 2) Authorship and instigators. Who commissioned the data to be collected, who eventually collected the data, and who evaluated and analysed the data. This part is expanding on the motivation of a study and helps contextualise the procedures and other parameters in the evaluation. 3) The data collected. What kind of data was collected. This element examines the purely methodological quality and quantity of a database. A survey will give different quality of data than an interview, and a quantitative study bring different insights than a qualitative. Establishing this, assists in seeing whether the study is a match for the analysis based on the research question. 4) Time and periodical scope. When the data was collected can give insight into the currency of the data and contextualise results. 5) Methodology. This is fundamentally in contrast to number three, in that it observes how the data was collected. The result and quality dependents sharply on the methods employed. And 6) strength and consistency. Does the study, its results, methodology, and motivation cohesively fit into the research landscape and comparable studies. This section elucidates the validity of a study and therefore the extent to which it can support the SDA.

There are limitations with SDA. Relying exclusively on secondary data means that the data identified can never be as specific to the research question as a customised primary data collection (Johnston, 2014). While SDA does support studies that might have to be conducted at a distance or within a limited timeframe, studies that do not have to deal with such limitation may require extra justification in

defending their employment of SDA over primary data analysis (Dale, Arbor, & Procter, 1988). This is why SDA in this study is supported by expert interviews and integrated into a nested analysis in a mixed methods approach. The current age of digital information however has been making a significant argument to utilise SDA over primary data collection, as it is a legitimate empirical exercise yielding identical results if not even building more substantiated and holistic cases (Heaton, 2008; Johnston, 2014).

In summary, SDA makes use of the excessive existing data produced in the digital age and offers a more comprehensive set of data than primary data collection. Like primary data collection in follows a set tradition of procedures than can be qualified by a set of parameters for cross control. It is ideal to study a broad field with rapidly changing revelations and theories such as EI, as it acknowledges and integrates the full spectrum of current knowledge rather than merely competing with it.

Validating with Expert Publications

Where the SDA provides a macro perspective allowing for the independent formulation of targeted recommendations for a particular subsection of the analysis, the LNA in itself cannot support the robustness only afforded by the SNA. The SNA consequently must expand beyond the secondary data reviewed in the LNA and introduce a new dimension into the analysis that cannot be covered by the researcher's evaluation alone. Consequently, the study will introduce publications by experts to compliment and moreover validate the findings of the LNA. Expert references in forms of publications, solicited advice, or interviews are routinely employed by both market strategist and policy makers to shape, validate, and evaluate policies and strategies (Schwager & Greenblatt, 2012). In fact, there is significant awareness within

academia about the influence expert input has one the transitive dimension of a field and to which extent it can harbour necessary validation for a research (Baker, 1993). As the validation by expert publication is being employed to test an already existing set of recommendations created as a result of the LNA, the threat of domination has been mitigated by the nature of the Nested Analysis chosen.

The expert publications used in this paper are three selected pieces by highly cited and reputed consortiums of experts published by official academic or governmental institutions. The three papers will briefly be addressed in the subsections to follow.

The Stanford Cyber Policy Center Report

The 2019 Cyber Policy Center (CPC) report published by Freeman Spogli Institute for International Studies at Stanford in response to the findings of Mueller investigation in context of the Russian interference in the 2016 presidential elections (McFaul et al., 2019) and is the cooperative effort of 15 authors among them Michael McFaul (U.S. Ambassador to Russia 2012-2014), Eileen Donahoe (United States Ambassador to the United Nations Human Rights Council 2010-2013), and Thomas Hendrik Ilves (President of Estonia 2006-2016). The report has been heavily cited in US media reporting on the electoral threats looming in the 2020 US presidential elections and beyond been popularly reference in academic work since publication (DeHaven, 2019). The report is broken down into eight chapters:

- *Understanding Putin's Intentions and Actions in the 2016 U.S. Presidential Election
- *Increase the Security of the U.S. Election Infrastructure
- *Regulate Online Political Advertising by Foreign Governments and Nationals
- *Confront Efforts at Election Manipulation from Foreign Media Organizations

- Combat State-Sponsored Disinformation Campaigns from State-aligned Actors
- Enhance Transparency about Foreign Involvement in U.S. Elections
- *Establish International Norms and Agreements to Prevent Election Interference
- Deter Foreign Governments from Election Interference

For quality control and comparability of results five of the eight chapter focuses have been chosen to constitute the chapter focuses of this research. The corresponding chapters are denoted with a '*'. Where necessary the titles have been adjusted to better suit the context of this research. Each of the chapter in the CPC report build on an explicatory section examining the data and observable facts established around EI in the 2016 US presidential election. Each chapter then continues to summaries the conclusion drawn into applicable recommendations similar to this research. However, the report does not tie various string of research together nor those it references academic traditions. It is rather an assessment of the Mueller reports complimented by the most current journalistic findings. In that sense, the CPC report also provides a positive precedence for the demand of such research, as conducted here in, and is proof that innovative research using existing data can be a valuable contribution in the rapid EI debate.

The report is focused on the case of the United States, however. Therefore, the CPC report is complimented by two NATO reports that expand the scope to involve other Western MLDs, as well as other regime-oriented nation states.

Government Responses to the Malicious Use of Social Media (Bradshaw et al., 2018)

As a part of the NATO STRATCOM Centre of Excellence series on 'Countering the Malicious Use of Social Media' this paper aggregates and analyses a total of 43 cases of complete, in progress or dismissed government regulation initiatives in response to the malicious use of social media. The scope is confined to legal and regulatory interventions carried out in specific as a response to SMM and considers strictly on new or recently updated legal measures formulated as part of an effort to combat EI. One limitation of this scope is that it excludes regional or transnational initiatives, such as the EU Code of Practice on Disinformation. We account for this omission by supplementing the report with our own independent research when deemed necessary to investigate the regulatory environment of EI in great depth. The time period of data collection is set after 2016, with the last update of the case studies undertaken in October 2018. The main analytical product of this report is the classification of EI countermeasures into four categories according to their target:

1. Social Media Platforms
2. Civil Actors and Media Organisations
3. Governments themselves
4. Offenders

Then its category is broken down according to the requirements and content of proposed or implemented intervention as shown in Fig. 3 below.

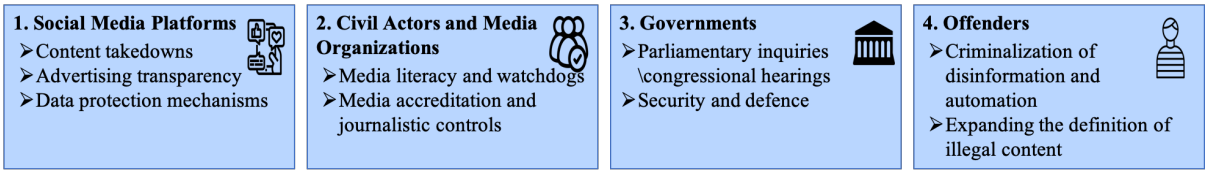


Fig. 3. Proposed or implemented interventions on EI, taken from Bradshaw et al. (2018)

After assessing these interventions, the authors argue that data protection laws remain highly fragmented, whereas algorithmic transparency and platform accountability have not been addressed sufficiently accounted for in countermeasures forwarded thus far. Accordingly, the report concludes by urging governments to "shift away from crude measures to control and criminalise content and to focus instead on issues surrounding algorithmic transparency, digital advertising, and data privacy" (Bradshaw, 2018: 12).

Industry Responses to the Malicious Use of Social Media (Taylor et al., 2018)

Also a part of the NATO STRATCOM Centre of Excellence series on 'Countering the Malicious Use of Social Media' this paper offers an account of the self-regulatory initiatives taken by the three more 'politically active' platforms between November 2016 and September 2018 to hinder the spread of disinformation. During these two years the researchers amassed 125 official company announcements about disinformation-targeted interventions that Facebook, Google and Twitter made in their Terms of Service agreements (ToS) (found in relevant company websites and blogs) and categorised them into 10 broad groups, as depicted in Fig. 6 below. The scope of the study was limited to the terms relevant to Europe and the UK, fact that partly limits the generalisability of the findings. Linearly comparing the terms and policies across jurisdictions can be tricky, since despite some universal terms, these companies have additional and/or different ones for users from different countries (a point that is further discusses in the analytical part of our paper).

The identified key intervention areas are better enforcement of existing terms and policies, mainly but not exclusively concerning news media, election committees and campaigns, fact-checkers and civil society organisations (Taylor et al., 2018: 14).

The main argument the authors put forward is that since no major changes to the existing terms and policies around user data, content and behaviour were observed, they must suffice to address the disinformation issues arising from their malicious use. In addition, the authors call for attention to the differing and/or even conflicting stances these three platforms take with regard to their responsibility for content and the problems this raises for tackling disinformation. They finally recommend a more proactive effort on behalf of platforms to work alongside governments and citizenry to arrive at responsible and sustainable solutions for combatting disinformation.

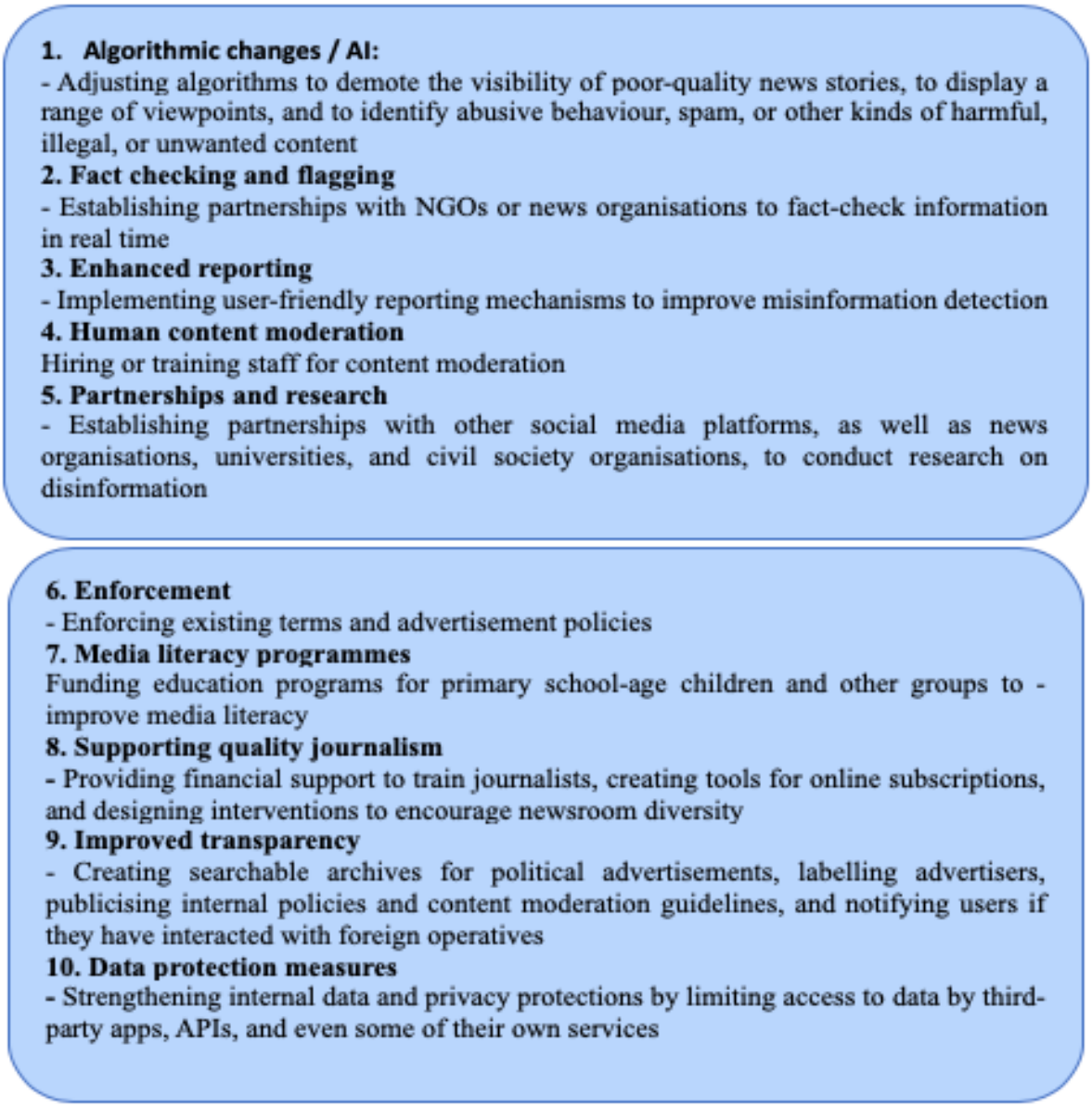


Fig. 4. Industry response capacity summary, based on Taylor et al. (2018)

Chapter Operationalisation

To execute the Nested Analysis appropriately, this section will shortly draw out the linear procedure for the chapters. A set framework will contribute to a cross-chapter quality control and facilitate comprehension for the reader and future studies replicating the methodology. The case execution follows a five-step principle in line with the hypothesis that SDA can produce replicable regulatory policy recommendations that can be substantiated by the LNA.

1) Establishing the chapter. Each chapter takes its angle from the chapters presented in the CPC report (McFaul et al., 2019). Unlike the CPC report however, the chapters in this study will aim to provide a general set of recommendations applicable to both private and public sector stakeholders across different modern Western MLDs. 2) Conducting the LNA. The first step for the Nested Analysis is the LNA. As stated in the LNA section this step goes beyond the literature review and establishes a literary scope for the particular topic explored in the chapter by means of SDA. The cases will be chosen to build a bridge across chapters while also ensuring a macro-level analysis. Secondary data is consulted to build a set of recommendations for the particular chapter topic. 3) Setting the recommendations. The recommendations need to be clearly defined and applicable in order to be tested in the SNA. 4) Conducting the SNA. In this step the expert evaluations are used to countercheck the validity and robustness of the recommendations created based on the SDA. 5) The chapter is concluded, and the success of the chapter's academic endeavour established. Throughout the branches laid out in the Nested Analysis section of the methodology shall be followed.

Analysis

Chapter 1: Understanding intentions behind interference

This chapter investigates Russian attempts to influence the electoral result in the US 2016 and Swedish 2018 elections with the focus placed on understanding and specifying the underlying reasons behind its digital information warfare strategy in each of these cases. Surfacing the particular interests and aims behind one of the best examples of a consistent and targeted EI strategy is the first 'test' to our original hypothesis; that EI destabilises the fundamental normative pillars of modern liberal democracies (the rule of law, political accountability, bureaucratic integrity and public deliberation). A thorough understanding of the historic, political and economic motivations that guide Russian disinformation campaigns and political hacking helps identify and assess their expected impact. This is deemed necessary for devising appropriate and effective countermeasures.

These two cases were chosen due to the relatively high availability of secondary data on the nature of Russian interference in their respective public spheres and democratic processes. Even though studying computational propaganda and digital EI can be tricky since the nature of cyberspace makes attribution of cyber operations difficult (Office of the Director of National Intelligence & National Intelligence Council, 2017: 2), in these two cases there exists enough evidence and information to help us identify the actors/stakeholders involved, the means employed and the desired outcomes and/or interests promoted. The similar EI methods used and an overlapping of aims, makes these cases comparable. The central findings of this chapter are that government transparency and accountability, the rule of law, media freedom and citizen engagement are best safeguarded against foreign-driven EI when designed countermeasures: a) combine top-down legislative action with a bottom-up digital education strategy, b) are backed by elaborate, precise and transparent

campaign and data protection laws and c) when there is an equilibrium between private and public interests that allows for regulation to prioritise 'democratic interest' over commercial/corporate profit. Lastly, assessing the responses of each country, enables us to compare the respective system 'resilience' of each state and draw conclusions for the appropriateness of each measure given certain contextual institutional and socio-political characteristics. The structure follows the logic of the argument, first laying out the content of Russian EI attempts and connecting them to larger geopolitical and economic goals; second, assessing and comparing the respective US/Swedish responses in order to set the foundations of the proposed countermeasures; and third, using the finding of the previous two steps, to devise a set of recommendations appropriate for effectively combatting this type of EI.

The Nature of Russian Interference: Stakeholders, Methods and Aims

Under president Vladimir Putin's command, Russia has launched what some commentators describe as the "the most amazing information warfare Blitzkrieg in the history of information warfare" (Abrams, 2016: 7). When discussing the multiple cases of digital interference in the function of MWDs, experts identify it as the modern version of traditional Soviet political warfare tactic/foreign policy tool known as "active measures" (Kragh & Åsberg, 2017; Abrams, 2016). Relying on disinformation and conducted secretly, under the principle of plausible deniability, these measures aim at influencing decision-making in a direction favour able or at least not harmful to the Kremlin by deceiving decision-making elites or public opinion (Kragh & Åsberg, 2017, 778). These activities vary in degrees of covertness and legality, with 'black operations' (as opposed to white and gray operations) listed as genuinely 'clandestine' and involving amongst other things, "the use of agents of influence,

spreading false rumours, duping politicians and journalists and disseminating forgeries and fake documents" (Abrams, 2016: 12).

As stated in earlier in the paper, such operations have proven to be the most corrosive type of foreign EI for democracies (ibid: 4). Under the EC's framework, a B2 type of disinformation campaign presents a critical global threat against democracy, interfering with sovereignty and causing geopolitical instability. After examining available information on the Russian EI, we identified two types of strategical targets.

The first being more practically, economically or geopolitically oriented, found in Russian security doctrines such as The Military Doctrine (2014), the National Security Strategy (2015) and Information Security Doctrine (2016). All these define information warfare as a defensive and a strategic priority (Kragh & Åsberg, 2017: 778, 882). Concerning the USA, they include 'weakening US Hegemony' portrayed as harmful to Russian national interests but also direct retaliation for sanctions imposed by the West following the annexation of Crimea back in 2014 and conflicting interests in the Syrian War (U.S. Government Publishing Office, 2018). In the case of Sweden, Russian geopolitical targets concern Swedish–NATO cooperation and Swedish/EU support for Ukraine (Kragh & Åsberg, 2017). These high politics/foreign policy goals can be seen as having a top-down scope, as they concern higher strata of political decision making, in which public opinion is less detrimental compared to other issues with a more direct and short-term social impact.

The second type of foreign policy goals we detected could be described having a more normative, ideological and long-term character with expected outcomes of a bottom-up nature. These would consist mainly of attacking democratic values and the liberal ideal in 'successful democracies', by portraying them as 'degenerated', 'obsolete' and 'corrupt', seeking to corrode trust and confidence of the respective citizenry in the electoral process, political leaders and institutions as well as regional

and international organisations (i.e. EU, NATO, etc.) and fostering division on top social and political issues (ibid; U.S. Government Publishing Office, 2018; Taylor et al, 2019). These aims are common both in the case of the USA and Sweden. This type of strategy is meant to indirectly increase Russia's geopolitical and economic sphere of influence by building a political profile which represents, captures and attracts groups with, amongst other things, populist, anti-establishment, Eurosceptic, anti-immigration sentiments. This way democratic resilience can be corroded from within, sowing and/or amplifying existing political and social divisions.

According to official documents (Mueller, 2019; U.S. Government Publishing Office, 2018; Swedish Security Service, 2018) in both examined cases, the Russian attempts of interference followed a bi-partite structure consisting of: 1) a social media manipulation, disinformation/propaganda campaign serving the second type, more long-term goal of amplifying socio-political discord and corroding democratic capital and 2) a barrage of cyber intrusion attacks targeting political parties and key election services, by releasing hacked materials and defaming specific candidates perceived as hostile towards the Kremlin. According to official investigations of Western states, disinformation campaigns are mainly carried through by the Internet Research Agency whereas political hacking falls within the duties of the Main Intelligence Directorate of the General Staff of the Russian Armed Forces (Bastos & Farkas, 2019).

'Black' SMM operations are distinguished from more transparent influence campaigns carried through by media puppets such as the RT or Sputnik (in Sweden) (Hofverberg, 2019). The Internet Research Agency has been reported to engage in SMM by the creation of fake accounts on Facebook, Instagram and Twitter pretending to be either; 1) an individual national of the targeted country, 2) a large social media group or page that is -falsely claiming to be- affiliated with the target country's political and grassroots organisations or even fictitious organisational and grassroots

groups and 3) mimicking real organisations (Pierre, 2020). At the same time, the Internet Research Agency has been observed to utilise Twitter by 4) creating accounts/individual personas that spread anti-democratic discourse, but most importantly by 5) building a bot network (an army of automated accounts) that spread disinformation and amplify existing decisive consent on the platform.

Recommendations

In the US, an effective agenda designed to respond to foreign EI and safeguard democratic processes has been proposed but not yet been implemented (Boot & Bergmann, 2019). With regard to campaign law and financing, 'The Honest Ads Act' (*H.R.2592/Honest Ads Act*, 2019) was designed to improve transparency and oversight of online political advertisements and ensure that they are not "directly or indirectly purchased by foreign actors" (ibid). With regard to domestic SMM, the 'Bot Disclosure and Accountability Act' (*Bot Disclosure and Accountability Act*, 2019) would prohibit any political party, candidate or authorised campaign committee to 1) "use or cause to be used any automated software programs or processes intended to impersonate or replicate human activity online to make, amplify, share, or otherwise disseminate any public communication" and 2) "solicit, accept, purchase or sell any automated software programs or processes intended to impersonate or replicate human activity online for any purpose." (*Bot Disclosure and Accountability Act*, 2019). But this Act does not afford enough protection from foreign attempts to interfere in the electoral process. This is would be sought in the 'Countering Foreign Propaganda and Disinformation Act' which directs the establishment of the "Center for Information Analysis and Response" responsible for exposing foreign information operations and coordinate counter responses (*Countering Foreign Propaganda and Disinformation Act*, 2016). Even though none of these Acts has been enacted to law until now, their

structure, provisions and aims seem to respond directly to the most immediate threats posed by B2 types of foreign-driven EI. In their totality, i.e. by complementing each other, these Acts represent a well-targeted and effective top-down regulatory response to the most critical type of threat for modern liberal democracies.

In Sweden, much more decisive steps have been taken to combat foreign EI, by heavily investing in a comprehensive and arguably successfully applied strategy to protect its democracy (Taylor, 2019). In the words of the Deputy Head of Protective Security: "[…] Influence operations happen all the time, but we now see an increase. There is also an increase compared with the 2014 elections. […] We can now see that the preventive efforts we have engaged in since early 2017 have paid off. People are more aware and alert than before, and this has increased national resilience. This, and the fact that we have an election system that is difficult to influence, will ensure a legitimate election result" (Swedish Security Service, 2018). What Linda Escar is referring to in this excerpt is Sweden's strategy for 'Promoting, Entrenching and Defending' its 'strong democracy' (ibid). This combined a series of measures in a 'whole-of-society and whole-of government' strategy which aimed at reinforcing the democratic resilience of all political actors; the government, the media, civil society and citizens. Highlights of this plan included setting-up a high-level interagency coordination forum to serve as a national platform1 for election planning, preparation and protection (Taylor, 2019; Brezina, 2018). Apart from technical, logistic and bureaucratic responsibilities, a main task of the Civil Contingencies Agency was to train local election officials and politicians on how to spot and counter information influence activities (e.g. by means of training sessions and the issue of a relevant handbook) (Swedish Security Service, 2018). Given the nature of modern EI and

[1] The Security Service, the Swedish Police, the Civil Contingencies Agency, and the Election Authority are the main governmental bodies collaborating in this strategy (Brezina: 2018)

especially micro-targeting this measure is essential for equipping citizens, officials and politicians at the local level with the apparatus to resist malign foreign influence.

Next, the biggest media outlets[2] collaborated with independent international journalists, fact-checkers and students to create a 'pop-up newsroom' (ibid) publishing daily newsletters addressed to news providers including tracked and identified sources of disinformation (ibid). Last but not least, Swedish authorities decided to expand the scope of digital literacy efforts to cover the whole constituency. The Civil Contingencies Agency issued and distributed to almost five million households a booklet containing instructions on spotting and resisting hostile information and propaganda and thus 'building psychological resilience' in civilians to anticipate and resist foreign interference (Berzina, 2018).

The vast differences between the responses of the two countries, can of course be linked to a number of contextual institutional, demographic and socio-political characteristics such as the size of the population, the structure of the political spectrum (bipartisanship vs. pluralism or two-party vs. multi-party system) or the electorate system itself. Yet, our research focus is not placed on explaining these discrepancies. Rather we seek to identify and replicate the successfully proposed or implemented policy examples to formulate a set of recommendations for tackling this type of EI.

In this light, the first 'lesson' learned is that because Russian intentions have both a practical immediate aim and a normative long-term one, combating EI requires technical safeguards (cybersecurity) to ensure the integrity of the electoral process by protecting against political hacking (1 type of Russian EI) but at the same time a proactive policy towards digital media literacy appropriate for enhancing the ability if both officials and citizens to resist social media manipulation (the second type). In simple words, Sweden's 'whole of society' defence strategy seeking to raise citizen

[2] Swedish public television, Swedish public radio and two major newspapers, Dagens Nyheter and Svenska Dagbladet (ibid)

awareness and foster social resilience should be coupled by the US's legislative propositions improving the transparency of campaign law and financing, regulating or in fact banning the use of bots for campaigns purposes, strictly monitoring and criminalising the intentional spread of disinformation.

The second main finding is that political campaign laws have to be elaborate, precise, and transparent in order for any framework for combatting EI to be effective. The content and targets of the legal reforms entailed in the 'Acts' proposed by American law-makers undoubtedly point to that direction. The fact that they have been 'frozen' and what it implies for American politics is a much broader discussion escaping the scope of this paper. In any case, legal action to account for the technical aspects of EI cannot be taken without a reconsideration of the election process, including and mainly concerning campaign law and financing (the details of which will be further discussed in Chapter 3). What is allowed, clearly drawing the line between legal and illegal conduct and prohibiting malign practices and who pays for it: ensuring a transparent system where candidates cannot 'hide behind' foreign actors when violating campaign law.

Finally, comparing the immediateness of the response between Sweden and USA could be taken to imply that in order to effectively combat SMM types of EI which are highly related to regulating the conduct of private social media platforms, a certain degree of separation of private and public interests must exist so that legislation can't favour the latter at the expense of the former. In the case of Sweden, the EU Code of Practice on Disinformation and the GDPR broadly -albeit not both hard-law instruments- tackle both data privacy and disinformation issues. In the USA, no nation-wide regulatory restrictions have been placed and/or any substantial policy changes taken place to meet the challenges that the proliferation of SMM raises for free and fair democratic processes. Third-party use of private data, campaign

transparency, the illegal use of bots and all other SMM-related topics cannot be monitored and controlled without a certain degree of state-based interference in the conduct of the private platforms. In this sense, the lack of response in part of the USA can maybe be connected to differences of statecraft between American and European culture (e.g. pro-business or pro-welfare approach). Hence, an intervention in the private sector (market) in order to regulate the malicious use of social media, cannot be effective if there is not enough separation of interests between the latter and legislative authorities, in order for cost-raising and profit-depleting measures to be enacted to law.

Assessing the recommendations

The CPC report lists the following actions as necessary for deterring foreign EI that are relevant to our cases (McFaul et al., 2019: 15-16):

- Signal a clear and credible commitment to respond to election interference
- Maintain a visible position of capabilities, intentions, and responses.
- Improve the quality and scope of detection tools and reporting policies for social media platforms.
- Build an industry-wide coalition to coordinate and encourage the spread of best practices.

As this chapter served to show, the USA seems has yet to materialise these objectives to concrete policy, whereas, Sweden's 'whole of society and whole of government' strategy successfully integrates them into a comprehensive response to Russian attempts to EI. Following primarily the latter's example but also utilising the former's proposed legal (re)actions, our suggested solutions combine technical defence mechanisms (e.g. legislative revisions of campaign law and strict regulation of bot use) with broader educational measures that facilitate the detection and

exposure of disinformation. Overall, these convey a convincing pledge of countering EI while at the same time stressing the importance of collaboration between different stakeholders. A point that perhaps needs to be stressed more, is the importance of communicating these efforts as a form of deterrence towards future EI. Both theory and empirical evidence suggests that in order to be effective, and ultimately successful, a deterrent strategy must transmit clear and convincing signals of "timely, tailored, consistent and credible costs" that "outweigh the benefits" of taking a specific action (McFaul et al., 2019: 63).

Our action plan's scope includes the first three categories of the Bradshaw et al. (2018) report. Namely, it targets offenders, citizens, civil society and media organisation and government capacity to intercept EI. As mentioned earlier in the paper, the report recognises the "fragmentary, heavy-handed, and ill-equipped implementation of counter-measures" (ibid: 12) while emphasising the deep roots of SMM in our current information ecosystem (ibid).In an attempt to overcome this difficulty, our solutions aim at requiring all stakeholders to act against foreign EI: from improving media literacy and disinformation monitoring and reporting infrastructure to criminalising disinformation dissemination and building legal protection against the malign use of bots. Lastly, not including measures targeting platforms themselves is intentional, as we undertake this task in Chapter 3.

Conclusions

In this chapter we attempted to clarify the intentions behind Russian interference in two modern liberal democracies, namely, the USA and Sweden. The purpose of this case analysis was to classify the nature, content and objectives of Russian EI efforts in order to assess its impact on the four parameters that define a well-functioning modern liberal democracy and thus inform our benchmarking of a

solution framework. We found that Russian EI strategy had a two-fold character: one immediate, economic, high political with a top-down scope of influence and second more normative and long-term with bottom-up effects on the target population. This led us to conclude that an effective response should protect against both, by combining legal safeguards against political hacking and disinformation campaigns with an investment on increasing societal and individual citizen capacity to support free and fair democratic process in the face of the challenges posed by our modern informational ecosystem. The differing degree to which these two states managed to successfully respond to Russian interference in their electoral processes and public political debate, underlined the significance of well-defined and transparent campaign law has for an effective response to EI. It also, pointed to an assumption about the influence of corporate interests on regulating the conduct of highly profitable, powerful and influential private social media companies. Consulting secondary data and reliable policy frameworks compiled by credible organisations, allowed us to confirm the robustness and validity of our recommendations. The only omission that surfaced after the assessment, is the strategic significance (as a deterrent) of making actors behind EI aware of the commitment, capabilities, intentions and responses of EI defence systems. This way, past foreign EI can be adequately penalised and future attempts prevented.

Chapter 2: Increasing the security of electoral infrastructures

This chapter addresses the structural security gaps ingrained in the vastly decentralised and often uncoordinated electoral infrastructure systems present in many modern democracies, particularly those of more developed nations often relying on digital infrastructure to conduct democratic processes (Underhill, 2012). Russian exploitations serve as particularly poignant examples of sophisticated and

comprehensive manipulation attempts, as they have been cohesively investigated by the U.S. Special Council on Russian Interference in the 2016 Presidential Elections, as well as by the European Commission in context of the 2019 EU parliamentary elections. Both cases lend themselves notably well to SDA due to the extensive publications and secondary data available. In line with chapter one, continuous analysis of the 2016 US presidential elections provides a constant dependent variable whereas the inspection of the 2019 EU parliamentary elections offer an additional substantiation of the robustness of the dependent variable, that is the elections consulted. Consequently, this chapter will test our hypothesis first by means of exploring the integrity obstruction of the electoral infrastructures in the US and the EU by Russia, based on which a set of impetrative regulatory needs can be identified to establish the necessary recommendations that will be held against the expert evaluations in the second step.

American Elections – A flawed gold standard

At the zenith of its geopolitical hegemony, shortly after the collapse of the Soviet Union in the early 1990s, the US democratic system was considered the gold standard of distributed electoral agency (Fukuyama, 1992). However, this changed notably with the turn of the millennium. While considerable scrutiny was applied to the American role in global politics post 9-11 in context of President George W. Bush's war on terror (Guyatt, 2003), the decay of confidence in the US electoral system set on largely with vulnerabilities exposed in the 2004 US presidential elections (Johnson, 2004). Besides the fall of the iron curtain and the apparent dissolution of the bi-polar world order, the 1990s brought with them a much more paramount dent in human history: the digital revolution (Helbing, 2015). Second only to the invention of the printing press (Wheeler, 2019), the internet radically transformed and structurally

reorganised all strands of society including electoral processes (Helbing, 2015). The 2004 US presidential elections were so pivotal because they unmasked inherent inconsistencies in data and systematic weaknesses of the supposedly strongest electoral system in the world, all of which were rooted in new digital processes (Johnson, 2004). Johnson (ibid) called the 2004 election: the year the internet came of age. A little more than a decade later, lacking responses and outstanding preventative measures to protect digital components in the electoral process have all but exacerbated the issue of US electoral exposure to EI (Pope, 2018). The 2016 US presidential election located the world's foremost economic, political, military, and cultural force at the epicentre of the most sophisticated and comprehensive EI observed today (Clinton, 2018).

Understanding the American capacity and context driving its ambitious and rapid advancement in the digital transformation provides a singular factette of the electoral problem. While America's need to perform and assert its standing at times forces it to endeavour into unchartered territory with the consequence of wide-ranging spheres of strategic exposure, it only constitutes a wider context that is substantiated by the inherent distributive nature of American democracy. The United States is a federation of states. Similar to its former metropole the UK or the German Federal Republic rebuilt in its image post WWII, each state is in its own right an autonomous political entity akin to a country (Rivlin, 2000). Each state possesses its own legislative, judicative, and executive institutions with considerable governance over its respective territory (Anzia & Jackman, 2013). However, states and all other entities of the United States are subject to federal law and can neither sign treaties with sovereign nations, issue currency, raise military forces, nor secede from the union (ibid). The complex balance between federal supremacy and state autonomy leads to elections being administered by the states on behalf of the federal government.

Supervision of voter's data assets consequently lies with each state. The primary responsibility for electoral execution is voter registration which entails major intricacies, including 1) continuous status records of each voter, 2) current applicable information points for each voter, 3) ensure accuracy of eligible voter lists by mean of constant updates of the current records, and 4) provide correct and up-to-date lists of voters to respective districts (Geys & Vermeir, 2014). Whereas voter registration and the administration of voter data assets are centralised with the state, ballot casting is delegated to the separate counties within the state. It is the counties' pejorative to decide whether they use analogue or digital voting procedures (Moynihan, 2008). This autonomy leads to wide ranging disparities across counties within a singular state line. More so, discrepancies between digital voting system capacities to resist manipulation and interference are starkly evident in the absence of a centralised auditing board (ibid). All digital voting systems however are obliged to comply with three core provisions: 1) electronic voting systems recoding ballots cast by voters in person at physical ballot boxes within a county, 2) tabulation systems counting absentee and postal votes, and 3) coded programmes identifying quantitative irregulates in voter numbers when set against the centralised state records (*Help America Vote Act*, 2002).

The decisions around voter systems and voters' county assignment are highly contested (Kennedy, 2016). Legal processes that allow for practices such as gerrymandering wherein partisan stakeholders can manipulate the district boundaries to favour voting results in favour of a particular candidate or party have been described as domestic EI due to the unfair advantage it creates (ibid). This alone illustrates how a system so inherently exposed to internal manipulation is prone to attract foreign hostilities. The election ecosystem is composed of various stakeholders each contributing and influencing the successful execution and procedure of the

electoral process. When errors, disruptions, and deliberate interference occur, voter confidence is undermined weakening important elements of the electoral ecosystem and offsetting the balance necessary to protect their roles in the process (Corstange & Marinov, 2012). The consequences of eroding voter confidence and trust in the electoral system include exacerbated partisanship, higher susceptibility to misinformation and digital campaigns to drive division, as well as lower engagement rates (ibid). According to the Muller report, in the 2016 US presidential elections, Russian bots have been employed in attempts to disrupt and distort election results in various districts with the aim to undermine electoral confidence and trust in the election results (Mueller, 2019). There is no record of these attempts succeeding but the report alludes to the suspicion that a successful attack was never the prime intention (ibid). These interference attempts, as well as the distribution of awareness around them, was sufficient enough to call into question the accuracy of the results and to erode trust in the electoral system (ibid). It further fed into disinformation campaigns of various political groups within the United States furthering partisanship in the American political culture (Vargo & Guo, 2016).

The US example communicates a clear need for 1) consistent and authorised auditing in order to ensure benchmarks across districts and verifying the accuracy of voter record implementations, 2) a common digital and electronic system to mediate the effect of discrepancies across different counties, 3) more extensive cybersecurity measures to build robustness of the voting infrastructure, 4) protection of the electorate by state enforced standards and norms baselined with federal law, and 5) provision of federal support to strengthen electoral infrastructure where necessary. The inherent vulnerabilities and the knowledge around their exploitation by internal actors has made the US elections prone to foreign hostilities. The needs identified are drawn from the secondary data provided around the particularities of

the US electoral system as well as the example of Russian exploitations thereof. To contextualise their relevance the US example has to be compared with a similar case offering sufficient secondary data on the electoral system and its vulnerabilities complimented by an actual example of its exploitation. As introduced in the beginning of this chapter the EU parliamentary elections and Russian interference therein have been chosen to connect the US needs to a more globally connected set of recommendations.

A Union Divided – European Electoral Vulnerabilities

To accurately identify the vulnerabilities in the European electoral infrastructure, it is paramount to first grasp an understanding of the European Union as a construct. The US example illustrated well the need to understand the inherent challenges within a legislative setup. And whereas the US is a sovereign nation composed of autonomous states, the EU is to some extent an inverse thereof, namely a union with autonomous legislative and judicative bodies endorsed by sovereign nations.

The European Union is the result of a sequence of treaties signed in the aftermath of WWII (Milward, 2005). The deadliest military conflict in human history was the direct result of weak and ineffective measurements taken in the direct aftermath of WWI (Blakemore, 2019). As Europe lay in ashes, its post-war leaders, as much as the victors East and West alike, were keen to prevent a third cycle of global devastation emphasising the need for interdependence and cooperation: the beginning of globalisation (Huwart & Verdier, 2013). On a global stage, the sudden end of Pax Britannica with the First World War had left a power vacuum neither Britain nor its contender France had the capacity or authority to reclaim (Barlas & Yilmaz, 2016). Britain was exhausted by war efforts and scrabbling to keep Empire

together (ibid), while de Gaulle's France post-Nazi-occupation was in domestic and colonial disarray and had to first anchor itself again in a new constitution (Micaud, 1946). Instead the US started to step up its global role and started to lay the foundation of what would come to be known as Pax Americana (Barlas & Yilmaz, 2016), an important element leading to the End of History theory introduced by Francis Fukuyama (1992) and cited in the introduction to the American section of this chapter. The Bretton-Woods systems established the International Bank for Reconstruction and Development (IBRD) and the International Monetary Fund (IMF) and set the new economic course for the Western world under Columbia's leadership, while the United Nations became the leading global authority for international affairs nested in America's biggest city, New York, just a few hours away from its capital (Jo, 2011). American domination in international politics significantly weakened British and French potency, certainly contributing to the French drive to cooperate with its historical arch enemy Germany in order to at least take the head position on the new continental order in Europe (MacMillan, 2009). Britain had culturally, political, and economically detached itself from most of the European continent during the hegemony of Empire (Samson, 2001) and its attempt at partaking in the European project failed in 2016 (McTague, 2020). It is therefore the Franco-German condition post-WWII that catalysed the European project. Today still the Franco-German twin engine that is credited with much of the European integration efforts over the last decades (Krotz, 2014).

In 1951 the Paris Treaties united Belgium, West Germany, France, Luxembourg, Italy and the Netherlands in the European Coal and Steel Community (ECSC), deriving from the premise that interdependence in one of the core industries necessary for war will make such less likely (Millward, 2005). The 1957 Treaties of Rome formed the European Atomic Energy Community (EURATOM) and European

Economic Community (EEC). These three communities were commonly referred to as the European Communities (EC). In 1985 the Schengen Area was formed to allow the free movement of goods and services across the community's borders. By this point the UK, Ireland, Greece, and Denmark had all signed on to the treaties of the EC and been admitted by the existing members. In 1986 Spain and Portugal, freshly released from the shackles of authoritarian regimes, joined the block. They were the last to join prior to the 1993 Maastricht treaty establishing the European Union. In 2007 the treaty of Lisbon amended the Maastricht treaty and reformed the voting systems of the EU's legislative bodies. Today the EU counts 27 member states, an internal single market (shared with the European Economic Area including approved non-member states), and a currency union called the Eurozone (Gänzle, Grimm & Makhan, 2012). The union consists of seven major bodies with the Council of the European Union, the European Parliament, and the European Commission forming its legislative heart (Tömmel, 2014). Strictly speaking the European Commission is the executive body of the union (ibid), however as the union does not constitute a sovereign state most experts agree that effectively the EU has no real executive powers (Curtin, 2016).

Understanding the European construct informs multiple inherent traits that affect its voting system. Firstly, the union is a set of treaties endorsed by sovereign states. While these treaties establish legislative and judicial bodies, they do not administer executive powers to either leaving the essential implementation with the sovereign executives of each member state. Secondly, each nation state joined the European project out of domestic contexts indicating a great discrepancy in incentives and goals among members. Thirdly, the union is primarily an economic confederation that serves as an insurance from mutually destruction. Dedication to it political unity is slim and fractions visible across the member states (Orenstein, 2015).

The inherent political disunity of the EU translates directly into its electoral infrastructure. While EU laws regulates the electoral cycle and the parliament in Brussels and Strasbourg calls for regular elections in accordance, it is at the members states discretion to choose the electoral voting system (Dinas & Riera, 2016). European electoral law provides merely two restrictions to that discretion: 1) proportional representation, be that by means of party lists or a single transferable voting system, must apply, and 2) subdivision of electoral districts is permitted where proportional representation can be guaranteed (ibid). These restrictions, while seemingly not extensive, actually prevent legal loopholes such as the American phenomenon of gerrymandering. In fact, for simplicity's sake, most EU member states have adopted simpler electoral districts assignments for EU elections than present during domestic elections, often using single constituency to cover the entire state (ibid). Nonetheless, there is a significant array of differences in electoral procedures per member state leading to a great deal of authority over electoral executions being left with national ledgers and auditors to report the respective results (ibid). With the notable exception of Estonia, most EU member states conduct analogue elections making digital exposure a negligible concern (Macintosh, 2008). The EU is a multi-party system wherein no singular party is likely to win an absolute majority leading to necessary cooperation regarding legislation (Tömmel, 2014). The parties of the European Parliament are conglomerates of national parties of the same or similar political affiliation. It is the exclusive pejorative of the EU parties to campaign during EU elections, with the explicit exclusion of participation from individual national parties under EU electoral law (Blasina, Tilford, Nevitt & Wisniewska, 2019). They further are bound in their campaigns by the national laws of each member states around political campaigning (ibid). Electoral behaviour devolving out of that systems show two pattern in particular, 1) EU elections are commonly employed as 'punishing traps',

that is voters cast ballots in order to punish national governments in times of low public endorsement of social or economic policy or during economic recessions (Reiff & Schmitt, 1980), and 2) similar to the US two party system, EU elections are often brought down to voter sympathy with EU integration, or in the US casa an analogue choice, making the ballot a yes/no endorsement vote (Reichert, 2012).

According to the European Commission report on the implementation of the action plan against disinformation (European Commission, 2019), Russia has been exploiting the electoral infrastructure of the European Union in the most recent parliamentary elections of 2019. As the EU parliamentary elections are not executed by means of a common system, nor via electronic ballot casting, Russia campaigns have focused on the inherently domestic campaign content of campaigns in EU member states, and more so the electoral behaviour patterns of punishment and pro/anti EU integration sentiment. Russian interference in the EU election consisted of 1) identifying, supplying, and building support for individuals likely to disrupt European unity, usually on the political far-right, 2) Russian banks and business allocated and afforded resources to far-right parties and party members campaigning for MEP seats by means of loans, and 3) sophisticated online bots and trolling was employed to spread targeted disinformation and create poignant biases among national electorates (ibid). The latter in particular reflects many similarities found in the American example. However, the European vulnerabilities lie particularly in the party systems and the disentangled voting infrastructure which caters more to domestic than European campaign affairs.

In light of the European construct, its history, and the exposed vulnerabilities anchored in domestic and autonomous voting procedures in each member states, a few needs become apparent when approaching the voting infrastructure of the European Union. 1) A common voting system. Quality control across all

constituencies can build robustness and afford centralised oversight of the electoral process. 2) Affording provisions and support. A common voting system will require the EU to provide assistance in setting up new physical and expertise infrastructures across the union. Brussels would be the core initiator and provide more assistance in the execution of elections. 3) Centralised auditing. The EU should be more involved in the audit of voter ledgers and ballot oversight to ensure results are treated with equal measure across the union rather than leaving counting up to individual member states. 4) Combat disinformation. A sophisticated counterforce to the comprehensive disinformation campaigns and SMM from Russian troll and bot farms is fundamental is protecting fair and informed elections. 5) Limit foreign involvement. The tunnelling of foreign resources to far-right, or any, parties should be closely monitored and prevented by the European Auditing Board with more consequent actions taken against breaches.

Recommendations

This section synthesises the findings of the SDA identifying intersections of recommendations that apply to both cases explored. Both the US and the EU have federal or confederate legislative bodies that fully or partly supersede national or autonomous states. Furthermore, they share disruption attempts by Russia in their electoral processes in the recent decade. Whereas the American shortcomings lie particularly with its digital ballot casting infrastructure, the EU is challenged by the fragmentation of its election infrastructure. Both however administer agency away from its central institutions to autonomous organs that hold both voter data points and voter ledgers, as well as administer the voting process. In both cases, the lack of centralised oversight causes significant discrepancies the electoral infrastructure robustness. This is the case in US digital and EU analogue electoral systems alike.

Russia exploits the insecurities of electronic ballot casting in the US, and domestic affair driven EU elections in Europe to cast doubt over the legitimacy of the electoral process and cause national partisanship. The literature section of this thesis substantiates the phenomenon of the European voter preference causing an inherent bias that leads to interference exposure (Achen & Bartels, 2017). Likewise does the literature endorse the assumption that merely creating the believe of American electronic ballot casting being vulnerable is sufficient to disrupt the elections (Corstange & Marinov, 2012). The literature further explored how the democratic ideal is fundamentally undermined by SMM. In both the European and the American case social media is employed on a large scale to push partisanship and shed doubt on institutions.

The recommendations consequently overlap significantly in terms of 1) creating centralised oversight, 2) affording more federal or confederate support to member states in equalising their election process, and 3) protecting the cybersphere around the electoral process. These steps in more detail as discussed in each section can noticeably contribute to prevent interference and strengthen the electoral infrastructures at hand.

Assessing the Recommendations

According to the CPC report the following recommendations should apply (McFaul et al., 2019: 24-26):

- Require that all vote-counting systems provide a voter-verified paper audit trail.
- Require risk-limiting auditing for all elections.
- Assess the security of computerized election-related systems in an adversarial manner.

- Establish basic norms regarding digital behaviour for campaign officials.
- Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.
- Retain the designation of election infrastructure as critical infrastructure.
- Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Multiple points become immediately apparent. Firstly, much emphasis is put with the protection and safeguarding of voter data points such as ballots and voter ledgers. Similar conclusions have also been established in the SDA. Forming the basis of the electoral infrastructure, ledgers and voter data needs to be trusted, updated, and safe from manipulation to be robust. This ties in with a second point stressed in the CPC report, namely the need for auditing oversight and more common systems. The recommendations found in the SDA also highlight that quality control is essential in guaranteeing the inherent defence mechanism of electoral infrastructures are in place. Thirdly, acknowledging that restructuring and reforming state specific infrastructures requires considerable assistance and resources, new spaces for federal and confederal support need to be built for these transitions to be executed. Both D.C. and Brussels need more access and involvement in realising far reaching and systematic change in the electoral processes guided by new centralised oversight bodies.

The CPC is one component of the evaluation, its recommendations pertain to the US example but are reflected in the NATO reports as well. According to data collected by the NATO report on government responses, out of the eleven EU member states researched, six had established national taskforces to tackle disinformation

domestically (Belgium, Czech Republic, Denmark, France, Germany, Sweden), while four had no such legislation in place or only had draft bills filled at the point of the research (Austria, Croatia, Ireland, Italy, Spain; Bradshaw et al., 2019). A core finding of the report also addresses the fundamental differences in disinformation prevention and tackling approaches across those member states that have implemented a domestic taskforce (ibid). There is a considerable lack of a common response and cooperative framework across member states. In response to the Russian interference in the European parliamentary election in 2019, the European Commission established an investigation regarding the affairs producing a communication on disinformation prevention in the European Union (European Commission, 2019). As previously established, however, the EU lacks the executive capacity to effectively actualise its policies without cooperation of its member states leaving much of the implementation up to national level decision, such as reported upon in the NATO reports.

Conclusions

Both the SDA and the expert evaluation crystallised sufficient overlap in common responses necessary for modern liberal democracies to strengthen and protect their electoral infrastructures. They further elucidated the core importance those systems play in the proper execution of fair and democratic elections. 1) Uniform electoral system. Any electoral system, analogue or digital, should comply with common qualifiers rather than comply by common limitations. Setting a common system, a) increases the ability for quality control by means of auditing, and b) builds robustness by setting standardised expectations and distributed electoral literacy for increased democratic agency (Mann, 2001). 2) Centralised oversight. Elections should be overseen by a centralised auditing body, as well as a centralised ledger in charge of keeping voter data points safe and updated (Bowler, Brunell, Donovan & Gronke,

2015). Decentralised oversight is prone to discrepancies and more vulnerable to susceptibility attacks that can undermine trust the authority of electoral processes and raise partisanship (ibid). 3) Federal assistance. Autonomous political entities under a unified government should be afforded the necessary resources, expertise, and labour to implement a standardised system regardless of their abilities to do so (Hague, Harrop & Breslin, 2001). The federal authorities should account for existing differences in capacity and capability and be prepared to step in and support constituencies. 4) Cybersecurity. Digital ballot casting and ledger keeping is suspectable to cyber-attacks. Governments need to invest in adequate cyber security walls and preventative algorithms to spot attacks early and decrease risk of potential attacks by means of deterrence (Hoke, 2010). The SDA has shown that attacks need not be successful in order to have the desired effect (Corstange & Marinov, 2012; Mueller, 2019). Therefore, it is paramount to secure the digital borders of electoral infrastructures three steps ahead of potential assailants. 5) Counterforce disinformation. A global phenomenon further explored in chapter 3 of this research, the sophisticated large-scale employment of (social) political bots, sockpuppets, trolls, astroturfing and political redlining significantly undermines the democratic process (Wooley & Howard, 2016). It is therefore important to take comprehensive action to counter these efforts across various media.

Chapter 3: Regulating Online Political Advertising by Foreign Governments and Nationals

As demonstrated in Chapter 1, any substantial effort to combat EI first requires a review of political campaign law, and particularly (paid-for) political advertising

(nowadays a standard practice[3] in electoral races). Data shows that neither states nor media platforms have taken enough substantial steps to inoculate the citizenry and the electoral process from the adverse impact of this shift in the space of political campaigning (Bradshaw et al., 2018; Taylor et al., 2018). The most imminent threat concerns campaign financing and the potential of a narrow range of interests capturing the electoral process. The second issue with online political ads, stems from its use of an immense amount of personal data, allowing it to become highly targeted. On the one hand, this enlarges the scope of disinformation and propaganda campaigns, and on the other, it implies that such practices far exceed the reach of regulatory measures applied to traditional media, the radio and printing-press.[4]

For these reasons, this chapter focuses on building a set of regulatory recommendations aimed at enhancing the transparency of online political advertising, focusing both on campaign financing as well as the use of private data for targeted messaging and content personalisation. Using the cases of Facebook and Twitter, two of the most 'active' social media platforms in the circulation of digital political ads, we attempt to identify the main focal points around which legal procedures should develop to protect free and fair electoral processes. In specific, our proposed solutions include: a) the extension, modification and application of campaign finance laws to meet the news realities of the digital sphere; b) platform providers institutionalising the disclosure, consent and secondary-use requirements for bot activity; c) strict and transparent auditing procedures carried out by a third-party (independent authority);

[3] Figures provided by Analytics Advertising Forecast (2005) show that in Europe, advertising spend has shifted significantly to digital over the past decade.(Tambini, 2017: 13)

[4] Perhaps the most thorough overview of current and emerging trends in political campaigning and the challenges they raise for democracies around the globe belong to Bartlett et al. (2018) "The Future of Political Campaigning"

d) harmonisation and standardisation of accepted practices across all platform providers.

With regard to structure, first, we present and analyse the implications of micro-targeting and personalised content for the realisation of the democratic ideal and thus develop a rationale for why there is a need to increase oversight of digital political campaigning. Second, we proceed to exploring the current regulatory environment around digital political campaigning, assessing governmental and industry responses, surfacing legal lacunas and proposing measures to cover them. Lastly, we discuss the core limitations of our recommendations and point to the direction of future research on the issue.

Push Online Advertising, the Right to Transparency and Freedom of Expression

In section 2 "Democracy in the Era of Disinformation" (p. 14) it was described how targeted messaging and content personalisation systems (CPSs) may be argued to violate Dahl's democratic ideal by: 1) hampering equal opportunity in formulating political preferences (freedom of demand) and 2) creating asymmetries in citizen range of political choice (freedom of supply). Moreover, under a Rawlsian and/or Habermasian conception of the public sphere and our definition of modern liberal democracies, it was established that political discourse should allow "a fair and critical exchange of ideas and values" (Mittelstadt, 2016: 4991). Accordingly, our working assumption, supported by scholarly research on the issue (e.g. Mittelstadt, 2016; Maréchal, 2016; Tambini, 2017), is that unregulated and uncontrolled CPSs and micro-targeted advertising undermine open and evidence-based deliberation among citizens and thus pose significant obstacles for the realisation of the ideal of democratic political discourse.

In order to enhance citizens' informational basis with regard to content personalisation, regulatory measures should focus on protecting their right to transparency[5]. As a minimal theoretical requirement of democratic political discourse, transparency can be defined as "the availability of information, the conditions of accessibility and how the information . . . may pragmatically or epistemically support the user's decision-making process" (Mittelstadt, 2016: 4992). Apart from open and accountable ad financing, this means keeping voters informed about the processes by and degree to which news or ad content reaching them is personalised, and thus making them aware of the type of political agendas and interests influencing the political discourse they are exposed to. At this point, sceptics would perhaps doubt the feasibility of such an idealised version of democratic discourse. Taking these concerns in account, our measures "would not necessarily prevent this influence, but rather inform actors of its existence and the informational blind spots personalization sustains by default" (ibid: 4994).

To understand how opaque content personalisation techniques, imply a low level of user awareness and generate vast informational asymmetries characterising 'the range of democratic choice' between each citizen recall the discussion in Section II: "the Role of Social Media Platforms in Data-driven Political Campaigning". This showed how ad personalisation evolved from serving commercial purposes to a powerful political campaigning tool as office-seekers, candidates, political consultants and campaign teams recognised the value of push advertising's ability to target users according to their demographic group, interests, web traffic, personal details and any

[5] All three of our main secondary data sources show that (self-)regulatory initiatives must include a monitoring of digital political campaigning by increasing transparency of its financing as well as its use of automation systems and private data (Bradshaw et al., 2018: 6-7; Taylor et al, 2018: 7, 11-12; McFaul et al., 2019: 27-33)

other type of private, politically relevant information that can become available through the use of sophisticated data-mining techniques (Tambini, 2017).

Notwithstanding its high political value and usefulness there are three issues with this delivery of personalised content. Firstly, it is not done in public and therefore it is not subject to monitoring or journalistic scrutiny or fact-checking (ibid). This enlarges the scope of disinformation, as false or inaccurate content can be spread without any public oversight and/or commitment, accountability on behalf of the politicians or candidates. Secondly, evidence from past election show that for optimisation purposes online political advertising targets the 'undecided or swing' fraction of voters (ibid). Heterogeneous content delivered to different strands of citizens, creates larges inequalities in terms of available political information as entire spectrum of political views/stances are deprived from those voters that don't belong to the 'key demographics' targeted by political campaign teams (redlining) (ibid). In simple words, decided voters are trapped into eco chambers and filter bubbles and exposed to ads that re-enforce their already held views whereas undecided ones are exposed to custom-made, manipulative messages. This human-caused restriction on the flow of information is damaging for the public sphere as it exacerbates polarisation (ibid).

Before proceeding to the next section, an important disclaimer about the regulation of online political advertising must be put forth. That is, online political ads belong to political speech practices and thus regulating them raises concerns over free speech (Brannon & Whitaker, 2020). Therefore, any regulatory initiative should aim at protecting the 'democratic ideal' and promoting citizen autonomy in making voting decisions but at the same time respecting the role of the internet in the public sphere of political discourse (GPO, 2019).

The Current Regulatory Environment of Digital Campaigning

In this section, we present and elaborate on our argument that there exists a joint responsibility between private and public actors in devising, implementing and monitoring rules and standards with regard to digital political campaigning. In doing so, we first analyse Twitter's and Facebook's policy with regard to paid-for political ads. After the self-regulatory priorities for platform providers are established, attention is shifted towards those of governments. We propose that the latter should take regulatory action to delimit the legal framework upon which private platforms should base their self-regulatory initiatives with regard to both the financing of online political ads and content personalisation/targeted messaging. At the same time, monitoring compliance to these standards by means of third-body, strict auditing procedures, is also recommended as a vital state duty towards protecting and promoting citizen free and equal democratic choice.

The Private Sector's Self-Regulation: Twitter and Facebook

In the USA, the plethora of political speech acts take place in digital platforms and are only governed by Terms of Service (ToS) agreements (Wooley and Howard, 2016). As a result, social media companies assume differing policies according to their main income-generating functions and commercial interests. Twitter, for instance, has completely banned online political advertising, whereas, Facebook cites 'freedom of speech' rights to deny censoring politicians (Financial Times, 2019). The former has the most elaborate and explicit guidelines when it to the use of bots and automation systems (Maréchal: 2016). In its "Automation Rules and Best Practices" the microblogging platform lists the types of automation systems (bots) that are prohibited, including amongst other things, the requirement of express consent for distributing user content, the ban of hashtag spamming and favoriting (Twitter, 2017).

These rules are meant to hamper the use of bots designed to actively participate in public deliberation by "harassing users, retweeting content produced by predetermined users, hijacking hashtags or other curated conversations, or impersonating public figures or institutions" (Maréchal, 2016: 5023).

On the other hand, Facebook's guidelines seem designed to protect the platform's ad income by placing restrictions on reaching user without purchasing Facebook ads or paying royalties to the company when doing so; rather than safeguarding public discourse and democratic processes from the malicious use of its services (Facebook Platform Policy, 2020). Whereas, many commentators would support that Facebook has every right to to protect its profits, we do identify a lack of a clear connection with citizen's digital rights, and more importantly, transparent ToS (Maréchal, 2016). The company's 'Community Standards' (2020) show a more relevant consideration of the most basic issues of authenticity, privacy and security, but still lack a clear connection with transparency at the algorithmic level (with regard to personalisation methods and criteria) as well as when it comes to financing of online political ads.

At this point, recall Taylor's et al. (2018) finding that social media platforms' failure to protect digital rights and combat EI due to the 'vague language' of ToS agreements and policies and the lack of their 'enforcement'. This becomes evident in the case of Twitter, whose policy contains prohibitions on political advertising pertaining to content and disclosure requirements, eligibility restrictions and so on, but lacks the instruments and schemes to effectively enforce them (Tambini, 2017). From this realisation an important question arises that merit further discussion: Why should private companies impose strict self-regulatory restrictions on their services in order to enhance transparency?

The most obvious answer is that as in many industries with governance gaps and issues, private adherence to publicly-set standards is promoted by soft-law instruments such as the "UN Guiding Principles on Business and Human Rights" that impose a corporate responsibility on companies to respect human rights (Maréchal, 2016; Bayer et al., 2019)[6]. Despite the non-binding legal nature of these voluntary standards, they do serve to connect these companies' function with a normative obligation to self-regulate. In this light, this provides a partial respond to Susskind's (2018) argument that relying on private companies to self-regulate is problematic due to a lack of moral and legal accountability. Partial because strict enforcement would require these companies to go against their private nature by prioritising the autonomy of voters over theirs. Therefore, it would be potentially very dangerous to rely *solemnly* self-regulation without some sort of independent monitoring. For this to be possible, constructive dialogue between these companies and public authorities needs to be pursued, and the cooperation of both sides guaranteed.

The Public Sector: Benchmarking and the Limits of Public Regulatory Reach

Extending Campaign Finance Controls to the Digital Sphere

As demonstrated in the opening of this chapter, regulation aimed at ensuring free, fair and vigorous democratic processes, should have a dual focus: First, facilitate the political preference formation process by promoting pluralism/curbing tribalism and political inoculation. Second, as a measure against 'the capture of the election

6 *"The corporate responsibility of all business enterprises to respect human rights requires private entities: to avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur, as well as to seek to prevent or mitigate adverse human rights impact that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts"* (UN Office of the High Commissioner, 2011)

process by a narrow range of interests' relevant legislation should attempt to limit the role of money in the electoral process/outcome (Tambini, 2017). Recalibrating campaign finance controls seems necessary since current legal stipulations do not account sufficiently for online spending and advertising (ibid). Transparency seems, again, to be key: if platforms don't publish detailed accounts of who paid for what, then it's impossible to monitor spending on online political ads.

Several countries have extensive laws governing campaign spending, messages, scope and timing (Bradshaw et al., 2018). The overarching objective of campaign law is to protect their integrity and ensure they are free and fair (McNeice, 2019). Why then, haven't governments proceeded in extending these laws to apply to cyberspace and digital political campaigning? Recall that Skierka (2014) attributes the scarcity of state-based responses to a: 1) lack of digital literacy, 2) lack of expertise fluency to identify areas of vulnerability, and consequently 3) ability to source adequate IT expertise. Even though 1 might still hold, we believe that (2) and (3) have improved significantly during the past decade, making a number of revisions available.

Our research shows that such an extension would first seek to modify traditional filter mechanism to apply to the online world; platforms are intermediaries and should be subject to the same standards that newspapers (and other traditional media) are when it comes to political campaigning. This means that values such as fact-checking, truth, separation of fact from opinion need to be institutionalised into regulatory mechanisms meant to ensure compliance of social media providers to the high-standards of journalistic ethics (Tambini, 2017). Second, laws over campaign funding are strict in most states, and most of the times requires full transparency on behalf of campaigners with regard to funding and and the origin of campaign communications (ibid). For instance, noting the printer and funder of leaflets, should

be replicated to noting the creators and funders of online political campaigning. At the same time, statutory limits should be imposed to the volume of/spending on advertising vis-a-vis referendums, regional, national and local elections (GPO, 2019).

Best-Practices: Ireland and the USA

A prime example of state-based regulation of online political advertising is Ireland. The Irish government approved in November 2019 a proposal to regulate online political ads by requiring, amongst other things, explicit labelling and displaying of key information in a clear and conspicuous manner (McNeice, 2019). Ireland's initiative supports our proposition of a joint effort as it acknowledges that the industry has taken 'steps to combat' the malicious use of social media but that regulation shouldn't be left to the market alone (Ibid). To put its actions where its mouths is, the government supported the partnership of an independent fact-checking network (TheJournal.ie) with Facebook to review stories, photos and videos for accuracy and false content (Tannam, 2018). Content deemed inaccurate or misleading, will be ranked lower on the platforms news feed, hence, reducing the rate of its distribution and the size of its potential audience (Ibid). Moreover, in regard to increasing accountability and transparency, the aforementioned Ad Honesty Act in the USA, would also help "extend federal campaign finance law disclosure and disclaimer requirements to online platforms for paid internet and paid digital communications and would require online platforms to maintain a publicly available file of requests to purchase certain political advertising" (Brannon & Whitaker, 2020: 1). Under similar lines the "Internet Ad Disclaimers Rule Proposal" provides a comprehensive and detailed enough framework for setting specific requirements for attribution statements (disclaimers) (Weintraub, 2019).

Recommendations

The first measure we recommend is a revision and re-adjustment of campaign financing laws to illuminate the 'grey areas' of digital campaigning funding. This requires action from both social media platforms and governments. The former is required to publicly disclose all available information with regard to purchasers of ads as well as visibly state the origins/sources of every article, video or photo that could be regarded as an object of political campaigning. The latter should proceed at imposing restrictions on the number of ads that can be purchased from the same funding source or the amount of money a single source can spend on political ad content. In addition, a measure that is worth further consideration depending on the national context of each country, would be the complete banning of foreign funding of domestic electoral campaigns.

The second recommendation aims at accounting for the threats that micro-targeting and content personalisation pose for autonomous voting and political decision-making at the citizen level. It includes three fundamental rules for the use of bots and a stipulation to increase citizen knowledge of content personalisation methods and criteria. So, platforms providers should take action to: 1) make sure all bot accounts are clearly identified as such (disclosure rule); 2) ensure that no bot initiates contact with human users without their consent and 3) ensure that no bot owner uses information accumulated about users for purposes other than those already indicated (secondary-use rule) (Maréchal, 2016). Apart from monitoring compliance of private companies with these rules, we propose that governments should compel private companies to share more accurate, accessible, and comprehensible information about the influence of personalisation systems handling of private data (Mittelstadt, 2016). This measure would support each citizen's 'right to transparency' which places, at a minimum, a requirement of awareness vis-à-vis the

profiling process and the values prioritised in content displayed to them; meaning, of how political preferences are being influenced or externally shaped (ibid).

The third recommendation is the establishment of a third-party. regulatory body, or independent authority in the form of an interdepartmental committee that will be responsible for autonomously leading and coordinating the governance of online political advertising (especially in times prior to big electoral events) by structuring, adjusting and validating auditing procedures. The latter would serve to supervise social media platforms for algorithmic and ad financing transparency (Mittelstadt, 2016). At the same time, it would increase the accuracy and effectiveness of regulation by providing a clear procedural record of platforms that are heavily involved in political deliberation as well as allow to classify algorithms according to their 'capacity' to predict and explain, i.e. to profile voters (ibid). Even though it will have no legislative power it can serve to reinforce democratic capital by serving as a mediator between governments, private companies and citizens as well as actively and practically raising the awareness level of the latter.

The fourth advised measure calls for a harmonisation and standardisation of accepted practices of online political advertising across all major social media platform providers. As it stands, it falls under the discretion/judgement of individual companies to decide the precise content of their ToS, privacy policies, guidelines and other types of documents setting the rules of a platform's use. Obviously, such a legal constellation does not allow a holistic, thorough and effective regulation of the industry's treatment of digital campaigning. A useful tool for assisting companies to evaluate the socio-political impact of their technologies and align their efforts to mitigate potential harm, can be found in the Ranking Digital Rights (RDR) project. This framework consists of 31 evaluation indicators that aim at measuring the "company's overall understanding of the role it plays in mediating its users'

participation in the public sphere, and its commitment to enhancing, rather than restricting, user's freedom of expression and privacy" (Maréchal, 2016: 5028).

Assessing the Recommendations

Our recommendations cover all the conditions that the CPC report offers as foundations for a regulatory response towards online political advertising (McFaul et al., 2019: 27-35). The only point we deliberately omitted is the limiting of the targeting capabilities for political advertising. We reckoned this would require even more intervention into the conduct of private social media platforms, which the latter is unlikely to accept without heavy resistance[7]. Moreover, our advisory action plan is aligned (but also expands upon) the state initiatives Bradshaw et al. (2018) catalogue surrounding increasing political advertising transparency (p. 7).

However, we did identify a number of obstacles on the feasibility of our recommendations' implementation. First, it seems to be important to harmonise expectations from private firms across different nations. It would be unrealistic and potentially dangerous to require social media platforms to maintain materially different policies with respect to different governments in varying political contexts (Tambini, 2017: 37). Second, CPSs are usually copyrighted and unavailable to the public, and affording too much algorithmic transparency can harm competitive advantage, national security and/or privacy (Mittelstadt, 2016). As Susskind (2018) also points out misaligned incentives, render platforms providers unwilling to loosen intellectual property protection and open-up their data libraries to third-party auditors (p.10-11). Moreover, CPSs "can function opaquely and be resistant to auditing because of poor accessibility and interpretability of decision-making

[7] Recall that the regulation of online political advertising is already hindered by the complexity characterising algorithmic function, the tension between censoring political speech and freedom of expression, as well as transparency and intellectual property protection.

frameworks" (as Mittelstadt, 2016: 4992). Potential solutions to this issue would be complementary regulation on data privacy and security that would require from data processors to share and explain their logic of automated decision-making when asked to do so (an example of such a scheme is the EU's GDPR) (ibid).

Third, when it comes to the transparency of digital campaign financing, the structure of digital payments raises difficulties for tracking the source of funding, as a lot of digital spending occurs via intermediaries such as advertising agencies and/or consultancies (ibid). To tackle this issue, governments should appraise the regulatory gaps and 'grey areas' regarding the content, provenance and jurisdictional scope of online political advertising (ICO, 2018). To this end the creation of an open data archive on digital political advertising would most probably assists in the analysis of data and this in increasing public scrutiny (ibid).

Conclusions

The associated threats of insufficient control of the funding, content and methods of modern digital political campaigning for free and fair elections and democratic deliberation are multi-fold and arguably quite alarming. In this chapter we attempted to address the question of enhancing the regulatory oversight of online political advertising by analysing the self-regulation policies of two of the biggest service providers, Facebook and Twitter, as well as the leading relevant measures national governments have undertaken to improve the legal (and moral) supervision of this practice. Our main finding is that the creation and serving of digital political ads involves a complex interplay of private and public actors, and thus, any effective monitoring/regulatory strategy would need to couple public benchmarks and auditing procedures assisted by company-oriented insider advocacy, with a strengthening of self-regulation aimed at 'opening up' these companies to public

scrutiny with regard to content personalisation and micro-targeting. At the same time, we argued that governments need to extend public oversight of political campaign finance to the digital context while platform providers should undertake steps to meet certain transparency requirements surrounding their 'hosting' of political ads and the algorithms used in CPSs. To do so, but also to enable a more thorough overall supervision of the practice, we called for an effort to harmonise and standardise rules and policies regarding political advertisings across social media platforms.

Chapter 4: Confronting Efforts at Election Manipulation from Foreign Media Organisations

Exploring the ever-increasing ability of foreign media to distribute information among domestic electorates and directly influence the democratic debate in sovereign nations, this chapter addresses the challenges and potential threats such a globalised capacity poses in context of the Age of Disinformation. This chapter opens by drawing the lines between domestic media agents and foreign media agents in the context of a national media landscape. Understanding where the differences matter, helps define the spheres of responsibility and ability to counter disinformation campaigns by overt media outlets (Louw, 2013). Once again Russia offers a prime example with its state-sponsored, and state-controlled, media channel RT (Stengel, 2014). Set up as an instrument for the Kremlin, RT provides news on international affairs from a Russian regime perspective to international audiences in English, German, French, Arabic, Spanish, and Russian (Orrtung & Nelson, 2018). To expand on the Russian news campaign, the second example concerns the Global Times. The Global Times is a less overt example of a foreign media outlet influencing domestic affairs abroad. The Chinese tabloid provides international news from a nationalistic and state scripted perspective with the intend to portray the People's Republic's policy in a less critical

and more support light on the international stage (Huang, 2016). Where RT clearly states its intent to provide an alternative perspective as a 'pro-Russian' news channel (Dowling, 2017), the Global Times brands itself more as China's international new outlet communicating 'facts and truths' where Western media is not (Huang, 2016). The SDA will be conducted at hand of the RT ad Global Times examples, elucidating necessary actions to limit their influence and oversee their actions in a domestic context. As with previous chapters the hypothesis will be tested against the expert evaluation and in summation recommendations be consolidated in the conclusions section of this chapter.

Domestic vs Foreign Involvement in Media Landscapes

While disinformation and SMM has been addressed as a predominantly foreign issue, cases such as the Cambridge Analytica scandal have shown there exists fertile ground and willing actors within domestic media landscapes happy to lead dis- and misinformation campaigns in lack of adequate legislation (Sullivan, 2020). As the literature section established there has been a persistent shift away from tradition news sources to digital media (Mitchell et al., 2016) affording alternative news outlets spaces to compete with established media (Algavy & Al-Hanaki, 2014). This modern trend that set on with increased digital literacy and openly accessible tools to unaccredited individuals and groups (Heft, Mayerhöffer, Reinhardt & Knüpfer, 2019), has been most noticeably identified for the first time in context of the 2016 US presidential election (Gallagher, 2019). Domestic election fraud and intentional manipulation and corruption of the electoral process and the independence of the electorate have long been studied as an underlying internal threat to democracy (Alvarez et al., 2009). Yet is was the 2016 elections that introduced the issue of domestic partisan propaganda. The American news outlet Fox News, owned by

controversial Australian-born American media mogul Rupert Murdoch, had long been identified as the flagship outlet for conservative political thought in the United States (Collins, 2004). While Fox News has been known for its strong republican bias since going on the air in 1996, it was not until the 2016 Trump electoral victory that affairs turned drastically towards domestic propaganda and misinformation (Arceneaux, Dunaway, Johnson & Vander Wielen, 2020). Fox News has been identified as a major driver in the spread of misinformation and in part disinformation often in context of defending the Trump administration's policy agenda (Gallagher, 2019). While Fox News has been a major subject in identifying the growing disparity in journalistic ethics and media standards in the United States, their influence has been largely supported and given undue credit by independent far-right news outlets such as Breitbart (Benkler, Faris & Roberts, 2018). While Fox News and Murdoch's News Corp face considerable public scrutiny over financing and political influence, outlets like Breitbart usually do not in the same way (Mayer, 2017). In fact, channels like Breitbart disseminating far-right thoughts and disinformation, are often financed by private donors (ibid). This makes it difficult to hold them accountable to the same extent that you can large cooperations. However, many of these outlets are domestic and can be limited in potency but domestic legislation. The matter becomes a lot more complex when dealing with foreign agents or state aligned actors, as described in the following sections. The core difference lies essentially in being able to 1) track financing and the various influences of different actors in disinformation distribution, 2) holding accountable those publishing and disseminating harmful content such as SMM and disinformation, 3) limiting reach and traction by domestic prevention measures, and 4) having news channels answerable to the public. None of these control mechanisms are possible in the same way when dealing with foreign threats, requiring a much more sophisticated approach.

RT: Russia's Trojan Horse

According to former Secretary of State John Kerry, the Russian Federation runs the most effective and most overt foreign media channel purposefully designed for meddling in foreign affairs and disrupting democratic discourse by disseminating false or construed information intently in line with Kremlin narration (LoGiurato, 2014). During a visit to RT studios in Moscow in 2013, Vladimir Putin clarified, "When we designed this project back in 2005 we intended introducing another strong player on the international scene, a player that wouldn't just provide an unbiased coverage of the events in Russia but also try, let me stress, I mean – try to break the Anglo-Saxon monopoly on the global information streams. [...] We wanted to bring an absolutely independent news channel to the news arena. Certainly, the channel is funded by the government, so it cannot help but reflect the Russian government's official position on the events in our country and in the rest of the world one way or another. But I'd like to underline again that we never intended this channel, RT, as any kind of apologetics for the Russian political line, whether domestic or foreign." (Fisher, 2013). Today RT offers international news coverage from a Russian perspective in English (since 2005), Arabic (since 2007), Spanish (since 2009), German (since 2014), and French (since 2017), and runs two dedicated channels with a local focus in the US with RT America (since 2010) and the UK with RT UK (since 2014; "About RT", 2020).

Established in 2005 as Russia Today, RT is registered as an autonomous non-profit organization. As reflected in the aforementioned statement by Vladimir Putin in 2013 (Fisher, 2013), the channels official intended is to provide objective news coverage from angles alternative to established news networks dominated by Western media ("About RT", 2020). However, the channel is being financed by the Federal Agency on Press and Mass Communications (FAPMC) of the Russian Federation

under the Russian federal budget implying a significant pressure to comply with government censorship (Yablokov, 2015). Yet, in an interview with Ekho Moskvy reported on by The Age in 2005, Svetlana Mironyuk then Director of Ria Novosti, Russia's state-operated domestic news agency and former prime news representation internationally, stated that "It is very difficult to imagine that the channel could earn itself a good name, good ratings and an audience if it was a tool of blatant propaganda." (Osborn, 2005) She continued, "The presidential administration is not managing this project. It is aware of it." (ibid) The official stance and image RT portrays is in direct conflict with many of the facts surrounding its existence. One example being that FAPMC officials have also allegedly fosters close ties with Internet Research Agency (IRA), also known as Glavset (Dawson & Innes, 2019). The misleading name actually denotes a private company that has become known as the 'troll factory' behind Russian interference attempt in global elections particularly the US elections of 2016 (Bastos & Frakas, 2019). While its links to the Kremlin have been repeatedly denied, many former employees have been persecuted in context of the Mueller investigation in the US (Weiss, Cranley, & Panetta, 2020), and content originating from its offices in Russia, Ghana, and Nigeria been featured in context of RT coverages and on Sputnik, another youth-oriented state-administered Russian media outlet (Ward, 2020). An independent investigation by Facebook, complemented by the Mueller Reports, has shown that between 2015 and 2017 over $100,000 were spent on over 3,500 advertisements disseminating false or manipulated content on Facebook and its co-owned platforms such as Instagram alone by fake accounts originating from the IRA (Satariano, 2019). Similar numbers are not known for media platforms such as Google or Twitter, but estimates assume those to mirror the efforts identified on Facebook (ibid).

Nonetheless, RT's official hard-line image building campaign around its supposed stance on objectivity and providing alternative news sources has won the channel great popularity in many parts of the world such as Africa, South Asia, and Russia where antipathy towards Western media is strong and sentiments prevail that major established news providers do not accurately portray the situations in these countries (Erlanger, 2017). While there is a slight correlation between RT's popularity and low levels of press freedom and civil liberties (Kokolis, 2020), its success is a lot more complex. In 2010, RT was the second most watch foreign news channel in the US after BBC (Rizvi, 2010), being particularly popular with young urban demographics taking the number one spot as most watched foreign news channel in New York City, Washington D.C., Chicago, Los Angeles, and San Francisco in 2012 (Russia Briefing, 2012). In spite of widely covered disinformation scandals involving RT pro-Kremlin reporting in the Syrian civil war, the Russian occupation of Crimea, the MH-17 disaster, the European Migrant Crisis, among others that resulted in multiple high-profile on the air resignations of non-Russian RT staff (Carroll, 2014), RT has only been strengthened its popular position as an 'opposition network to the establishment' (Semple, 2018; van Zuylen-Wood, 2017). Similar trends have been observed in Trump supporters whose support levels have only become more adamant with cycles of public scrutiny and exposure of Trump policy and actions (Pettigrew, 2017).

RT remains openly accessible and uncensored in the Western hemisphere causing considerable concern as to the effect of its broadcasting, and the deeper networks such as with IRA its presence might be supporting. Consequently, since 2017, the United States Department of Justice (DOJ) decided to consider the broadcasting cooperation RT America as a foreign agent and requires it to register with the DOJ under the Foreign Agents Registration Act (FARA; Chappell, 2017). As

both the Mueller and Facebook investigations revealed, the FARA does not by far provide sufficient transparency on RT operations in the United States. In fact, few other countries have consistent and comprehensive legislative frameworks in place to address the operations of foreign media in domestic media landscapes (Packard, 2013). Moreover, most countries lack adequate approaches to counter domestic disinformation production and spread, as the example of Fox News in the US demonstrates (Marsden, Meyer & Brown, 2020). RT and its increasing popularity even in face of consistent scrutiny by established media outlets, proves that 1) more transparency by foreign media agents is require to permit operation alongside domestic media, 2) the legislative frameworks, such as the FARA, need to be expanded to address sophisticated networks of disinformation by means of stronger disclosure measures, and 3) substantiate legal consequences for breaches of domestic law by foreign media agents.

China's Global Times: Nationalistic Ambitions Broadcasting Live

Whereas RT markets itself as a an 'objective, alternative source of news' to the Western establishment, contrary to its consistent promotion of covert disinformation attempts and journalistic manipulation, the Global Times exploits a very different asset both RT and Russia are officially lacking: soft power. China's economic rise on the global stage in the twenty-first century has given wind to its political gravity (Leal-Arcas, 2011). The People's Republic of China under authoritarian leadership of the Chinese Communist Party is exerting great confidence in its increased global capacity (Shambaugh, 2013). To grasp the role of the Global Times, it is important to understand China's foreign policy operations of which the tabloid is an important element. China knows that the majority of its geopolitical power lies with its economic power (Andornino, 2017). In 2013, China launched its Belt and Road Initiative (BRI);

a project described as the 'twenty-first century Silk Road' by Chinese president Xi Jinping (Kuo & Kommenda, 2013). The global development strategy involves nearly 70 different nations and entails Chinese foreign investment in infrastructure to ensure developed maritime and land trade roads from and to mainland China (ibid). However, the BRI is not merely a development project. Many of the initiatives that require large scale financial foreign investment by Chinese business and public organisations come with significant leverage (Nordin & Weissmann, 2018). The BRI strategy in Africa has been described as 'Chinese neo colonialism', as China offers much needed capital investment in return for exclusive trade rights, access to resources, and exclusive partnerships with governments (Kelven, 2019). Many nations particularly in Africa and South East Asia are happy to accept Chinese investments as they come without many of the monetary and fiscal obligations imposed by IMF or World Bank loans, as well as requirements to improve on certain civil and human rights issues domestically such as is often the case with development aid from Western MLDs (Van Mead, 2018). Long term consequences of the global shift in diplomatic relations are yet to be seen but the result of these geopolitical expansions evident already today are: 1) softened international pressure on China regarding its territorial ambitions and domestic civil liberty records, 2) increased support in international organisations, and 3) strengthened domestic confidence (Kelven, 2019). Consequently, the BRI has been much criticised and scrutinised by established Western media, and its 'threat narrative' to global order contributed to the escalation of the American Chinese trade war in 2018-2019 (Liu & Woo, 2018). Similar examples have been observed in the case of Asian Infrastructure Investment Bank (AIIB) established in 2016 as an alternative to the World Bank (De Jonge, 2017). Even though it had been heavily criticised by Western media and Western-led international

organisations such as the UN, it was eventually joined by many leading Western European countries and Canada (ibid).

The Global Times was established in 1993 as a Chinese language tabloid reporting on international affairs. The intention was to provide and opening and rapidly developing China with a media gateway to the globalised world it was striving to join (Zeng & Spark, 2019). It was only as the Chinese economic miracle set in that Beijing's focus and the tone of the newspaper changed (ibid). In 2009 the Global Times started an English language version with extensive online services. The English language coverage focuses heavily on Chinese domestic policy such as the Hong Kong protests, the South China expansion, and Beijing's position on the Republic of China (Taiwan; ibid). Much like RT the Global Times has set the goal to disrupt the Anglo-Saxon media dominance in established news outlets to provide a more Chinese perspective on global issues. However, in the same line as RT the Global Times employs its global voice to often present and promote false, manipulated, and government-narrated information (Tharoor, 2017). The Global Times actively undermines and discredits US foreign policy while simultaneously strengthening a China centric narrative that is catching on with many of its geopolitical partners bound to Beijing by means of the BRI and the AIIB (Zeng & Sparks, 2019). The efforts of the Global Times are much more overt and have yet to show deeper links to wider disinformation campaigns such as in the case of RT and the IRA. This makes it difficult to force accountability for disinformation because the matter of the Global Times operating in the United States, or any foreign media landscape, does not constitute an issue of transparency but rather of accuracy. Legislative responses have so far been hesitant to implement legal consequence for the spread of dis- and misinformation by means of official broadcasting due to a general legislative fear of limiting civil liberties by introducing journalistic censoring (Suzor, 2019). Examples such as Singapore's

Protection from Online Falsehoods and Manipulation Act (POFMA) of 2019 contribute to that fear. The tone of the Singaporean government indicates that POFMA can be used to persecute media outlets, journalists, and individuals who disseminate disinformation in the eyes of the government (Newton, 2019). There is considerable suspicion internationally that the POFMA will be applied to silence opposition and censor domestic media critical of the government (ibid).

The example of the Global Times shows that an effective response to foreign media distributing dis- and misinformation is not merely a matter of transparency but of equipping the public with an adequate literacy to respond to these threats. The Global Times might not particularly target US elections but certainly aims to raise distrust among the American and Western electorate, which will inevitably be reflected at the ballot box. While there is a call to limit the ability of foreign networks by means of disinformation legal consequences as in the case of RT's illicit covert campaigns, those might not ring true for cases such as the Global Times. Policies addressing this kind of manipulation must carefully balance the line between censorship and protection. Therefore, recommendations must include increased transparency not just for the government but also for the individual citizen.

Recommendations

In light of the examples provided by RT and the Global Times this section is able to shape the outline of the recommendations necessary to confront efforts at election manipulation from foreign media organisations.

The case of RT showed the intent manipulation and disruption of a democratic process by a state-aligned actor. With much lacking transparency and many unexplained links that only occasionally come to light in context of legal investigations such as the Mueller reports, the SDA on RT elucidates the needs for

more transparency obligations for foreign actors in domestic media landscapes. Furthermore, the supportive roles of organisations such as the IRA press urgency to involve the private sector in setting norms and standards that prevent the spread of SMM. It is not sufficient to leave that authorship to business alone. Rather it should be a unified effort of legislators and business experts to build a common framework of preventative measures.

Legal pressure alone however cannot address wider underlying damages caused in the electorate as the popularity of RT in face of continuous scrutiny and scandals has shown. Moreover, the Global Times shows that even when media outlets are predominantly transparent about their intent and content, dis- and misinformation still easily spreads. Measures must therefore also address responses that support the individual to engage in informed media consumptions. The government can assist by setting regulations that will increase literacy and help spread increased awareness about the issue of SMM and disinformation.

Assessing the Recommendations

Many of the recommendations do reflect in the three core recommendations named in the CPC report (McFaul et al., 2019: 40-41), which states the following responses as necessary:

- Require greater disclosure measures for FARA-registered foreign media organisations.
- Mandate additional disclosure measures during pre-election periods.
- Support existing disclosure measures of specific social media platforms.

The recommendations of the CPC report place a great emphasis with the legal regulations that concern disclosure and transparency of foreign news agencies. This makes particular sense considering that the CPC report is aimed at a US context where the case of RT has caused significant pressure to legislate on its activities in the country

(Gerstein, 2017). It is in the third recommendation addressing social media that the CPC touches upon the issue further explained in its chapter on state aligned actors wherein it expands on the following regulations (McFaul et al., 2019). The chapter emphasises digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.

These recommendations do not only cover those found in the SDA but go beyond by suggesting far reaching systematic reforms that would affect even the school system. The recommendations are further meant to address the behaviour of state aligned individuals rather than media organisations such as RT or the Global Times. Consequently, it is difficult to translate them into elements that can be integrated into the findings of the SDA. As the aim of this research is to build benchmarks of policy recommendations, the recommendations themselves can also not afford to be to narrow risking to sacrifice applicability across a wide range of national contexts. Nonetheless, the CPC confirms much of the recommendations identified in the SDA, and in the absence of specific recommendation in the NATO reports, they also build the most fertile basis for proper formulation.

Conclusions

The SDA in synthesis with the expert evaluation were able to bring together a holistic picture of the recommendations required to tackle efforts of election manipulation by foreign media organisations. 1) Transparency and Disclosure. The main issue of any media organisation operation in a national media landscape is their adherence to journalistic codes and ability to prove if necessary, the integrity of their work to authorities. With foreign media organisations it is even more so important to understand the content and sources of their reporting in order to place them adequately in the existing media stream. It is therefore paramount that foreign media

organisations are obliged to disclose their operational structures and be transparent about their operation under existing legislation (Persily, Metzger & Krowitz, 2019). 2) Build literacy. The main damage of misinformation, as established in the literature review of this paper, lies with the partisanship that is created among media consumers (Corstange & Marinov, 2012). Sophisticated diversity in digital manipulation is easy created but less easily identified (Berghel, 2017). It should be the government's responsibility to ensure that distributors of false and unverified information are labelled and that it is easy for the individual consumer to identify potentially malicious content. 3) Public responsibilities for the private sector. The private sector in and of itself has neither got the mandate nor the capacity to tackle a nationwide campaign against SMM and disinformation. The government must therefore benchmark mechanism to retrain the ability of foreign media to distribute targeted mis- and disinformation on social media platforms. It is important that these measures include mechanism for reporting and oversight to keep track of traffic and potentially hold the distributor legally responsible. 4) No censorship but independent oversight. A body consistent of elected officials, government and private sector representatives, as well as selected experts should be formed to evaluate when and where lines of disinformation have been crossed in order to support the potential persecution of these cases.

Chapter 5: Establishing International Norms and Agreements to Prevent Election Interference

There is widespread agreement among experts, policymakers and politicians, that any effort to combat EI at the national-level (revision of political campaign laws, fostering of media literacy and so on), can only deliver suboptimal results without a complementary international normative framework that clearly delimits acceptable

and appropriate behaviour in cyberspace (Fidler, 2017; McFaul et al., 2019; UN General Assembly, 2013; 2015). Despite this divergence of views on their necessity, related scholar testimonies and ad-hoc studies unanimously recognise a mismatch between the growth of the internet and the elaboration of universal, well-defined and agreed-upon norms that would nudge (public and private) actor behaviour towards abiding to some generally accepted standards (ibid). A fact that after consideration compels us to include in the analysis an exploration of the current shape and forms of the global governance of EI. We argue that norms by themselves do no provide sufficient incentives to deter non-compliant actors from engaging with EI. Given the highly premature state of international norms applicable to this phenomenon –if they are to have any significant impact upon the actions of states and companies- they need to be institutionalised into domestic legal instruments with the capacity to impose effective, proportionate and dissuasive sanctions on deviants. Following this, bilateral or regional legally binding agreements should be signed, criminalising the use of illegally acquired information (be it citizen's private data or confidential government documents) for political purposes. Succeeding these two policy changes and assuming they are proven successful, then, foreign EI operations can potentially be regarded as an object of international law.

In order to support and help materialise this policy framework, we forward three recommendations: First and foremost, the expansion of the scope of interpretation and application of certain international legal principles relevant to EI. Second, the utilisation of International Humanitarian Law (IHL) to develop international norms (and gradually hard law) regulating and restricting cyberwarfare directly or indirectly targeting core political processes and outcomes. And finally, the introduction of universal guidelines for social media companies focused on reducing the likelihood of their (active, tacit, direct or indirect) involvement in EI operations.

We start by establishing the significance of norms for global governance before determining the ones that are relevant to EI. Then, we proceed to discussing their applicability and usefulness in implementing international law and safeguarding democratic processes. Conclusively, with proposing future directions for developing more intricate and germane international standards of appropriate behaviour in the cyber realm, and particularly vis-à-vis building a universal legal and moral benchmark against which actions involving EI can be assessed.

The Constitutive and Regulatory Effects of Norms on EI-relevant Actor Behaviour

A norm is defined as a generally accepted value that circumscribes a standard of appropriate behaviour. In international relations theory, norms are found to have both 'regulatory' and 'constitutive' effects. The former refers to their utility in constraining or regulating states by altering the incentives that shape their behaviour (Hobson, 2000: 147). This conveys a 'logic of consequences' which "attributes action to the anticipated costs and benefits, mindful that other actors are doing just the same" (Baylis et al., 2014: 159). The latter concerns their function as rules that define the identity of actors, meaning that they "specify what actions will cause relevant others to recognize a particular identity" (Viotti & Kauppi, 2012: 286). Behind this, a 'logic of appropriateness' is implied, in which identities, rules, and norms fuse in prescribing a certain range of legitimate state actions.

To explain, the norm of non-intervention, has a regulatory effect on, for instance, Russia as it establishes the probability of sanctions in case it is violated. In this sense, it influences its incentives and shapes its decision to interfere or not, depending on a cost-benefit analysis. In a less realist understanding, it also has a constitutive effect in portraying Russia as a violator of sovereignty and thus as a state

that does not adhere to the types of actions generally accepted as appropriate; an illegitimate international partner. An identity of a non-cooperative and aggressive state is distinguished from a norm-compliant and rule-abiding one in the eyes of the international community. In turn, transaction and cooperation costs are higher for non-compliant 'players' than their conformable counterparts.

In our understanding, these two concepts are not mutually exclusive or independent of each other. The perceived illegitimate identity of Russia engaging into EI can and should not be separated from the size and severity of the costs of doing so. In simple words, the greater the deviation from legitimate behaviour, the higher the costs of doing so. This notion of proportionality implicit in the dual understanding of norms and their impact on state behaviour is the cornerstone of our recommendations in this final chapter of our analysis. International norms and standards of behaviour need to be developed specifically around EI in order for a regulatory threshold to grow out of them. Without clearly defining what is permitted and what not, how can we devise an effective framework for dealing with it?

To support this claim, consider how the Obama administration only responded with economic sanctions on Russia after the 2016 election hacks (Fidler, 2017). It maintained that cyberactivities transgress norms of appropriate behaviour but don't violate international law since the legal principles of sovereignty and non-intervention are not legally-speaking violated (ibid). This immediately problematises the deterrent effect of established international law and norms (McFaul et al., 2019; Fidler, 2017). The same logic applies to private companies too. Since the costs of self-regulation are quite high, so need to be the costs of non-compliance with norms and standards of ethical business conduct and inadequate and opaque data protection, political

advertising and content personalisation policies.[8] The example of the US serves also to emphasize the importance of distinguishing between norms and international law (Fidler, 2017). Indeed, the norm of sovereignty- embedded into the UNC and thus in customary international law- may be regarded as being violated by 'black operations' (Tomz & Weeks, 2019 :1). Still, event show how the established norm carried no significance for Moscow.

The Current State of EI-relevant International Law

Since there is no single principle of international law directly applicable to EI, using existing normative principles and interpreting them accordingly, seems to be the first step for delineating and defining relevant standards of appropriate behaviour. This is the task we undertake in this section, first by laying out the current state of EI-relevant international law and afterwards identifying which principles' interpretational scope can be expanded to create a solid normative basis for developing EI-focused international law in the future.

When it comes to regulating cybercrime and illicit electronic activity at a transnational-level, the "Budapest Convention on Cybercrime" (2001) "serves as a guideline for any country developing comprehensive national legislation against cybercrime, and as a framework for international cooperation between State parties to this Treaty" ("Election Interference & The Convention on Cybercrime | NGM Lawyers", 2020). In an attempt to specify its applicability to EI, the Council of Europe Cybercrime Convention Committee (T-CY) issued an open communication in which it set out the digital aspect of EI that are covered by the convention (ibid). The T-CY

[8] Facebook was made by the British government to pay a £500,000 for its role in the Cambridge Analytica scandal (Zialcita, 2019)

points out that Articles 2-7 and 11-13[9] of the Budapest Convention are relevant to EI as they criminalise conduct pertaining, amongst other things, illegal access of, interception and interference in data and computer systems as well as misuse of devices (political hacking, information theft, documents leaking etc.). As an instrument of hard law, this convention legally binds signatories to comply with its stipulations. Yet, major perpetrators of EI (e.g. Russia and China) have neither signed nor ratified it. Nonetheless, the Budapest Convention on Cybercrime is the solemn and most rigorous instrument of international law that can be applied to EI. Therefore, prior to the establishment of international norms to deter states from carrying out EI operation, its relevant articles should be incorporated into bilateral or regional agreements between platform providers and MLDs. This would serve to clarify 'grey areas' of existing international law and decrease the occurrence of EI by preventing social media companies to allow their services to be maliciously used by aggressive foreign states.

The earliest attempts to devises soft law instruments that align international norms with the realities and challenges of the digital/information era are found in the Tallinn Manual and Tallinn Manual 2.0 (McFaul et al., 2019). These two academic studies were conducted as part of a NATO-based initiative to support the application of existing international law (mainly humanitarian and jus ad bellum) to new forms of cyber conflicts and warfare. Even though their current scope does not adequately cover the practices of EI to an extent that they can serve as guidelines to regulating it, they do provide foundations for its further expansion to meet that end (which are discussed in the next paragraph). A more up-to-date effort to adjust and apply international law to cyber space was the formation of the UN's Group of Governmental Experts (GGE) assigned with the task of considering cyber technologies

[9] See Appendix Table 5 (Cybercrime Convention Committee (T-CY), 2019)

and international security (Fidler, 2017). Before it broke down in 2017, the GGE issued two reports: The first in 2013 (UN General Assembly, 2013), asserted that existing international law can and should be applied to cyber space, but said very little as to how this could be done and even less as to why should interested parties accept such an expansion of international law's scope and jurisdiction (Fidler, 2017). The second issued in 2015 (UN General Assembly, 2015), articulated a list of voluntary norms for appropriate state behaviour around Information and communications technologies (ICTs) (Fidler, 2017), which mainly build upon the application of human rights on cybercrime, the principle of non-interference (sovereignty) and the call for interstate as well as public-private cooperation (UN General Assembly, 2015: 7-8). Although these norms were never established to an extent that they exert any substantial influence on actor behaviour, they are useful for informing our action plan on how to establish well-defined and widely accepted standards of behaviour surrounding EI. Below, we attempt to use the norms asserted in these international documents for making a case for expanding their scope of interpretation and increasing their effectiveness in deterring EI.

Recommendations

Developing a Solid Legal Basis for Applying Established International Norms to EI

The most obvious aspect of customary international law relevant to EI, is the non-intervention principle. This affords the right of every sovereign State to govern its affairs without outside interference (Eisenstein, 2019). Even though at first its application seems straightforward, the broad language and grey areas of international law raises difficulties in applying the principle to EI. This is mainly because political hacking, disinformation campaigns, content personalisation, private data abuse and

other means of SMM and EI do not directly affect the electoral outcome thus lack the 'coercive element' that constitutes a violation of sovereignty according to international law. As the Tallinn Manual concluded, the non-intervention principle applies to EI when states "use cyber-operations to remotely alter electronic ballots and thereby manipulate an election" (Schmitt, 2013: 313). What this means is that, if EI does not manipulate the election process in itself, but rather attempts to employ influence and information operations to sway (otherwise free) voters, then the non-intervention principle is not activated (Eisenstein, 2019). Moreover, following the conclusions of the Tallinn Manual 2.0, EI does not amount to an 'act of war' either. The United Nations Charter (UNC) contains a very narrow conception of the 'use of force' not including any action that is not inherently violent (United Nations Conference on International Organization, 1945: Article 2). As a result, since EI does not cause physical damage or casualties, it cannot under international law be regarded as 'using force'.

Furthermore, adjust the scope of these principles in a manner that makes it applicable to EI could also be expedited by clarifying its definition. For instance, drawing a distinction between influence/information operations (targeting voters) and technical ones (targeting and disrupting the voting process itself). Accordingly, the latter could fall within the definitional range of 'use-of-force' since they cause tangible disruptions to the voting process, whereas the manipulation of foreign voters would violate the principle of non-intervention (withstanding the expansion of the coercive element). This would allow the formulation of different operational levels of EI, enhance definitional accuracy, and provide a more flexible and context-specific legal interpretation basis for institutionalising norms of appropriate behaviour. At the same time, establishing a clear application of existing norms of non-interference in elections, would also promote cooperation among MLDs to develop, support and

enforce universal standards of appropriate state behaviour when it comes to EI as well as suitable responses to it. States that share respect for the rule of law would have valid principles to rely upon in leading an international coalition focused on protecting their democratic electoral processes.

In sum, we are led to disagree with those supporting that the current legal interpretation and scope of application of international legal principles assume a sufficient contemporary legal basis and thus provide states with comprehensive legal instruments to combat EI. This automatically implies the need to adjust and mould current legal principles to fit the realities of the modern digital world. To this end, and considering the analysis above, we propose a more contextualised and flexible interpretation benchmark that will treat cyberspace as a new operational dimension and hence allow for a clearer and broader application and implementation of legal paradigms relevant to EI. Namely, the principles of sovereignty, non-intervention and the use of force as an act of war could serve as the cornerstone of a normative framework that directly applies to EI.

Connect IHL to EI in order to Build Legitimate and Universal Norms Focused on Protecting Against It

Our data shows that the only far-reaching, widely endorsed legal framework that can be connected to EI is IHL (McFaul et al., 2019; Council of Europe, 2001). Therefore, we propose using the Human Rights regime as the legal foundation for developing international norms that delimit illegitimate and illegal EI operations, and sufficiently incentivise private companies and state actors to withhold from getting involved and/or engaging in such activities. Amongst numerous regional covenants

[10], the 1948 Universal Declaration of Human Rights (UDHR), the 1966 United Nations International Covenant on Civil and Political Rights (ICCPR), and the 2000 Warsaw Declaration represent ratified agreements that compel signatories to protect and reaffirm: the right of every citizen to hold opinions without interference, the right to freedom expression, including the freedom to seek, receive and impart information and ideas of all kinds, the right to have their privacy respected (Council of Europe, 2001: 2), and the right of every citizen to choose their representatives through open and fair election that are free of fraud and intimidation and without any state, group or person using means to interfere with or subvert their ability to do so (McFaul et al., 2019: 57). Developing an international normative framework that supplements these conventions by establishing a clear connection of EI with IHL will enable states to carry out more effective criminal investigations and proceedings concerning political hacking, disinformation campaigns, opaque and non-consensual content personalisation, private data abuse and other means of SMM, as well as permit the collection of digital evidence of such operations (since they could be regarded as criminal offenses). We thus propose MLDs, as well interested and relevant civil society and international organisations to fortify their commitment to IHL so that the creation of norms that deter SMM takes place upon a universal framework connected to hard-law instruments that will increase their effectiveness.

Establish International Standards and Guidelines for Social Media Platforms

The last recommendation concerns the elaboration of state-based guidelines for social media companies focused on reducing the likelihood of their (active, passive,

[10] e.g. the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (European Court of Human Rights, 1950)

direct or indirect) involvement in foreign EI. Major platform providers' interaction and cooperation with foreign governments should be regulated by their 'home states' by the establishment of norms and rules about the appropriate level of cooperation with foreign governments with regard to disinformation dissemination, user privacy protection and censorship, as well as designated responses to it. In order to achieve global recognition and enforcement of such guidelines, MLDs should synchronise their initiatives and collaborate with relevant international bodies to support platform integrity and safeguard user rights under international law (McFaul et al., 2019).

An aforementioned useful tool in institutionalising community norms of platform interaction with foreign governments into tangible international law, is the Ranking Digital Rights (RDR) project. The RDR index is based on 31 indicators measuring company's commitment to human rights, freedom of expression (anticensorship) and privacy ("2019 Ranking Digital Rights Corporate Accountability Index", 2019). These three categories are broadly applicable to the full range of companies and product lines and also cover all aspects of platform-foreign government interaction. Hence, we propose that they are used to arrive at accurate criteria of assessing the appropriate level of such cooperation.

Assessing the Recommendations

As underlined in the CPC report, EI is an international phenomenon, a global problem, and therefore a systematic response must be both domestic and international (McFaul, et al. 2019: 59). Espousing this view, we attempted to provide an advisory action plan for devising international norms that deter EI, which will encourage individual states to institutionalise them into domestic legal instruments with the capacity to impose effective, proportionate and dissuasive sanctions on deviants. This would then support the ratification of bilateral and regional agreements between

states on regulating EI and eventually enable the incorporation of EI-relevant norms and rules into hard international law. Assessing our recommendations according to our metrological framework is less straightforward in this case, as the two NATO reports which are used as an evaluation benchmark contain no data on the establishment of appropriate standards of behaviour around EI. However, the CPC does provide a number of insights that can be used to refine our proposed solutions.

The first one is the consideration of the deterrent effect of existing norms relevant to EI. The authors advocate the need to articulate clear, proportionate and swift punitive countermeasures in order to strengthen and consolidate the prevention of EI by translating normative pressures into concrete and substantial non-compliance costs. The totality of our recommendations aims exactly at this outcome and therefore can be seen as conducive to creating space under international law for an effective criminal justice response to deter EI and protect citizens of MLDs from the malicious use of information and communication technologies (Cybercrime Convention Committee (T-CY), 2019). The second insight concerns the cooperation of MLDs in leading a unified transnational response against EI, which in our recommendations was not sufficiently elaborated. As the CPC report highlight, such a coalition should be based on the establishment of multilateral information centres which will share diagnostic intel and conduct and distribute in real time situational analysis (McFaul et al., 2019: 61). In turn, these multilateral centres would bolster bilateral, regional and multilateral cooperation (through one-time initiatives but also enduring official agreements).

Conclusions

In this final chapter of our analytical exploration, attention was placed on the significance of developing (or reinforcing already existing) normative principles that

will shape actor behaviour with regard to interfering in the electoral process of foreign sovereign states. After a brief theoretical overview of the constitutive and regulatory effects of norms and their function in a global governance context, it was argued that the current level of normative deterrence around EI is highly underdeveloped and in urgent need of updating and adjustment to the digital age. In this light, we forwarded a series of actions that governments, private social media companies, international bodies and civil actors should or could take in order to consolidate the incorporation of EI-relevant democratic principles of under international law.

In specific, it was proposed: First, that the interpretational scope of three core widely endorsed principles (non-intervention, sovereignty and use of force as an act of war) should be expanded to include and apply to the methods and impacts of modern EI operations. Second, that the most effective and efficient way to provide a solid legal basis for EI prosecution, criminalisation and meaningful punitive responses is to draw a series of bilateral, multilateral and regional agreements which ties SMM with violation of human rights. And last but not least, once again emphasising the important role of private companies in preventing EI, we advocated for state-based guidelines and regulatory requirements focusing on the interaction of platform providers with foreign governments. Democracies around the world should start –in tandem- tightening the regulatory grip around the capacity of foreign governments cooperating with social media platforms to spread disinformation, breach data privacy and arbitrarily filter content (censorship). The assessment of our recommendations provided some additional insights on the significance of imposing timely, tailored, consistent and credible costs to non-compliant actors for enhancing the deterrent effects of norms, as well as on how to better synchronise a unified response across democratic states by establishing multilateral centres for situational analysis.

Conclusion

Concluding Remarks & Discussion of Findings

In this paper we set out to explore the potential content and scope of regulatory measures aiming at safeguarding free and fair electoral processes/outcomes and pluralistic and productive public political dialogue at the face of emerging hazards caused by the rapid advancement in information technologies and infrastructure as well as automation. The digital revolution and the rise of social media as influential news sources and increasingly denser fora of political debate has unlocked many opportunities for more open and inclusive political deliberation as well as transparent and accountable decision-making in modern, complex and diverse democracies around the globe. However, it has also exposed 'grey areas' in current national, international and corporate regulatory policies that create new opportunities for domestic, corrupted and/or foreign malicious, aggressive actors to promote their particular political and economic interests at the expense of a democratic state's electoral integrity and citizen voting autonomy. In broad terms, our mission in this research project was to identify a course of regulatory action that will safeguard against the perils of this paradigm shift in the methods of information circulation and ensuing political interaction while at the same time allowing politicians and citizens to utilize these new technological tools for enhancing the democratic character of political decision-making and electoral outcomes.

In more explicit terms, this 'governance gap' has allowed a phenomenon known as digital 'Election Interference' to unfold. For this paper's purpose EI was defined as the illegitimate and unlawful attempt to interfere with and/or undermine the democratic processes of an electoral race or a vote on an issue of high political importance in a MLD, by means that involve the violation of fundamental human and civil/political rights, in order to influence the electoral outcome towards a direction

that furthers particular economic and political interests. Our conception of a MLD was formed around an identification of four institutional pillars that distinct it from any other type of 'democratic' political constellation: namely, the rule of law, political accountability, bureaucratic integrity and public deliberation.

Accordingly, a cornerstone of our argument (that there is an urgent need to develop and reinforce existing regulation surrounding EI) was based on the assumption that these four institutional pillars are both theoretically and practically challenged by the set of actions, techniques and tactics entailed in EI operations. Throughout the paper, we use the term Social Media Manipulation, to refer to the digital techniques employed in EI that involve interaction with individual citizens on social media platforms and the management of the content that is available to them, underlined by opaqueness and an ambiguous moral and legal nature.

This thesis derived from the research question: *Employing secondary data analysis, can a concrete set of policy recommendations be produced to set a benchmark for modern liberal democracies to counter election interference and prevent uncoordinated national efforts?* The research question articulates a delineated problem, namely the need for concrete policy recommendations in rapidly developing debates around EI and social media manipulation that will 'fill' the aforementioned governance gap. We approached this by operationalising secondary data analysis in context of a qualitative Nested Analysis. This saw the inspection of five topics that were taken from the structure of the CPC report: 1) intent recognition behind election interference, 2) electoral infrastructures, 3) online advertising by foreign governments and nationals, 4) foreign media organisations, and 5) international norm setting against election interference and disinformation. Each chapter first executed the SDA consulting various and diverse sources of literature to build a comprehensive set recommendation in the recommendations section of each chapter. To substantiate

these recommendations, they were validated against the CPC and NATO reports in the recommendation assessment section of each chapter. A final cohesive presentation of the Nested Analysis results was then presented in form of the individual chapter conclusions.

We also established a comprehensive literature review as the academic basis of our thesis. This enabled us to select, adapt and apply relevant theories on our topic of research as well as delimit the definitional scope of key terms and thus clarify the research scope of the project. Our choice of a narrow definitional scope allowed us to focus the investigation to the most harmful types of EI and thus prioritise the aims of regulatory initiatives, so as to forward holistic and generalizable recommendations that MLDs can contextualize according to their specific circumstances. Below we will list (not exhaustively) the main contribution of this section to our overall research objective.

Recommendations Summary

Chapter 1: Understanding intentions behind interference

1.1. Distinguish between two set of approaches: 1) immediate/economic/political/top-down vs. 2) long-term/normative/target demographic/bottom-up.
1.2. Build legal safeguards that serve as early warning systems, incl. transparent and well-defined political campaign laws (prevent domestic promotion)
1.3. Build digital literacy among population to identify intentions behind and build resilience against disinformation and manipulation campaigns.
1.4. Involve private sector capacity to identify foreign interference attempts and intentions.

Chapter 2: Increasing the security of electoral infrastructures

2.1. Uniform electoral systems. Any electoral system, analogue or digital, should comply with common qualifiers rather than comply by common limitations.
2.2. Centralised oversight. Elections should be overseen by a centralised auditing body, as well as a centralised ledger in charge of keeping voter data points safe and updated.

2.3. Federal assistance. Autonomous political entities under a unified government should be afforded the necessary resources, expertise, and labour to implement a standardised system regardless of their abilities to do so.
2.4. Cybersecurity. Governments need to invest in adequate cyber security walls and preventative algorithms to spot attacks early and decrease risk of potential attacks by means of deterrence.
2.5. Counterforce disinformation. It is important to take comprehensive action to counter digital manipulation and disruption efforts across various media.

Chapter 3: Regulating Online Political Advertising by Foreign Governments and Nationals

3.1. Disclosure laws and regulations. Ads need to comply with common standards that indicate when sources are operated by bots or state-aligned actors.
3.2. Strict limitations on bots. Ensure that no bots initiates contact with human users without their explicit consent.
3.3. Protect data. Block bots and bot owners from amassing and exploiting user data for political gains.
3.4. Industry cooperation. Data asset holders should share more accurate, accessible, comprehensible information about the influence of personalisation systems handling of private data.

Chapter 4: Confronting Efforts at Election Manipulation from Foreign Media Organisations

4.1. Transparency and disclosure regulations. Ensure adherence to journalistic codes and ability to prove, if necessary, the integrity of an organizations journalistic work to authorities.
4.2. Informed consumers. Assist media consumers in identifying false and inaccurate media outlets and reporting.
4.3. Public responsibilities for the private sector. Oblige social media companies to comply with stricter regulations around administering SMM on their hosting platforms.
4.4. No censorship but independent oversight. Instead of censoring the press, support it by building independent oversight bodies constituted of experts and industry professionals.

Chapter 5: Establishing International Norms and Agreements to Prevent Election Interference

5.1 Align laws with modern realities. Cyberspace requires legislation that is broad and dynamic to adequately frame challenges of a rapidly developing field.
5.2 Commit to IHL. Strengthen legitimacy by means of a universal hard-law instruments in regulation social media.

5.3 International Standards and Guidelines for Social Media Platforms. Synchronise their initiatives and increase collaboration of international bodies.

Discussion of Findings

We believe that our approach and the extensive groundwork done has built a nouvelle and relevant method to comprehensively analyse the rapid flow of election interference discourse to produce employable and replicable policy frameworks that can help governments benchmark their efforts and coordinate them on an international level. In specific, we trust our paper enlarges current literature surrounding EI in the following manner.

First, we contribute to the growing body of theoretical literature on emphasizing the tensions between EI and democracy. This main theoretical contribution is found on the clear delineation of the specific citizen capacities and democratic processes, which modern information ecosystem as well as current trends in political campaigning (as manifested in EI operations) seem to undermine. This is arguably a highly relevant contribution since both digital political campaigning (and its use of micro-targeting and automatic content generation) as well as social media news sourcing are expected to increase in the future (Bossetta, 2018).

Second, we sought to better understand and explain the role of private companies in promoting democratic resilience in a manner which problematizes the current state of self-regulatory initiatives and supports a more proactive corporate identity with regard to the political effects of social media use. This complements research on the regulation of cyberspace and the role of social media and technology.

Third, our research involved a broad and detailed empirical analysis of case-based private and public regulatory responses which provided concrete and straightforward empirical findings in the form of policy recommendations that both academics and policymakers could potentially consult when devising effective EI

countermeasures. They also surfaced severe policy gaps and thus afforded ample space for legislative revision as well as further research on the matter.

Limitations

As previously stated this study was designed to have a high replicability factor and serve as the basis for policy design and research across Western MLDs. To this end we identify the following limitations to our methodological approach and theoretical assumptions. First, a major practical restriction on our empirical findings is posed by the absence of statistical evidence on a direct causal relationship between individual voting behaviour and EI. This is an obstacle that all researchers in the field encounter mainly due to a number of statistical difficulties in measuring and isolating the impact of EI on voting behaviour. Second, temporal and spatial proximity blur the lines between speculation and facts which potentially undermines parts of the authority of our results. Third, besides the absence of quantitative data establishing robust causality, our methodological choice of relying on publications for 'expert testing' our findings, rather than more dynamic qualitative input (interviews) could be challenged by critics. However, given the above two limitations the verification of our results and the statistical representation of our sampling method could not withstand the highly subjective nature of observations based on personal experience and knowledge. Therefore, we consciously chose to rely on static qualitative data that would provide a broad, generalizable set of findings but also allow for complementary secondary sources to enrich their interpretation and understanding of EI as a phenomenon. Lastly, the fact that EI represents uncharted waters for political scientists, academics, and researchers creates a high chance that our recommendations would require some re-consideration and revision following breakthroughs and new discoveries in the study of the relationship of election integrity and information technology.

Appendix

Figures

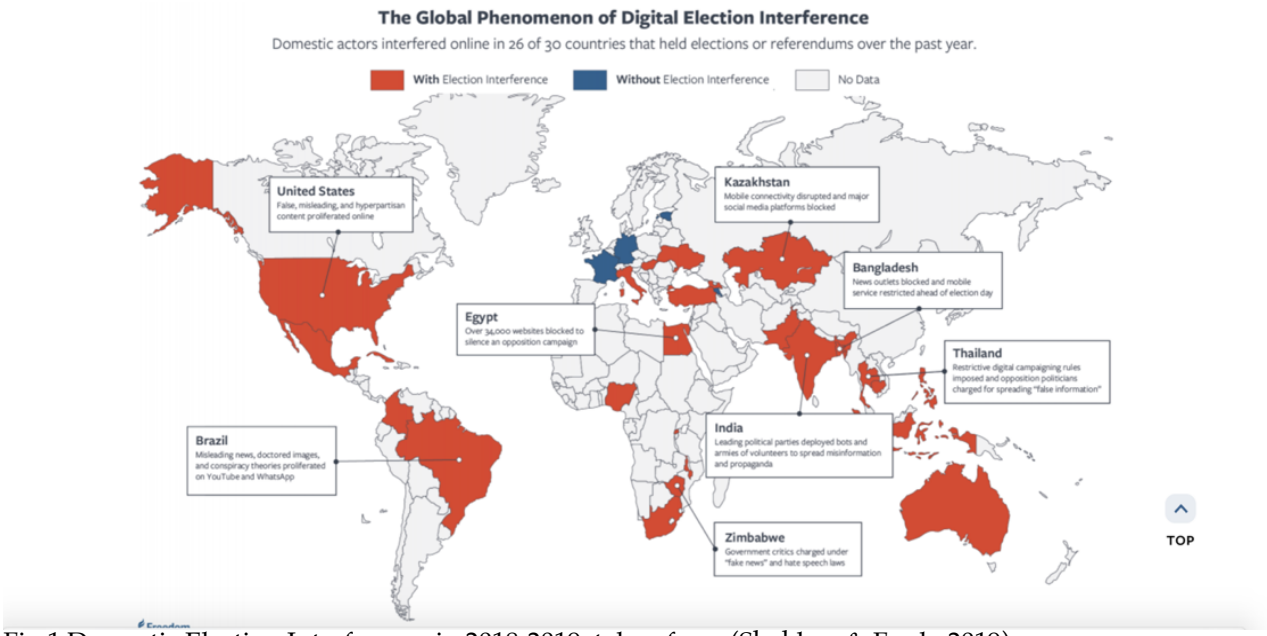


Fig.1 Domestic Election Interference in 2018-2019, taken from (Shahbaz & Funk, 2019)

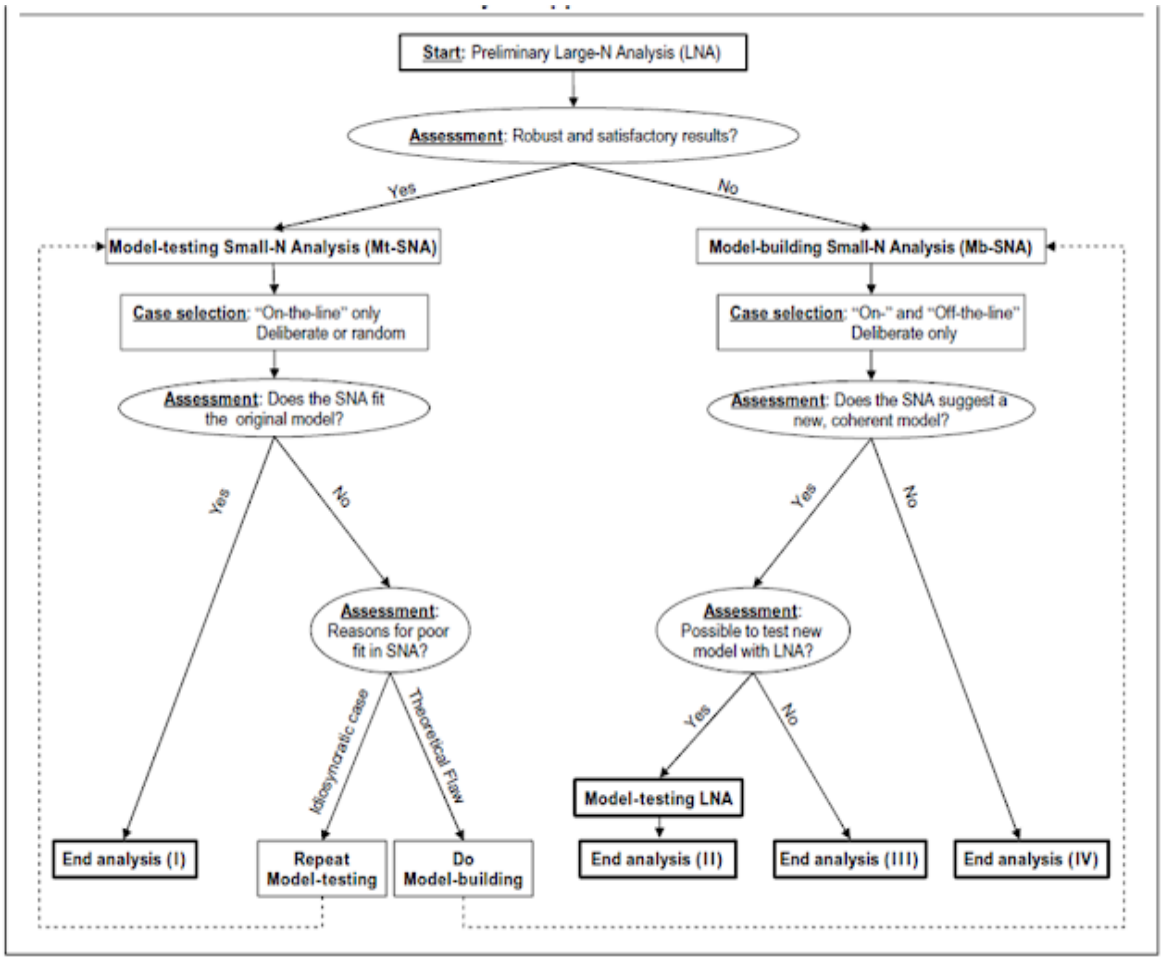


Fig. 2. Nested Analysis procedural branches, as taken from Liebman (2005)

Tables

Social Media	Pros	Cons
Issues: Privacy, Security, Accuracy (of publicly available data) and Archiving, Manipulation, Polarisation	Participation and Engagement: fostering participatory dialogue, providing a voice for citizens in discussions of policy development and implementation (Berrot et al, 2012)	Depressing voter turnout; leading to sub-optimal policy outcomes
	Co-production of government services (ibid)	Shattered Public Sphere → Polarisation, Militant Democracies, lack of consensus→ social instability (public deliberation)
	Crowdsourcing solutions and Innovations (ibid)	Lower trust in democratic institutions (Tomz & Weeks, 2019)

Table. 2 Summary of positive and negative actors in social media and bot use.

TABLE 1—THE CHAIN OF DEMOCRATIC CHOICE

	DIMENSIONS OF CHOICE	NORMATIVE PREMISES OF DEMOCRATIC CHOICE	STRATEGIES OF NORM VIOLATION
1	The object of choice	*Empowerment:* Democratic elections involve the delegation of decision-making authority.	• *Reserved positions:* limiting the scope of elective offices • *Reserved domains:* limiting the jurisdiction of elective offices
2	The range of choice	*Freedom of supply:* Citizens must be free to form, join, and support conflicting parties, candidates, and policies.	• *Exclusion of opposition forces:* restricting access to the electoral arena • *Fragmentation of opposition forces:* disorganizing electoral dissidence
3	The formation of preferences	*Freedom of demand:* Citizens must be able to learn about available alternatives through access to alternative sources of information.	• *Repression:* restricting political and civil liberties • *Unfairness:* restricting access to media and money
4	The agents of choice	*Inclusion:* Democracy assigns equal rights of participation to all full members of the political community.	• *Formal disenfranchisement:* legal suffrage restrictions • *Informal disenfranchisement:* practical suffrage restrictions
5	The expression of preferences	*Insulation:* Citizens must be free to express their electoral preferences.	• *Coercion:* voter intimidation • *Corruption:* vote buying
6	The aggregation of preferences	*Integrity:* One person, one vote. The democratic ideal of equality demands weighting votes equally.	• *Electoral fraud:* "redistributive" election management • *Institutional bias:* "redistributive" electoral rules
7	The consequences of choice	*Irreversibility:* Elections without consequences do not qualify as democratic.	• *Tutelage:* preventing elected officers from exercising their constitutional powers • *Reversal:* preventing victors from taking office, or elected officers from concluding their constitutional terms

Table. 3 The Chain of Democratic Choice, taken from Schedler (2002) p. 39

Table 4. Current government responses to disinformation (Bradshaw et al., 2018)

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed to modify websites, to alter voter databases, or to manipulate results of votes such as by tampering with voting machines.
Article 5 – System interference	The functioning of computer systems used in elections or campaigns may be hindered to interfere with campaign messaging, hinder voter registration, disable the casting of votes or prevent the counting of votes through denial of service attacks, malware or other means.
Article 6 – Misuse of devices	The sale, procurement for use, import, distribution or other acts making available computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate election interference such as the theft of sensitive data from political candidates, parties or campaigns.
Article 7 – Computer-related forgery	Computer data (for example the data used in voter databases) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. For example, some countries require election campaigns to make public financial disclosures. Forgery of computer data could create the impression of incorrect disclosures or hide questionable sources of campaign funds.
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of election interference.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of election interference may be carried out by legal persons that would be liable under Article 12.
Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against fundamentals of political life such as elections. Criminal actions and their effects may differ in different countries, but election interference may undermine trust in democratic processes, change the outcome of an election, require the expense and upheaval of a second election, or cause physical violence between election partisans and communities. A Party may provide in its domestic law a sanction that is unsuitably lenient for election-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example, if such acts affect an election significantly or cause deaths or physical injuries or significant material damage.

Table 5. Articles 2-7 and 11-13 of the Budapest Convention, taken from (Cybercrime Convention Committee (T-CY), 2019)

Bibliography

About RT. (2020). Retrieved 10 April 2020, from https://www.rt.com/about-us/

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, *15*(1), 5-31. doi: 10.11610/connections.15.1.01

Akçayır, M., Dündar, H., & Akçayır, G. (2016). What makes you a digital native? Is it enough to be born after 1980?. *Computers In Human Behavior*, *60*, pp.435-440. https://doi.org/10.1016/j.chb.2016.02.089

Algavy, L., & Al-Hanaki, D. (2014). Spreadability in the news journalism: the modern news criteria Author. *RUDN Journal Of Studies In Literature And Journalism*, (4), 124-133.

Alvarez, R., Hall, T., & Hyde, S. (2009). Election fraud (1st ed., pp. 42-44). Brookings Institution Press.

Anderson, C., Blais, A., Bowler, S., Donovan, T., & Listhaug, O. (2005). Losers' Consent. doi: 10.1093/0199276382.001.0001

Andornino, G. (2017). The Belt and Road Initiative in China's Emerging Grand Strategy of Connective Leadership. *China & World Economy*, *25*(5), 4-22. doi: 10.1111/cwe.12211

Andrews, L., Higgins, A., Andrews, M. W., & Lalor, J. G. (2012). Classic grounded theory to analyse secondary data: Reality and reflections. *The Grounded Theory Review*, 11(1), 12-26.

Anzia, S., & Jackman, M. (2013). Legislative Organization and the Second Face of Power: Evidence from U.S. State Legislatures. *The Journal Of Politics*, *75*(1), 210-224. doi: 10.1017/s0022381612000977

Aral, S., & Eckles, D. (2019). Protecting elections from social media manipulation. *Science*, *365*(6456), 858-861. https://doi.org/10.1126/science.aaw8243

Arceneaux, K., Dunaway, J., Johnson, M., & Vander Wielen, R. (2020). Strategic Candidate Entry and Congressional Elections in the Era of Fox News. *American Journal Of Political Science*, *64*(2), 398-415. doi: 10.1111/ajps.12478

Automation rules. (2020). Retrieved 8 April 2020, from https://help.twitter.com/en/rules-and-policies/twitter-automation

Babington, C. (2019). The Disinformation Age. *GW Magazine*. Retrieved 10 February 2020, from http://magazine.gwu.edu/the-disinformation-age.

Babones, S. (2020). Taiwan Deserves to Be a Normal Country. *Foreign Policy*. Retrieved 12 April 2020, from https://foreignpolicy.com/2020/01/15/taiwan-deserves-normal-country-tsai-election/.

Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign. *2018 IEEE/ACM International Conference On Advances In Social Networks Analysis And Mining (ASONAM)*. doi: 10.1109/asonam.2018.8508646

Badawy, A., Addawood, A., Lerman, K., & Ferrara, E. (2019). Characterizing the 2016 Russian IRA influence campaign. *Social Network Analysis And Mining*, 9(1). https://doi.org/10.1007/s13278-019-0578-6

Baldini, G. (2017). Populism in Europe: everywhere and nowhere?. *European Political Science*, 16(2), 258-262. https://doi.org/10.1057/eps.2016.9

Barker, A. (1993). The Politics of Expert Advice: Creating, using and manipulating scientific knowledge for public policy. *Edinburgh Univ. Press*.

Barlas, D., & Yilmaz, Ş. (2016). Managing the transition fromPax BritannicatoPax Americana: Turkey's relations with Britain and the US in a turbulent era (1929–47). *Turkish Studies*, *17*(3), 449-473. doi: 10.1080/14683849.2016.1165616

Bartlett, J., Smith, J., & Acton, R. (2020). *The Future of Political Campaigning*. London: Demos. Retrieved from https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf

Barton, J., Castillo, M., & Petrie, R. (2014). What Persuades Voters? A Field Experiment on Political Campaigning. *The Economic Journal*, *124*(574), F293-F326. https://doi.org/10.1111/ecoj.12093

Bastos, M., & Mercea, D. (2017). The Brexit Botnet and User-Generated Hyperpartisan News. *Social Science Computer Review*, *37*(1), 38-54. https://doi.org/10.1177/0894439317734157

Bastos, M., & Farkas, J. (2019). "Donald Trump Is My President!": The Internet Research Agency Propaganda Machine. *Social Media + Society*, *5*(3), 205630511986546. doi: 10.1177/2056305119865466

Bartels, L. (2017). *Democracy for realists - why elections do not produce responsive government*. Princeton, NJ: Princeton University Press.

Bayer, J., Bitiukova, N., Bárd, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States European Parliament's Committee on Civil Liberties, Justice and Home Affairs*. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs. Retrieved from https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

Baylis, J., Smith, S., & Owens, P. (2014). The Globalization of World Politics: An Introduction to International Relations (6th ed.). Oxford: Oxford University Press.

Benkler, Y., Faris, R., & Roberts, H. (2018). The Architecture of Our Discontent. *Oxford Scholarship Online*. doi: 10.1093/oso/9780190923624.003.0002

Béland, D., & Cox, R. (2011). *Ideas and Politics in Social Science Research*. Oxford University Press.

Benton, T., & Craib, I. (2011). *Philosophy of Social Science* (p. 121, 131-133). Palgrave Macmillan.

Berghel, H. (2017). Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election. *Computer*, *50*(9), 87-91. doi: 10.1109/mc.2017.3571054

Bertot, J., Jaeger, P., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly*, *29*(1), 30-40. doi: 10.1016/j.giq.2011.04.004

Berzina, K. (2018). Sweden — Preparing for the Wolf, not Crying Wolf: Anticipating and Tracking Influence Operations in Advance of Sweden's 2018 General Elections. *GMF*. Retrieved from https://www.gmfus.org/blog/2018/09/07/sweden-preparing-wolf-not-crying-wolf-anticipating-and-tracking-influence

Bessi, A., & Ferrara, E. (2020). Social bots distort the 2016 US presidential election online discussion. *First Monday*, *21*.

Blakemore, E. (2019). How the Treaty of Versailles ended WWI and started WWII. *National Geographic*. Retrieved from https://www.nationalgeographic.com/culture/topics/reference/treaty-versailles-ended-wwi-started-wwii/

Blasina, N., Tilford, C., Nevitt, C., & Wisniewska, A. (2019). The European Parliament elections — an interactive guide. *Financial Times*. Retrieved from https://ig.ft.com/european-parliament-elections-guide/

Boot, M., & Bergmann, M. (2019). *Defending America From Foreign Election Interference*. Washington D.C.: National Security and Defense Program. Retrieved from https://www.cfr.org/report/defending-america-foreign-election-interference

Bossetta, M. (2018). The Digital Architectures of Social Media: Comparing Political Campaigning on Facebook, Twitter, Instagram, and Snapchat in the 2016 U.S. Election. Journalism & Mass Communication Quarterly, 95(2), 471-496. doi: 10.1177/1077699018763307

Bowler, S., Brunell, T., Donovan, T., & Gronke, P. (2015). Election administration and perceptions of fair elections. *Electoral Studies*, *38*, 1-9. doi: 10.1016/j.electstud.2015.01.004

Bradshaw, S., Neudert, L., & Howard, P. (2018). *Government Responses to Malicious Use of Social Media*. Riga: NATO Strategic Communications Centre of Excellence.

Brannon, V., & Whitaker, L. (2020). *Appeals Court Says First Amendment Limits Regulation of Online Political Advertising: Implications for Congress*. Washington D.C.: Congressional Research Service. Retrieved from https://crsreports.congress.gov/product/pdf/LSB/LSB10393

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved 16 April 2020, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cantor, G., & Bhaskar, R. (1982). The Possibility of Naturalism: A Philosophical Critique of the Contemporary Human Sciences. *The Philosophical Quarterly*, 32(128), 280. https://doi.org/10.2307/2219329

Carroll, R. (2014). This article is more than 6 years old Russia Today news anchor Liz Wahl resigns live on air over Ukraine crisis. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/mar/06/russia-today-anchor-liz-wahl-resigns-on-air-ukraine

Chappell, B. (2017). TV Company Linked To Russia's RT America Registers As Foreign Agent In U.S. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/11/14/564045159/rt-america-firm-registers-as-foreign-agent-in-u-s-russia-looks-to-retaliate

Chernick, M. (2011). Hypothesis Testing. The Essentials Of Biostatistics For Physicians, Nurses, And Clinicians, 72-94. https://doi.org/10.1002/9781118071953.ch6

Clinton, H. (2018). *What Happened*. Simon & Schuster UK Ltd.

Collins, S. (2004). *Crazy like a Fox*. New York, NY: Portfolio.

Community of Democracies. (2000). Warsaw Declaration: Toward a Community of Democracies. Warsaw.

Community Standards | Facebook. (2020). Retrieved 8 April 2020, from https://www.facebook.com/communitystandards/

Conover, M., Ratkiewicz, J., Francisco, M., Goncalves, B., Flammini, A., & Menczer, F. (2011). Political Polarization on Twitter. *ICWSM*, *133*, 89–96.

Council of Europe. (2001). Convention on Cybercrime. Budapest: Council of Europe.

Coppins, M. (2020). Popular Latest Sign In Subscribe The Billion-Dollar Disinformation Campaign to Reelect the President. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/

Corstange, D., & Marinov, N. (2012). Taking Sides in Other People's Elections: The

Polarizing Effect of Foreign Intervention. American Journal Of Political Science, 56(3), 655-670.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage. https://doi.org/10.1111/j.1540-5907.2012.00583.x

Crilley, R., & Gillespie, M. (2018). What to do about social media? Politics, populism and journalism. *Journalism*, 20(1), 173-176. https://doi.org/10.1177/1464884918807344

Curtin, D. (2016). The European Union and Executive Power. *A Companion To European Union Law And International Law*, 109-118. doi: 10.1002/9781119037712.ch8

Cybercrime Convention Committee (T-CY). (2019). *T-CY Guidance Note #9 Aspects of election interference by means of computer systems covered by the Budapest Convention*. Budapest: Cybercrime Convention Committee (T-CY). Retrieved from https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23

Dahl, R. (1971). *Polyarchy: Participation and Opposition* (1st ed.). New Haven, CT: Yale University Press.

Dale, A., Arbor, S., & Procter, M. (1988). *Doing Secondary Analysis.* London, UK: Unwin Hyman.

Davies, W. (2019). Why can't we agree on what's true any more?. *The Guardian*. Retrieved 18 April 2020, from https://www.theguardian.com/media/2019/sep/19/why-cant-we-agree-on-whats-true-anymore.

De Cleen, B. (2017). Populism, Exclusion, Post-truth. Some Conceptual Caveats Comment on "The Rise of Post-truth Populism in Pluralist Liberal Democracies: Challenges for Health Policy". *International Journal Of Health Policy And Management*, 7(3), 268-271. https://doi.org/10.15171/ijhpm.2017.80

DeHaven, K. (2019). Stanford Scholars Set Forth 2020 Election Security Recommendations. *Security Today*. Retrieved from https://securitytoday.com/articles/2019/06/11/stanford-scholars-set-forth-2020-election-security-recommendations.aspx?admgarea=mag&m=1

De Jonge, A. (2017). Perspectives on the emerging role of the Asian Infrastructure Investment Bank. *International Affairs*, *93*(5), 1061-1084. doi: 10.1093/ia/iix156

DeMaio, T., & Landreth, A. (2004). Do Different Cognitive Interview Techniques Produce Different Results?. Methods For Testing And Evaluating Survey Questionnaires, 89-108. https://doi.org/10.1002/0471654728.ch5

Department of the Taoiseach. (2018). *Discussion Paper – Regulation of Online Political Advertising in Ireland*. Dublin: Department of the Taoiseach.

Dinas, E., & Riera, P. (2017). Do European Parliament Elections Impact National Party System Fragmentation?. *Comparative Political Studies*, *51*(4), 447-476. doi: 10.1177/0010414017710259

Doolan, D. M., & Froelicher, E. S. (2009). Using an existing data set to answer new research questions: A methodological review. Research and Theory for Nursing *Practice: An International Journal*, 23(3), 203-215. doi:10.1891/1541-6577.23.3.203

Dowling, T. (2017). 24-hour Putin people: my week watching Kremlin 'propaganda channel' RT. *The Guardian*.

Eisenstein, A. (2019). The (il)Legality of Interference in Elections under International Law. *The Federman Cyber Security Research Center*. Retrieved from https://csrcl.huji.ac.il/people/illegality-interference-elections-under-international-law#_ftn20

El-Bermawy, M. (2016). Your Filter Bubble is Destroying Democracy. *Wired*. Retrieved 14 April 2020, from https://www.wired.com/2016/11/filter-bubble-destroying-democracy/.

Election Interference & The Convention on Cybercrime | NGM Lawyers. (2020). Retrieved 8 April 2020, from https://ngm.com.au/budapest-convention-on-cybercrime-international-election-interference/

Erlanger, S. (2017). Russia's RT Network: Is It More BBC or K.G.B.?. *The New York Times*. Retrieved from

https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html

European Commission. (2018). *Code of Practice on Disinformation*. Brussels.

European Commission. (2019). *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*. Brussels: European Commission. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

European Court of Human Rights. (1950). *European Convention on Human Rights*. Brussels: European Court of Human Rights. Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf

Ewing, P. (2019). What You Need To Know About Foreign Interference And The 2020 Election. *NPR*. Retrieved from https://www.npr.org/2019/09/01/737978684/what-you-need-to-know-about-foreign-interference-and-the-2020-election

Falush, D. (2020). As the west is in lockdown, China is slowly getting back to business. *The Guardian*. Retrieved 12 April 2020, from https://www.theguardian.com/world/commentisfree/2020/mar/30/lockdown-china-coronavirus-outbreak.

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, *22*(8). doi: 10.5210/fm.v22i8.8005

Fidler, D. (2017). The U.S. Election Hacks, Cybersecurity, and International Law. *AJIL Unbound*, *110*, 337-342. doi: 10.1017/aju.2017.5

Financial Times. (2019). Online political ads are in urgent need of regulation. Retrieved from https://www.ft.com/content/e0a93d3c-fbd3-11e9-a354-36acbbb0d9b6

Fisher, M. (2013). In case you weren't clear on Russia Today's relationship to Moscow, Putin clears it up. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2013/06/13/in-case-you-werent-clear-on-russia-todays-relationship-to-moscow-putin-clears-it-up/

Flegenheimer, M. (2020). What if the Most Important Election of Our Lifetimes Was the Last One. *The New York Times*. Retrieved 12 April 2020, from https://www.nytimes.com/2020/04/07/us/politics/2020-vs-2016-election.html.

Flynn, P. (2020). Brexit What Brexit should have taught us about voter manipulation. *The Guardian*. Retrieved 14 April 2020, from https://www.theguardian.com/commentisfree/2017/apr/17/brexit-voter-manipulation-eu-referendum-social-media.

Freedom House. (2019). *Freedom in the World Report 2019*. Washington D.C.: Freedom House.

Fukuyama, F. (1992). *The End of History and the Last Man* (1st ed.). Free Press.

Gallagher, T. (2019). Trump TV: The Trump Campaign's Real News Update as Competitor to Cable News. *Visual Communication Quarterly*, *26*(1), 32-43. doi: 10.1080/15551393.2019.1576047

Gänzle, S., Grimm, S., & Makhan, D. (2012). *The European Union and global development*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.

Gerstein, J. (2017). DOJ told RT to register as foreign agent partly because of alleged 2016 election interference. *Politico*. Retrieved from https://www.politico.com/story/2017/12/21/russia-today-justice-department-foreign-agent-election-interference-312211

Geys, B., & Vermeir, J. (2014). Party Cues in Elections under Multilevel Governance: Theory and Evidence from US States. *Journal Of The European Economic Association*, *12*(4), 1029-1058. doi: 10.1111/jeea.12081

Gorwa, R., & Guilbeault, D. (2018). Unpacking the Social Media Bot: A Typology to Guide Research and Policy. *Policy & Internet*. doi: 10.1002/poi3.184

(GPO) Government Press Office. (2019). Proposal to Regulate Transparency of Online Political Advertising. Retrieved from https://www.gov.ie/en/news/9b96ef-proposal-to-regulate-transparency-of-online-political-advertising/

Greene, J. C. (2007). *Mixed Methods in Social Inquiry*. San Francisco, CA: Jossey-Bass.

Guilbeault, D. (2016). Political bots as ecological agents: The ethical implications of digital space. *International Journal of Communication*, 10 (Special Section).

Guyatt, N. (2003). *Another American century?* (1st ed.). Zed Books Ltd.

Habermas, J. (1995). Reconciliation Through the Use of Reason: Remarks on J. Rawl's Political Liberalism. *The Journal Of Philosophy*, *92*(3), 109-131. Retrieved 18 April 2020, from.

Hague, R., Harrop, M., & Breslin, S. (2001). *Comparative government and politics: an introduction* (5th ed.). London: Palgrave.

Heaton, J. (2008). Secondary analysis of qualitative data: An overview. *Historical Social Research*, 33(3), 33-45.

Heft, A., Mayerhöffer, E., Reinhardt, S., & Knüpfer, C. (2019). Beyond Breitbart: Comparing Right-Wing Digital News Infrastructures in Six Western Democracies. *Policy & Internet*, *12*(1), 20-45. doi: 10.1002/poi3.219

Helbing, D. (2015). *The automation of society is next* (1st ed.). Createspace.

Hobson, J. (2000). *The State and International Relations*. Cambridge: Cambridge University Press.

Hofverberg, E. (2019). *Government Responses to Disinformation on Social Media Platforms: Sweden*. Washington D.C.: Library of Congresss. Retrieved from https://www.loc.gov/law/help/social-media-disinformation/sweden.php

Hoke, C. (2010). Internet voting. *Proceedings Of The 2010 Workshop On Governance Of Technology, Information And Policies - GTIP '10*. doi: 10.1145/1920320.1920329

Huang, Z. (2016). Inside the Global Times, China's hawkish, belligerent state tabloid. *Quartz*. Retrieved from https://qz.com/745577/inside-the-global-times-chinas-hawkish-belligerent-state-tabloid/

Huwart, J., & Verdier, L. (2013). *Economic Globalisation: Origins and consequences*. Paris: OECD.

(ICO) Information Commissioner's Office. (2018). *Democracy disrupted? Personal information and political influence*. London. Retrieved from https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

Johnston, M., 2014. Secondary Data Analysis: A Method of Which the Time has Come. *Qualitative and Quantitative Methods in Libraries*, 3, pp.619-626.

Johnson, D. (2004). 2004 U.S. Presidential Elections. *Journal Of Political Marketing*, *3*(4), 111-113. https://doi.org/10.1300/j199v03n04_06

Jones, K. (2019). *Online Disinformation and Political Discourse: Applying a Human Rights Framework* (Fellowship). Chatman House: International Law Programme.

Jo, Y. (2011). The Capitalist World-System and U.S. Cold War Policies in the Core and the Periphery: A Comparative Analysis of Post-World War II American Nation-building in Germany and Korea. *Journal Of World-Systems Research*, 428-455. doi: 10.5195/jwsr.2011.420

Kang, C., & Frenkel, S. (2018). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. *The New York Times*. Retrieved 17 February 2020, from https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

Kauppi, M., & Viotti, P. (2012). International Relations Theory (5th ed.). Glenview: Pearson Education.

Kelven, A. (2019). Belt and Road: colonialism with Chinese characteristics. *The Interpreter - Lowy Institute*. Retrieved from https://www.lowyinstitute.org/the-interpreter/belt-and-road-colonialism-chinese-characteristics

Kennedy, S. (2016). Electoral Integrity: How Gerrymandering Matters. *Public Integrity*, *19*(3), 265-273. doi: 10.1080/10999922.2016.1225480

Kiecolt, K. J., & Nathan, L. E. (1985). *Secondary Analysis of Survey Data*. Sage University Paper Series on Quantitative Applications in the Social Sciences, 53.

Kokolis, C. (2020). Comparing the Social Media Reach of Chinese, Iranian and Russian State-Sponsored News Outlets. *Foreign Policy Research Institute*. Retrieved from https://www.fpri.org/fie/social-media-state-sponsored-news/

Kovic, M., Rauchfleisch, A., Sele, M., & Caspar, C. (2018). Digital astroturfing in politics: Definition, typology, and countermeasures. *Studies In Communication Sciences.*, *18*, 69-85. https://doi.org/10.24434/j.scoms.2018.01.005

Kragh, M., & Åsberg, S. (2017). Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal Of Strategic Studies*, *40*(6), 773-816. doi: 10.1080/01402390.2016.1273830

Krotz, U. (2014). Three eras and possible futures: a long-term view on the Franco-German relationship a century after the First World War. *International Affairs*, *90*(2), 337-350. doi: 10.1111/1468-2346.12112

Kuo, L., & Kommenda, N. (2013). What is China's Belt and Road Initiative?. *The Guardian*. Retrieved from https://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer

Leal-Arcas, R. (2011). China's Economic Rise and Regional Trade. *APEC And The Rise Of China*, 93-120. doi: 10.1142/9789814329415_0005

Lever, R. (2019). Fake Facebook accounts: the never-ending battle against bots. *Physorg*. Retrieved from https://phys.org/news/2019-05-fake-facebook-accounts-never-ending-bots.html

Levin, D. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Studies Quarterly*, *60*(2), 189-202. doi: 10.1093/isq/sqv016

Libakova, N., & Sertakova, E. (2015). The Method of Expert Interview as an Effective Research Procedure of Studying the Indigenous Peoples of the North. *Journal of Siberian Federal University*, 8(1).

Lieber, E., & Weisner T. S. (2010). Meeting the practical challenges of mixed methods research. In A. Tashakkori & C. Teddlie (Eds.), *Mixed Methods in Social & Behavioral Research*, 2nd Ed. (pp. 559–611). Thousand Oaks, CA: Sage.

Lieberman, E. (2001). National Political Community and the Politics of Income Taxation in Brazil and South Africa in the Twentieth Century. *Politics & Socie*ty, 29(4), 515-555. https://doi.org/10.1177/0032329201029004003

Lieberman, E. (2005). Nested Analysis as a Mixed-Method Strategy for Comparative Research. *American Political Science Review*, 99(3), 435-452. https://doi.org/10.1017/s0003055405051762

Lippert, T. (2019). *NATO, Climate Change, and International Security: A Risk Governance Approach* (1st ed.). Springer International Publishing.

Liu, T., & Woo, W. (2018). Understanding the U.S.-China Trade War. *China Economic Journal*, *11*(3), 319-340. doi: 10.1080/17538963.2018.1516256

LoGiurato, B. (2014). RT Is Very Upset With John Kerry For Blasting Them As Putin's 'Propaganda Bullhorn'. *Business Insider*. Retrieved from https://www.businessinsider.com/john-kerry-rt-propaganda-bullhorn-russia-today-2014-4?international=true&r=US&IR=T

Louw, P. (2013). *The Media and Political Process* (1st ed.). Los Angeles: Sage.

Ma, C. (2020). *The Computational Propaganda Project*. The Computational Propaganda Project. Retrieved 12 April 2020, from https://comprop.oii.ox.ac.uk/.

Macintosh, A. (2008). E-Democracy and E-Participation Research in Europe. *Digital Government*, 85-102. doi: 10.1007/978-0-387-71611-4_5

MacMillan, M. (2020). Rebuilding the world after the second world war. *The Guardian*. Retrieved from https://www.theguardian.com/world/2009/sep/11/second-world-war-rebuilding

Magee, T., Lee, S. M., Giuliano, K. K., & Munro, B. (2006). Generating new knowledge from existing data: The use of large data sets for nursing research. *Nursing Research*, 55(2), S50-S56.

Maher, L., & Dertadian, G. (2017). Qualitative research. *Addiction*, *113*(1), 167-172. doi: 10.1111/add.13931

Maisel, L. (2007). *American political parties and elections* (1st ed.). Oxford University Press.

Mann, T. (2001). An Agenda for Election Reform. *Brookings*. Retrieved from https://www.brookings.edu/research/an-agenda-for-election-reform/

Mansfield-Devine, S. (2018). Hacking democracy: abusing the Internet for political gain. *Network Security*, *2018*(10), 15-19. https://doi.org/10.1016/s1353-4858(18)30102-8

Maréchal, N. (2016). When bots tweet: Toward a normative framework for bots on social networking sites. *International Journal of Communication*, 10 (Special Section).

Marsden, C., Meyer, T., & Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation?. *Computer Law & Security Review*, *36*, 105373. doi: 10.1016/j.clsr.2019.105373

Martínez, C., Belleboni, E., García, S., Oliva y, A., & Blázquez, J. (2007). Use of web service orchestration strategies in operations on digital democracy platform. *Proceedings Of The 2007 Euro American Conference On Telematics And Information Systems - EATIS '07*. https://doi.org/10.1145/1352694.1352745

Martin-Rozumiłowicz, B., & Kužel, R. (2019). *Social Media, Disinformation and Electoral Integrity: IFES Working Paper*. IFES. Retrieved from https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf

McDermott, D. (1999). The Duty to Punish and Legitimate Government. *Journal of Political Philosophy*, 7(2), 147-171. https://doi.org/10.1111/1467-9760.00071

McFaul, M., Kass, B., Lin, H., Stamos, A., Grotto, A., & Persily, N. et al. (2019). *Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*. Stanford: The Cyber Policy Center of the Freeman Spogli Institute for International Studies at Stanford.

McNeice, S. (2019). New proposals aimed at regulating online political advertising have been approved by the Cabinet. *Newstalk*. Retrieved from https://www.newstalk.com/news/online-political-ads-regulation-921802

McTague, T. (2020). Why Britain Brexited. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2020/01/britain-brexit-boris-johnson-influence-control/605734/

Micaud, C. (1946). The Launching of the Fourth French Republic. *The Journal Of Politics*, *8*(3), 292-307. doi: 10.2307/2125331

Milward, A. (2005). *Politics and economics in the history of the European Union*. London: Routledge.

Mitchell, A., Gottfried, J., Barthel, M., & Shearer, E. (2016). The Modern News Consumer: News attitudes and practices in the digital era. *Pew Research Center*.

Retrieved 16 April 2020, from https://www.journalism.org/2016/07/07/the-modern-news-consumer/.

Mittelstadt, B. (2016). Auditing for transparency in content personalization systems. *International Journal of Communication*, 10 (Special Section).

Moore, M. (2018). *Democracy Hacked : How Russian Hackers, Secretive Plutocrats, and Freextremists Are Undermining Democracy and Gaming Elections*. London: Oneworld Publications.

Moynihan, D. (2008). E-Voting in the United States. *Electronic Government*, 1247-1254. doi: 10.4018/978-1-59904-947-2.ch092

Mueller, R., 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. 1st ed. Washington D.C.: Special Counsel Robert S. Mueller, III.

Munck, G. L., & Snyder, R. (2007a). Debating the direction of comparative politics: An analysis of leading journals. *Comparative Political Studies*, 40(1), 5-31.

Neuman, W. (2018). *The Digital Difference* (1st ed.). Cambridge, Massachusetts: Harvard University Press.

Newton, C. (2019). Singapore's fake news law should be a warning to American lawmakers. *The Verge*. Retrieved from https://www.theverge.com/interface/2019/12/3/20991422/singapore-fake-news-law-censorship-politics-usa

Nordin, A., & Weissmann, M. (2018). Will Trump make China great again? The belt and road initiative and international order. *International Affairs*, *94*(2), 231-249. doi: 10.1093/ia/iix242

Norris, P. (2014). Why Electoral Integrity Matters. doi: 10.1017/cbo9781107280861

Office of the Director of National Intelligence, & National Intelligence Council. (2017). *Assessing Russian activities and intentions in recent US elections* (1st ed.). Washington D.C.: Penny Hill Press.

Omotosho, M. (2019). Information Revolution and Growing Power of Communication: A Foundation of New Diplomacy. *Jadavpur Journal Of International Relations*, *23*(2), 142-157. doi: 10.1177/0973598419861472

107th United States Congress. Help America Vote Act (2002).

114th Congress. Countering Foreign Propaganda and Disinformation Act (2016). Washington D.C.

116th Congress. Bot Disclosure and Accountability Act (2019). Washington D.C.

116th Congress. H.R.2592 / Honest Ads Act (2019). Washington D.C.

Orenstein, M. (2015). Geopolitics of a Divided Europe. *East European Politics And Societies: And Cultures*, *29*(2), 531-540. doi: 10.1177/0888325414559050

Orttung, R., & Nelson, E. (2018). Russia Today's strategy and effectiveness on YouTube. *Post-Soviet Affairs*, *35*(2), 77-92. doi: 10.1080/1060586x.2018.1531650

Osborn, A. (2005). Russia's 'CNN' wants to tell it like it is. *The Age*. Retrieved from https://www.theage.com.au/world/russias-cnn-wants-to-tell-it-like-it-is-20050816-ge0p8t.html

OSCE. (2015). *Propaganda and Freedom of the Media*. Vienna. Retrieved from https://www.osce.org/fom/203926?download=true

OxfordLanguages. (2016). Word of the Year 2016. Retrieved 18 April 2020, from https://languages.oup.com/word-of-the-year/2016/.

Pacepa, I., & Rychlak, R. (2013). Disinformation (2nd ed., pp. 4-6, 34-39, 75). WND Books.

Packard, A. (2013). *Digital Media Law*. Chichester: Wiley-Blackwell.

Paquet-Clouston, M., Bilodeau, O., & Décary-Hétu, D. (2017). Can We Trust Social Media Data?. *Proceedings Of The 8Th International Conference On Social Media & Society - #Smsociety17*. doi: 10.1145/3097286.3097301

Patton, M. (2015). *Qualitative Research & Evaluation Methods*. Sage.

Raymer, K., & Harriss, L. (2017). Online Information and Fake News. *UK Parliamentary Blog*. Retrieved from https://post.parliament.uk/research-briefings/post-pn-0559/

Persily,, N., Metzger, M., & Krowitz, Z. (2019). Confronting Efforts at Election Manipulation from Foreign Media Organizations. *Stanford Cyber Policy Center*.

Pettigrew, T. (2017). Social psychological perspectives on Trump supporters. *Journal Of Social And Political Psychology*, *5*(1), 107-116. doi: 10.5964/jspp.v5i1.750

Pierre, J. (2020). Make America Open Again: Grassroots Protest or Astroturfing?. *Psychology Today*. Retrieved from https://www.psychologytoday.com/hk/blog/psych-unseen/202004/make-america-open-again-grassroots-protest-or-astroturfing

Platform Policy - Facebook for Developers. (2020). Retrieved 8 April 2020, from https://developers.facebook.com/policy/

Pope, A. (2018). Cyber-securing our elections. *Journal Of Cyber Policy*, *3*(1), 24-38. https://doi.org/10.1080/23738871.2018.1473887

Rawls, J. (1993). *Political Liberalism* (1st ed.). Columbia University Press.

Reichert, F. (2012). *You Vote What You Read?* (1st ed., pp. 4-6). München: GRIN Verlag GmbH.

Reif, K., & Schmitt, H. (1980). 'Nine Second-Order National Elections: A Conceptual Framework for the Analysis of European Election Results'. *European Journal Of Political Research*, *8*(1), 3-44. doi: 10.1111/j.1475-6765.1980.tb00737.x

Regeringskansliet. (2018). *Strategi för en stark demokrati – främja, förankra, försvara*. Stockholm: Regeringskansliet. Retrieved from https://www.regeringen.se/informationsmaterial/2018/06/strategi-for-en-stark-demokrati--framja-forankra-forsvara/

Rivlin, A. (2000). *Reviving the American Dream* (1st ed.). Boulder, Colo.: NetLibrary, Inc.

Rizvi, H. (2010). MEDIA: Foreign News Channels Drawing U.S. Viewers. *Inter Press Service News Agency*. Retrieved from http://www.ipsnews.net/2010/01/media-foreign-news-channels-drawing-us-viewers/

Rohlfing, I. (2007). What You See and What You Get. *Comparative Political Studies*, 41(11), 1492-1514. https://doi.org/10.1177/0010414007308019

Russia Briefing. (2012). 'Russia Today' Doubles its U.S. Audience. Retrieved from https://www.russia-briefing.com/news/russia-today-to-double-its-u-s-audience.html/

Samson, J. (2001). *The British empire*. Oxford: Oxford University Press.

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2016). When the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software. *International Journal of Communication*, 10 (Special Section).

Satariano, A. (2019). Facebook Identifies Russia-Linked Misinformation Campaign. *The New York Times*. Retrieved from https://www.nytimes.com/2019/01/17/business/facebook-misinformation-russia.html

Schedler, A. (2002). The Menu of Manipulation. *Journal Of Democracy*, *13*(2), 36-50. doi: 10.1353/jod.2002.0031

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare* (1st ed.). Cambridge: Cambridge University Press.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (1st ed.). Cambridge: Cambridge University Press.

Seagrave, S. (2015). Madison's Tightrope: The Federal Union and the Madisonian Foundations of Legitimate Government. *Polity*, 47(2), 249-272. https://doi.org/10.1057/pol.2015.4

Semple, J. (2018). Growing popularity of Kremlin network RT signals the age of information war. *Global News*. Retrieved from https://globalnews.ca/news/4540034/fake-news-wars-kremlin-network-rt/

Shahbaz, A., & Funk, A. (2019). *Freedom on the Net 2019 Key Finding: Politicians and hyperpartisans use digital means to manipulate elections.*. Washington D.C.: Freedom House. Retrieved from https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference

Shambaugh, D. (2013). *China Goes Global* (1st ed.). Oxford: Oxford University Press.

Shenkman, R. (2019). The Shocking Paper Predicting the End of Democracy. *Politico*. Retrieved from https://www.politico.com/magazine/story/2019/09/08/shawn-rosenberg-democracy-228045

Shorey, S., & Howard, P. (2016). Automation, Big Data, and Politics: A Research Review. *International Journal Of Communication*, *10*, 5032–5055. Retrieved 23 April 2020, from.

Skierka, I. (2014). Cybersecurity – How Policy Makers Fail. The Centre Of Ethical Education In The Armed Forces, 1(2). Retrieved 10 February 2020, from http://www.ethikundmilitaer.de/en/full-issues/20142-cyberwar/skierka-cybersecurity-how-policy-makers-fail/.

Stengel, R. (2014). *Russia Today's Disinformation Campaign*. Washington D.C.: U.S. Department of State.

Stewart, D. W., & Kamins, M. A. (1993). *Secondary Research: Information Sources and Methods*. Newbury Park, CA: Sage.

Smith, A. K., Ayanian, J. Z., Covinsky, K. E., Landon, B. E., McCarthy, E. P., Wee, C. C., & Steinman, M. A. (2011). Conducting high-value secondary dataset analysis: An introductory guide and resources. *Journal of General Internal Medicine*, 28(8), 920- 929. doi:10.1007/s11606-010-1621-5

Sullivan, B. (2020). Fox News Faces Lawsuit For Calling COVID-19 A 'Hoax'. *Forbes*. Retrieved from https://www.forbes.com/sites/legalentertainment/2020/04/10/covid-19-lawsuit-against-fox-news/#6ec39cd35739

Susskind, J. (2018). Future Politics: Living Together in a World Transformed by Tech

Suzor, N. (2019). *Lawless: the secret rules that govern our digital lives* (1st ed., pp. 11-12). Cambridge: Cambridge University Press.

Swedish Security Service. (2018). *Attempts to influence confidence in the election process*. Stockholm: Swedish Security Service. Retrieved from https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-08-31-attempts-to-influence-confidence-in-the-election-process.html

Synovitz, R. (2020). As Countries Emerge From COVID-19 Lockdowns, Debates Emerge On How, When To Hold Elections. *Radio Free Europe - Liberty Radio*. Retrieved from https://www.rferl.org/a/as-countries-emerge-from-covid-19-

lockdowns-debates-emerge-on-how-when-to-hold-important-elections/30605872.html

Tambini, D. (2017). *Study on the use of internet in electoral campaigns*. Brussels: EU Committee of experts on media pluralism and transparency of media ownership. Retrieved from https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24

Tarran, B. (2018). What can we learn from the Facebook-Cambridge Analytica scandal?. *Significance*, *15*(3), 4-5. doi: 10.1111/j.1740-9713.2018.01139.x

Taylor, E., Walsh, S., & Bradshaw, S. (2018). *Industry Responses to Malicious Use of Social Media*. Riga: NATO Strategic Communications Centre of Excellence.

Taylor, M. (2019). Combating disinformation and foreign interference in democracies: Lessons from Europe. *Brookings*. Retrieved 9 April 2020, from https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

Tett, G. (2020). Can you win an election without digital skulduggery?. *Financial Times*. Retrieved from https://www.ft.com/content/b655914a-3209-11ea-9703-eea0cae3f0de

Tharoor, I. (2019). The world doesn't want to pick between the U.S. and China. *The Washington Post*. Retrieved from https://www.washingtonpost.com/

Tomz, M., & Weeks, J. (2019). Public Opinion and Foreign Electoral Intervention. *American Political Science Review*, 1-18. https://doi.org/10.1017/s0003055420000064

Tömmel, I. (2014). *The European Union: what it is and how it works* (1st ed.). Basingstoke: Palgrave Macmillan.

2019 Ranking Digital Rights Corporate Accountability Index. (2019). Retrieved 8 April 2020, from https://rankingdigitalrights.org/index2019/indicators/

Uchill, J. (2019). U.S. laws don't cover campaign disinformation. *Axios*. Retrieved from https://www.axios.com/us-laws-dont-cover-campaign-disinformation-b45267dc-270f-4cc9-bb79-a5b61e60ffc0.html

Underhill, W. (2012). *Elections in the Digital World: February 2012*. Washington D.C.: National Conference of State Legislatures. Retrieved from https://www.ncsl.org/research/elections-and-campaigns/elections-in-the-digital-world.aspx

UN General Assembly. (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN General Assembly. Retrieved from https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf

UN General Assembly. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York City: UN General Assembly. Retrieved from https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

(UN) United Nations. (1948). Universal Declaration of Human Rights. New York City.

(UN) United Nations. (1966). International Covenant on Civil and Political Rights. New York City.

United Nations Conference on International Organization. (1945). *Charter of the United Nations*. San Francisco: United Nations Conference on International Organization.

UN Office of the High Commissioner. (2011). *Guiding Principles on Business and Human Rights*. New York City: United Nations. Retrieved from https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

U.S. Federal Election Commission. (2016). *FEDERAL ELECTIONS 2016 Election Results for the U.S. President, the U.S. Senate and the U.S. House of Representatives*. Washington D.C.: Federal Election Commission. Retrieved from https://transition.fec.gov/pubrec/fe2016/federalelections2016.pdf

U.S. Government Publishing Office. (2018). *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security, A Minority Staff Report*

Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session. Washington D.C.: U.S. Government Publishing Office.

Van Mead i, N. (2018). China in Africa: win-win development, or a new colonialism?. *The Guardian*. Retrieved from https://www.theguardian.com/cities/2018/jul/31/china-in-africa-win-win-development-or-a-new-colonialism

van Zuylen-Wood, S. (2017). At RT, News Breaks You. *Bloomberg*. Retrieved from https://www.bloomberg.com/features/2017-rt-media/

Vargo, C., & Guo, L. (2016). Networks, Big Data, and Intermedia Agenda Setting: An Analysis of Traditional, Partisan, and Emerging Online U.S. News. *Journalism & Mass Communication Quarterly*, *94*(4), 1031-1055. doi: 10.1177/1077699016679976

Verhofstadt, G. (2020). Is COVID-19 Killing Democracy?. *Project Syndicate*. Retrieved from https://www.project-syndicate.org/commentary/covid19-democracy-violations-by-guy-verhofstadt

Ward, C. (2020). Russian election meddling is back -- via Ghana and Nigeria -- and in your feeds. *CNN*. Retrieved from https://edition.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

Weintraub, E. (2019). *Internet Ad Disclaimers Rulemaking Proposal*. Washington D.C.: Federal Election Commission.

Weiss, B., Cranley, E., & Panetta, G. (2020). Here's everyone who has been charged, convicted, and sentenced in the Russia probe so far. *Business Insider*. Retrieved from https://www.businessinsider.nl/who-has-been-charged-in-russia-investigation-mueller-trump-2017-12?international=true&r=US

Wendling, M. (2018). The (almost) complete history of 'fake news'. *BBC*. Retrieved 21 April 2020, from https://www.bbc.com/news/blogs-trending-42724320.

Wheeler, T. (2019). Don't Panic: The Digital Revolution Isn't as Unusual as You Think. *Knowledge@Warton*. Retrieved 21 April 2020, from https://knowledge.wharton.upenn.edu/article/tom-wheeler-fcc-book/.

Wong, J. (2018). Mark Zuckerberg apologises for Facebook's 'mistakes' over Cambridge Analytica. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica#maincontent

Wooley, C., & Howard, P. (2016). Political Communication, Computational Propaganda, and Autonomous Agent. *International Journal Of Communication*, *10*, 4882–4890.

Yablokov, I. (2015). Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). *Politics*, *35*(3-4), 301-315. doi: 10.1111/1467-9256.12097

Yun Chee, F. (2019). Facebook, Google, Twitter urged to do more to combat fake news in EU. *Reuters*. Retrieved from https://www.reuters.com/article/us-eu-tech-fakenews/facebook-google-twitter-urged-to-do-more-to-combat-fake-news-in-eu-idUSKBN1X819V

Zeng, W., & Sparks, C. (2019). Popular nationalism: Global Times and the US–China trade war. *International Communication Gazette*, *82*(1), 26-41. doi: 10.1177/1748048519880723

Zialcita, P. (2019). Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal. *NPR*. Retrieved from https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal?t=1588262865709